PROYECTO DE NORMA MEXICANA

PROY-NMX-I-27002-NYCE-2022

Seguridad de la información, ciberseguridad y protección de la privacidad – Controles de seguridad de la información

Information security, cybersecurity and privacy protection – Information security controls

ESTA NORMA MEXICANA CANCELA A LA NORMA NMX-I-27002-NYCE-2015

SINEC-20221125204641986 **ICS: 35.030**

P R E F A C I O

1. **Este Proyecto de Norma Mexicana fue elaborado en el seno del Subcomité de Seguridad de TI del Comité Técnico de Normalización Nacional de Electrónica y Tecnologías de la Información y Comunicación de NYCE, con la participación de las siguientes Instituciones y Empresas:**

   - C8 CONSULTING SERVICES, S.A. DE C.V.
   - CREATIVIDAD Y EXPERIENCIA EN TI A.C.
   - NATIONAL ELECTRICAL MANUFACTURERS ASSOCIATION
   - NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C.
   - ONSILIUM S.A. DE C.V.
   - SEGURIDATA PRIVADA, S.A. DE C.V.
   - SIGNIFY
   - SOCIEDAD INTERNACIONAL DE ACREDITACIÓN, A.C.
   - TEMANOVA
   - TMI ABOGADOS, S.C.
   - UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

2. **Por otra parte, también fue aprobado por las instituciones y empresas que a continuación se señalan y que conforman el Comité Técnico de Normalización Nacional de Electrónica y Tecnologías de la Información y Comunicación de NYCE.**

   - ADVANCE WIRE&WIRELESS LABORATORIOS
   - ASOCIACIÓN MEXICANA DE EMPRESAS DEL RAMO DE INSTALACIONES PARA LA CONSTRUCCIÓN, A.C.
   - ASOCIACIÓN MEXICANA DE INTERNET, A.C.
   - ASOCIACIÓN NACIONAL DE INSTITUCIONES DE EDUCACIÓN EN INFORMÁTICA.
   - ASOCIACIÓN NACIONAL DE TELECOMUNICACIONES.
   - ASOCIACIÓN DE PERMISIONARIOS, OPERADORES Y PROVEEDORES DE LA INDUSTRIA DEL ENTRETENIMIENTO Y JUEGO DE APUESTA EN MÉXICO, A.C.
   - AUREN IBEROAMERICA S. DE R.L. DE C.V.
   - BEST PRACTICES GURUS, S.A. DE C.V.
   - CÁMARA NACIONAL DE LA INDUSTRIA ELECTRÓNICA, DE TELECOMUNICACIONES Y TECNOLOGÍAS DE LA INFORMACIÓN.

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

- COLEGIO DE INGENIEROS EN COMUNICACIONES Y ELECTRÓNICA.
- COMISIÓN NACIONAL PARA EL USO EFICIENTE DE LA ENERGÍA.
- DIRECCIÓN GENERAL DE NORMAS.
- ERICSSON TELECOM, S.A. DE C.V.
- GRUPO ADO.
- INSTITUTO POLITÉCNICO NACIONAL.
- INSTITUTO MEXICANO DE NORMALIZACIÓN Y CERTIFICACIÓN, A.C.
- INNOVACIONES TELEMÁTICAS, S.A. DE C.V.
- INTELI, S.C.
- LEGRAND S.A. DE C.V.
- ORGANISMO NACIONAL DE NORMALIZACIÓN Y CERTIFICACIÓN DE LA CONSTRUCCIÓN Y EDIFICACIÓN, S.C.
- PROCURADURÍA FEDERAL DEL CONSUMIDOR.
- REDIT.
- SIEMON.
- TELEMATICA INNOVO CONTINUO, S.A DE C.V.
- UNIVERSIDAD AUTÓNOMA METROPOLITANA.
- UNIVERSIDAD IBEROAMERICANA.
- UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO.

3. La entrada en vigor de esta Norma Mexicana será 60 días después de la publicación de su Declaratoria de Vigencia en el Diario Oficial de la Federación.

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

Índice del contenido

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

PROYECTO DE NORMA MEXICANA

PROY-NMX-I-27002-NYCE-2022

Seguridad de la información, ciberseguridad y protección de la privacidad – Controles de seguridad de la información

(Cancelará a la NMX-I-27002-NYCE-2015)

Information security, cybersecurity and privacy protection – Information security controls

0 Introducción

0.1 Antecedentes y contexto

Este Proyecto de Norma Mexicana está diseñado para organizaciones de todos los tipos y tamaños. Se utiliza como referencia para determinar e implementar controles para el tratamiento de riesgos de seguridad de la información en un sistema de gestión de seguridad de la información (SGSI) basado en la NMX-I-27001-NYCE-2015. También se puede utilizar como un documento de orientación para las organizaciones que determinan e implementan controles de seguridad de la información comúnmente aceptados. Además, este Proyecto de Norma Mexicana está destinado a ser utilizado en el desarrollo de directrices de gestión de seguridad de la información específicas de la industria y la organización, teniendo en cuenta su entorno específico de riesgo de seguridad de la información. Los controles organizacionales o específicos del entorno distintos de los incluidos en este Proyecto de Norma Mexicana se pueden determinar a través de la evaluación de riesgos según sea necesario.

Organizaciones de todos los tipos y tamaños (incluidos los sectores público y privado, comercial y sin fines de lucro) crean, recopilan, procesan, almacenan, transmiten y eliminan información en muchas formas, incluidas las electrónicas, físicas y verbales (por ejemplo, conversaciones y presentaciones).

El valor de la información va más allá de las palabras escritas, los números y las imágenes: el conocimiento, los conceptos, las ideas y las marcas son ejemplos de formas intangibles de información. En un mundo interconectado, la información y otros activos asociados merecen o requieren protección contra diversas fuentes de riesgo, ya sean naturales, accidentales o deliberadas.

La seguridad de la información se logra mediante la implementación de un conjunto adecuado de controles, incluidas políticas, reglas, procesos, procedimientos, estructuras organizativas y funciones de software y hardware. Para cumplir con sus objetivos específicos de seguridad y negocio, se sugiere que la organización defina, implemente, monitore, revise y mejore estos controles cuando sea necesario. Un SGSI como el especificado en la NMX-I-27001-NYCE-2015 adopta una visión holística y coordinada de los riesgos de seguridad de la información de la organización para determinar e implementar un conjunto integral de controles de seguridad de la información dentro del marco general de un sistema de gestión coherente.

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

Muchos sistemas de información, incluida su gestión y operaciones, no han sido diseñados para ser seguros en términos de un SGSI como se especifica en la NMX-I-27001-NYCE-2015 y este Proyecto de Norma Mexicana. El nivel de seguridad que sólo puede lograrse mediante medidas tecnológicas es limitado y es conveniente este respaldado por actividades de gestión y procesos organizativos adecuados. Se recomienda identificar qué controles están en su lugar requiere una planificación cuidadosa y atención al detalle al llevar a cabo el tratamiento de riesgo.

Un SGSI exitoso requiere el apoyo de todo el personal de la organización. También puede requerir la participación de otras partes interesadas, como accionistas o proveedores. También se puede necesitar el asesoramiento de expertos en la materia.

Un sistema de gestión de la seguridad de la información adecuado y eficaz garantiza a la dirección de la organización y a otras partes interesadas que su información y otros activos asociados se mantienen razonablemente seguros y protegidos contra amenazas y daños, lo que permite a la organización alcanzar los objetivos comerciales establecidos.

0.2 Requisitos de seguridad de la información

Es especial que una organización determine sus requisitos de seguridad de la información. Existen tres fuentes principales de requisitos de seguridad de la información:

a) la evaluación de los riesgos para la organización, teniendo en cuenta la estrategia y los objetivos generales de la organización. Esto se puede facilitar o apoyar a través de una evaluación de riesgos específica de la seguridad de la información. Se recomienda dar lugar a la determinación de los controles necesarios para garantizar que el riesgo residual para la organización cumpla con sus criterios de aceptación de riesgos;

b) los requisitos legales, estatutarios, reglamentarios y contractuales que una organización y sus partes interesadas (socios comerciales, proveedores de servicios, etc.) se recomienda cumplir y su entorno sociocultural;

c) el conjunto de principios, objetivos y requisitos de negocio para todos los pasos del ciclo de vida de la información que una organización ha desarrollado para apoyar sus operaciones.

0.3 Controles

Un control se define como una medida que modifica o mantiene el riesgo. Algunos de los controles de este Proyecto de Norma Mexicana son controles que modifican el riesgo, mientras que otros mantienen el riesgo. Una política de seguridad de la información, por ejemplo, solo puede mantener el riesgo, mientras que el cumplimiento de la política de seguridad de la información puede modificar el riesgo. Además, algunos controles describen la misma medida genérica en diferentes contextos de riesgo. Este Proyecto de Norma Mexicana proporciona una mezcla genérica de controles de seguridad de la información organizacionales, de personas, físicos y tecnológicos derivados de las mejores prácticas reconocidas internacionalmente.

0.4 Determinación de controles

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

La determinación de los controles depende de las decisiones de la organización después de una evaluación de riesgos, con un alcance claramente definido. Se recomienda que las decisiones relacionadas con los riesgos identificados se basen en los criterios de aceptación de riesgos, las opciones de tratamiento de riesgos y el enfoque de gestión de riesgos aplicado por la organización. Se recomienda que la determinación de los controles también tenga en cuenta toda la legislación y los reglamentos nacionales e internacionales pertinentes. La determinación del control también depende de la forma en que los controles interactúan entre sí para proporcionar una defensa en profundidad.

La organización puede diseñar controles según sea necesario o identificarlos desde cualquier origen. Al especificar tales controles, se recomienda que la organización considere los recursos y la inversión necesarios para implementar y operar un control contra el valor comercial realizado. Consulte la norma que se indica en el inciso 10.21 para obtener orientación sobre las decisiones relativas a la inversión en un SGSI y las consecuencias económicas de estas decisiones en el contexto de los requisitos competitivos de recursos.

Se recomienda halla un equilibrio entre los recursos desplegados para la aplicación de los controles y el posible impacto en el negocio resultante de los incidentes de seguridad en ausencia de esos controles. Es conveniente que los resultados de una evaluación de riesgos ayuden a orientar y determinar las medidas de gestión adecuadas, las prioridades para gestionar los riesgos de seguridad de la información y para aplicar los controles que se determinen necesarios para protegerse contra estos riesgos.

Algunos de los controles de este Proyecto de Norma Mexicana pueden considerarse como principios rectores para la gestión de la seguridad de la información y aplicables a la mayoría de las organizaciones. Puede encontrar más información sobre la determinación de controles y otras opciones de tratamiento de riesgos en la NMX-I-27005-NYCE-2019.

0.5 Elaboración de directrices específicas para cada organización

Este Proyecto de Norma Mexicana puede considerarse como un punto de partida para desarrollar directrices específicas de la organización. No todos los controles y orientaciones de este Proyecto de Norma Mexicana pueden ser aplicables a todas las organizaciones. También se pueden requerir controles y directrices adicionales no incluidos en este Proyecto de Norma Mexicana para abordar las necesidades específicas de la organización y los riesgos que se han identificado. Cuando se desarrollan documentos que contienen directrices o controles adicionales, puede ser útil incluir referencias cruzadas a capítulos en este Proyecto de Norma Mexicana para futuras referencias.

0.6 Consideraciones del ciclo de vida

La información tiene un ciclo de vida, desde la creación hasta la eliminación. El valor y los riesgos para la información pueden variar a lo largo de este ciclo de vida (por ejemplo, la divulgación no autorizada o el robo de las cuentas financieras de una empresa no es significativo después de que se hayan publicado, pero la integridad sigue siendo crítica), por lo tanto, la seguridad de la información sigue siendo importante en cierta medida en todas las etapas.

Los sistemas de información y otros activos relevantes para la seguridad de la información tienen ciclos de vida dentro de los cuales se conciben, especifican, diseñan, desarrollan, prueban, implementan, utilizan, mantienen y, finalmente, se retiran del

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

servicio y se eliminan. Se recomienda que la seguridad de la información sea considerada en cada etapa. Los nuevos proyectos de desarrollo de sistemas y los cambios en los sistemas existentes brindan oportunidades para mejorar los controles de seguridad al tiempo que se tienen en cuenta los riesgos de la organización y las lecciones aprendidas de los incidentes.

0.7 Normas internacionales conexas

Si bien este Proyecto de Norma Mexicana ofrece orientación sobre una amplia gama de controles de seguridad de la información que se aplican comúnmente en muchas organizaciones diferentes, otras normas de la familia NMX-I-27000-NYCE brindan asesoramiento o requisitos complementarios sobre otros aspectos del proceso general de gestión de la seguridad de la información.

Consulte la NMX-I-27000-NYCE-2019 para obtener una introducción general tanto al SGSI como a la familia de normas. La NMX-I-27000-NYCE-2019 proporciona un glosario, que define la mayoría de los términos utilizados en toda la familia de normas NMX-I-27000-NYCE, y describe el alcance y los objetivos para cada miembro de la familia.

Existen normas sectoriales específicas que tienen controles adicionales que tienen como objetivo abordar áreas específicas (por ejemplo, la norma que se indica en el inciso 10.22 para servicios en la nube, la NMX-I-27701-NYCE-2021 para privacidad, la norma que se indica en el inciso 10.23 para energía, la norma que se indica en el inciso 10.20 para organizaciones de telecomunicaciones y la NMX-I-27799-NYCE-2015 para la salud). Tales normas están incluidas en la Bibliografía y algunas de ellas se mencionan en los incisos de orientación y otra información en los capítulos 5 al 8.

1 Objetivo y campo de aplicación

Este Proyecto de Norma Mexicana proporciona un conjunto de referencia de controles genéricos de seguridad de la información, incluida la guía de implementación. Este Proyecto de Norma Mexicana está diseñado para ser utilizado por organizaciones:

a) en el contexto de un sistema de gestión de la seguridad de la información (SGSI) basado en la NMX-I-27001-NYCE-2015;

b) para aplicar controles de seguridad de la información basados en las mejores prácticas reconocidas internacionalmente;

c) para desarrollar directrices de gestión de la seguridad de la información específicas de la organización.

2 Referencias normativas

Para la correcta aplicación de este Proyecto de Norma Mexicana, se requiere consultar las siguientes Normas Mexicanas vigentes o las que la sustituyan:

NMX-CC-9000-IMNC-2015	Sistemas de gestión de la calidad - Fundamentos y vocabulario (Cancela a la NMX-CC-9000-IMNC-2008)

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

NMX-I-22301-NYCE-2021	Tecnologías de la información - Seguridad y resiliencia - Sistemas de gestión de la continuidad del negocio - Requerimientos (Cancela a la NMX-I-22301-NYCE-2015)
NMX-I-27000-NYCE-2019	Tecnologías de la información - Técnicas de seguridad - Sistemas de gestión de seguridad de la información - Fundamentos y vocabulario (Cancela a la NMX-I-27000-NYCE-2014)
NMX-I-27001-NYCE-2015	Tecnologías de la información – Técnicas de seguridad – Sistemas de gestión de seguridad de la información – Requisitos (Cancela a la NMX-I-27001-NYCE-2009)
NMX-I-27002-NYCE-2015	Tecnologías de la información - Técnicas de seguridad - Código de buenas prácticas para el control de la seguridad de la información (Cancela a la NMX-I-27002-NYCE-2009)
NMX-I-27005-NYCE-2019	Tecnologías de la información – Técnicas de seguridad – Gestión del riesgo en seguridad de la información (Cancela a la NMX-I-27005-NYCE-2011)
NMX-I-27018-NYCE-2021	Tecnologías de la información - Técnicas de seguridad - Código de práctica para la protección de datos personales (DP) en nubes públicas que actúan como encargados de DP (Cancela a la NMX-I-27018-NYCE-2016)
NMX-I-27031-NYCE-2019	Tecnologías de la información - Técnicas de seguridad - Guías sobre preparación de tecnologías de la información y comunicación para la continuidad del negocio
NMX-I-27037-NYCE-2015	Tecnologías de la información - Técnicas de seguridad - Directrices para la identificación, recopilación, adquisición y preservación de la evidencia digital
NMX-I-27701-NYCE-2021	Tecnologías de la información - Técnicas de seguridad - Extensión de la NMX-I-27001-NYCE-2015 y la NMX-I-27002-NYCE-2015, para la gestión de la privacidad de la información - Requisitos y lineamientos
NMX-I-27799-NYCE-2015	Tecnologías de la información - Informática sanitaria – Gestión de la seguridad de la información en sanidad utilizando la NMX-I-27002-NYCE-2015
NMX-J-SAST-55001-ANCE-IMNC-2015	Gestión de activos - Sistemas de gestión – Requisitos

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

NMX-SAST-31000-IMNC-2018 Gestión del riesgo-Directrices (Cancela a la NMX-SAST-31000-IMNC-2016)

3 Términos, definiciones y términos abreviados

3.1 Términos y definiciones

Para los propósitos de este Proyecto de Norma Mexicana se aplican las definiciones siguientes, así como las del portal del inciso 10.49 y las del portal del inciso 10.50:

3.1.1 Control de acceso

Significa garantizar que el acceso físico y lógico a los activos (3.1.2) esté autorizado y restringido en función de los requisitos empresariales y de seguridad de la información.

3.1.2 Activo

Cualquier cosa que tenga valor para la organización

Nota 1 a la entrada: En el contexto de la seguridad de la información, se pueden distinguir dos tipos de activos:

- los activos primarios:
  - información;
  - procesos de negocio (3.1.27) y actividades;
- los activos de apoyo (de los que se basan los activos primarios) de todo tipo, por ejemplo:
  - hardware;
  - programas informáticos;
  - red;
  - personal (3.1.20);
  - sitio;
  - estructura de la organización.

3.1.3 Atacar

Intento no autorizado exitoso o fallido de destruir, alterar, deshabilitar, obtener acceso a un activo (3.1.2) o cualquier intento de exponer, robar o hacer uso no autorizado de un activo (3.1.2).

3.1.4 Autenticación

Garantía de que una característica reivindicada de una entidad (3.1.11) es correcta.

3.1.5 Autenticidad

Propiedad que una entidad (3.1.11) es lo que dice ser.

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

3.1.6 Cadena de custodia

Posesión, movimiento, manipulación y localización demostrables del material desde un punto en el tiempo hasta otro.

Nota 1 a la entrada: El material incluye información y otros activos asociados (3.1.2) en el contexto de la NMX-I-27002-NYCE-2015.

[FUENTE: La norma que se indica en el inciso 10.29, inciso 3.1, modificada — "Nota 1 a la entrada" añadida].

3.1.7 Información confidencial

Información que no está destinada a ser puesta a disposición o divulgada a personas, entidades o procesos no autorizados (3.1.11) o procesos (3.1.27).

3.1.8 Control

Medida que mantiene y/o modifica el riesgo

Nota 1 a la entrada: Los controles incluyen, entre otros, cualquier proceso (3.1.27), política (3.1.24), dispositivo, práctica u otras condiciones y/o acciones que mantengan y/o modifiquen el riesgo.

Nota 2 a la entrada: Es posible que los controles no siempre ejerzan el efecto modificador previsto o supuesto.

[FUENTE: NMX-SAST-31000-IMNC-2018, inciso 3.8]

3.1.9 Ruptura

Incidente, ya sea anticipado o imprevisto, que cause una desviación negativa no planificada de la entrega esperada de productos y servicios de acuerdo con los objetivos de una organización.

[FUENTE: La NMX-I-22301-NYCE-2021, inciso 3.10]

3.1.10 Dispositivo de punto final

Dispositivo de hardware de tecnología de la información y la comunicación (TIC) conectado a la red

Nota 1 a la entrada: El dispositivo de punto final puede referirse a computadoras de escritorio, computadoras portátiles, teléfonos inteligentes, tabletas, clientes ligeros, impresoras u otro hardware especializado, incluidos medidores inteligentes y dispositivos de Internet de las cosas (IoT).

3.1.11 Entidad

Elemento relevante a los efectos del funcionamiento de un dominio que tiene una existencia reconociblemente distinta.

Nota 1 a la entrada: Una entidad puede tener una realización física o lógica.

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

EJEMPLO Una persona, una organización, un dispositivo, un grupo de tales artículos, un suscriptor humano a un servicio de telecomunicaciones, una tarjeta SIM, un pasaporte, una tarjeta de interfaz de red, una aplicación de software, un servicio o un sitio web.

[FUENTE: La norma que se indica en el inciso 10.17, inciso 3.1.1]

3.1.12 Instalación de procesamiento de información

Cualquier sistema, servicio o infraestructura de procesamiento de información, o la ubicación física que lo alberga.

[FUENTE: La NMX-I-27000-NYCE-2019, inciso 3.27, modificada — "instalaciones" ha sido reemplazada por instalación.]

3.1.13 Violación de la seguridad de la información

Compromiso de la seguridad de la información que conduce a la destrucción, pérdida, alteración, divulgación o acceso no deseados a la información protegida transmitida, almacenada o procesada de otra manera.

3.1.14 Evento de seguridad de la información

Ocurrencia que indique una posible violación de la seguridad de la información (3.1.13) o una falla de los controles (3.1.8).

[FUENTE: La norma que se indica en el inciso 10.26, 3.3, modificada - "violación de la seguridad de la información" ha sido reemplazada por "violación de la seguridad de la información"].

3.1.15 Incidente de seguridad de la información

Uno o varios eventos de seguridad de la información relacionados e identificados (3.1.14) que pueden dañar los activos de una organización (3.1.2) o comprometer sus operaciones.

[FUENTE: La norma que se indica en el inciso 10.26, 3.4].

3.1.16 Gestión de incidentes de seguridad de la información

Ejercicio de un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información (3.1.15).

[FUENTE: La norma que se indica en el inciso 10.26, 3.5].

3.1.17 Sistema de información

Conjunto de aplicaciones, servicios, activos de tecnología de la información (3.1.2) u otros componentes de tratamiento de la información.

[FUENTE: La NMX-I-27000-NYCE-2019, inciso 3.35].

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

3.1.18 Parte interesada

Interesado
Persona u organización que puede afectar, ser afectada por, o percibirse a sí misma como afectada por una decisión o actividad

[FUENTE: La NMX-I-27000-NYCE-2019, inciso 3.37].

3.1.19 No repudio

Capacidad para probar la ocurrencia de un evento o acción reclamada y sus entidades de origen (3.1.11).

3.1.20 Personal

Personas que trabajan bajo la dirección de la organización

Nota 1 a la entrada: El concepto de personal incluye a los miembros de la organización, como el órgano de gobierno, la alta dirección, los empleados, el personal temporal, los contratistas y los voluntarios.

3.1.21 Información de identificación personal (PII)

Cualquier información que (a) pueda utilizarse para establecer un vínculo entre la información y la persona física a la que se refiere dicha información, o (b) esté o pueda estar directa o indirectamente vinculada a una persona física.

Nota 1 a la entrada: La "persona física" en la definición es el principal de PII (3.1.22). Para determinar si un principal de PII es identificable, se recomienda tener en cuenta todos los medios que puedan ser utilizados razonablemente por la parte interesada en la privacidad que posee los datos, o por cualquier otra parte, para establecer el vínculo entre el conjunto de PII y la persona física.

[FUENTE: La norma que se indica en el inciso 10.31, inciso 2.9]

3.1.22 Principal de PII

Persona física a la que se refiere la información de identificación personal (PII) (3.1.21).

Nota 1 a la entrada: Dependiendo de la jurisdicción y la legislación particular de protección de datos y privacidad, también se puede usar el sinónimo "sujeto de datos" en lugar del término "principal de PII".

[FUENTE: La norma que se indica en el inciso 10.31, inciso 2.11]

3.1.23 Procesador de PII

Parte interesada de privacidad que procesa información de identificación personal (PII) (3.1.21) en nombre y de acuerdo con las instrucciones de un controlador de PII.

[FUENTE: La norma que se indica en el inciso 10.31, inciso 2.12]

3.1.24 Política

Intenciones y dirección de una organización, según lo expresado formalmente por su alta dirección

[FUENTE: La NMX-I-27000-NYCE-2019, inciso 3.53].

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

3.1.25 Evaluación de impacto sobre la privacidad

Proceso general (3.1.27) de identificación, análisis, evaluación, consultoría, comunicación y planificación del tratamiento de los posibles impactos en la privacidad con respecto al procesamiento de información de identificación personal (PII) (3.1.21), enmarcado dentro del marco más amplio de gestión de riesgos de una organización.

[FUENTE: La norma que se indica en el inciso 10.33, inciso 3.7, modificada — Nota 1 a la entrada eliminada.]

3.1.26 Procedimiento

Forma especificada de llevar a cabo una actividad o un proceso (3.1.27).

[FUENTE: La norma que se indica en el inciso 10.36, inciso 3.12]

3.1.27 Proceso

Conjunto de actividades interrelacionadas o que interactúan que utilizan o transforman entradas para entregar un resultado

[FUENTE: La NMX-CC-9000-IMNC-2015, 3.4.1, modificada— Notas a la entrada eliminadas.]

3.1.28 Grabar

Información creada, recibida y mantenida como prueba y como activo (3.1.2) por una organización o persona, en cumplimiento de obligaciones legales o en la transacción de negocios.

Nota 1 a la entrada: Las obligaciones legales en este contexto incluyen todos los requisitos legales, legales, reglamentarios y contractuales.

[FUENTE: La norma que se indica en el inciso 10.3, inciso 3.14, modificada— "Nota 1 a la entrada" añadida.]

3.1.29 Objetivo de punto de recuperación RPO

Punto en el tiempo en el que se van a recuperar los datos después de que se haya producido una interrupción (3.1.9).

[FUENTE: La NMX-I-27031-NYCE-2019, inciso 3.12, modificada — "debería" sustituido por "deberían ser".]

3.1.30 Objetivo de tiempo de recuperación RTO

Período de tiempo dentro del cual los niveles mínimos de servicios y/o productos y los sistemas o aplicaciones de soporte o funciones, sean recuperados después de que se haya producido una interrupción (3.1.9).

[FUENTE: La NMX-I-27031-NYCE-2019, INCISO 3.13, modificada — "debería" sustituido por "deberían ser".]

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

3.1.31 Fiabilidad

Propiedad del comportamiento y los resultados previstos coherentes.

3.1.32 Regla

Principio o instrucción aceptada que establece las expectativas de la organización sobre lo que se requiere hacer, lo que está permitido o no permitido.

Nota 1 a la entrada: Las reglas pueden expresarse formalmente en políticas específicas del tema (3.1.35) y en otros tipos de documentos.

3.1.33 Información confidencial

Se recomienda que la información que se proteja de la falta de disponibilidad, el acceso no autorizado, la modificación o la divulgación pública debido a posibles efectos adversos en un individuo, organización, seguridad nacional o seguridad pública.

3.1.34 Amenaza

Causa potencial de un incidente no deseado, que puede resultar en daños a un sistema u organización.

[FUENTE: La NMX-I-27000-NYCE-2019, inciso 3.74]

3.1.35 Directiva específica del tema

Intenciones y dirección sobre un tema o tema específico, según lo expresado formalmente por el nivel apropiado de gestión.

Nota 1 a la entrada: Las directivas específicas de cada tema pueden expresar formalmente reglas (3.1.32) o estándares de organización.

Nota 2 a la entrada: Algunas organizaciones utilizan otros términos para estas directivas específicas del tema.

Nota 3 a la entrada: Las directivas específicas del tema a las que se hace referencia en este Proyecto de Norma Mexicana están relacionadas con la seguridad de la información.

EJEMPLO Política específica del tema sobre control de acceso (3.1.1), política específica del tema en escritorio y pantalla limpios.

3.1.36 Usuario

Parte interesada (3.1.18) con acceso a los sistemas de información de la organización (3.1.17).

EJEMPLO Personal (3.1.20), clientes, proveedores.

3.1.37 Dispositivo de punto final de usuario

Dispositivo de punto final (3.1.10) utilizado por los usuarios para acceder a los servicios de procesamiento de información.

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

Nota 1 a la entrada: El dispositivo de punto final del usuario puede referirse a computadoras de escritorio, computadoras portátiles, teléfonos inteligentes, tabletas, clientes ligeros, etc.

3.1.38 Vulnerabilidad

Debilidad de un activo (3.1.2) o control (3.1.8) que puede ser explotado por una o más amenazas (3.1.34).

[FUENTE: La NMX-I-27000-NYCE-2019, inciso 3.77].

3.2 Términos abreviados

ABAC – Control de acceso basado en atributos
ACL – Lista de control de acceso
BIA – Análisis de impacto en el negocio
BYOD – Trae tu propio dispositivo
CAPTCHA – Prueba de Turing pública completamente automatizada para diferenciar computadoras y humanos
CPU – Unidad central de procesamiento
DAC – Control de acceso discrecional
DNS – Sistema de nombres de dominio
GPS – Sistema de posicionamiento global
IAM – Gestión de identidades y accesos
TIC – Tecnologías de la información y comunicaciones
ID – Identificador
IDE – Entorno de desarrollo integrado
IDS – Sistema de detección de intrusos
IoT – Internet de las cosas
IP – Protocolo de internet
IPS – Sistema de prevención de intrusiones
IT – Tecnologías de la información
ISMS – Sistema de gestión de seguridad de la información
MAC – Control de acceso obligatorio
NTP – Protocolo de tiempo de red
PIA – Evaluación de impacto sobre la privacidad
PII – Información de identificación personal
PIN – Número de identificación personal
PKI – Infraestructura de clave pública
PTP – Protocolo de tiempo de precisión
RBAC – Control de acceso basado en roles
RPO – Objetivo del punto de recuperación
RTO – Objetivo de tiempo de recuperación
SAST – Pruebas de seguridad de aplicaciones estáticas
SD – Digital seguro
SDN – Redes definidas por software
SD-WAN – Redes de área amplia definidas por software
SIEM – Seguridad de la información y gestión de eventos
SMS – Servicio de mensajes cortos
SQL – Lenguaje de consulta estructurado
SSO – Inicio de sesión único
SWID – Identificación de software
UEBA – Análisis del comportamiento de usuarios y entidades
UPS – Fuente de alimentación ininterrumpida

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

URL – Localizador uniforme de recursos
USB – Bus serie universal
VM – Máquina virtual
VPN – Red privada virtual
WIFI – Fidelidad inalámbrica

4 Estructura de este Proyecto de Norma Mexicana

4.1 Capítulos

Este Proyecto de Norma Mexicana está estructurado de la siguiente manera:

a) controles organizativos (Capítulo 5),

b) controles de personas (Capítulo 6),

c) controles físicos (Capítulo 7),

d) controles tecnológicos (Capítulo 8).

Hay 2 apéndices informativos:

- Apéndice A — Uso de atributos.
- Apéndice B — Correspondencia con la NMX-I-27002-NYCE-2015.

En el apéndice A se explica cómo una organización puede utilizar atributos (ver el inciso 4.2) para crear sus propias vistas basadas en los atributos de control definidos en este Proyecto de Norma Mexicana o en su propia creación.

El apéndice B muestra la correspondencia entre los controles de esta edición de la NMX-I-27002-NYCE y la edición anterior.

4.2 Temas y atributos

La categorización de los controles dada en los capítulos 5 al 8 se denominan temas.

Los controles se clasifican en:

a) personas, si se refieren a personas individuales;

b) físicos, si se refieren a objetos físicos;

c) tecnológicos, si se refieren a la tecnología;

d) de lo contrario, se clasifican como organizativos.

La organización puede usar atributos para crear diferentes vistas que son diferentes categorizaciones de controles vistos desde una perspectiva diferente a los temas. Los atributos se pueden usar para filtrar, ordenar o presentar controles en diferentes vistas para diferentes audiencias. En el apéndice A se explica cómo se puede lograr esto y se ofrece un ejemplo de una opinión.

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

A modo de ejemplo, cada control de este Proyecto de Norma Mexicana se ha asociado a cinco atributos con los valores de atributo correspondencia (precedidos por "#" para que se puedan buscar), de la siguiente manera:

a) Tipo de control

El tipo de control es un atributo para ver los controles desde la perspectiva de cuándo y cómo el control modifica el riesgo con respecto a la ocurrencia de un incidente de seguridad de la información. Los valores de atributo consisten en preventivo (el control que está destinado a prevenir la ocurrencia de un incidente de seguridad de la información), Detectivo (el control actúa cuando ocurre un incidente de seguridad de la información) y Correctivo (el control actúa después de que ocurre un incidente de seguridad de la información).

b) Propiedades de seguridad de la información

Las propiedades de seguridad de la información son un atributo para ver los controles desde la perspectiva de qué característica de la información el control contribuye a preservar. Los valores de atributo consisten en Confidencialidad, Integridad y Disponibilidad.

c) Conceptos de ciberseguridad

Los conceptos de ciberseguridad son un atributo para ver los controles desde la perspectiva de la asociación de controles a los conceptos de ciberseguridad definidos en el marco de ciberseguridad descrito en la norma que se indica en el inciso 10.30. Los valores de atributo consisten en Identificar, Proteger, Detectar, Responder y Recuperar.

d) Capacidades operativas

Las capacidades operativas son un atributo para ver los controles desde la perspectiva del profesional de las capacidades de seguridad de la información. Los valores de atributo consisten en Gobernanza, Gestión_de_activos, Protección_de_la_información, Seguridad_de_los_recursos_humanos, Seguridad_física, Seguridad_de_sistemas_y_redes, Seguridad_de_aplicaciones, Configuración_segura, Identidad_y_control_de_acceso, Amenazas_y_gestión_de_vulnerabilidades, Continuidad, Seguridad_en_la_relación_con_proveedores, Cumplimiento_y_legal, Gestión_de_eventos_de_seguridad_de_la_información y Aseguramiento_de_seguridad_de_la_información.

e) Dominios de seguridad

Los dominios de seguridad son un atributo para ver los controles desde la perspectiva de cuatro dominios de seguridad de la información: "Gobernanza y ecosistema" incluye "Gobernanza de seguridad del sistema de información y gestión de riesgos" y "Gestión de la ciberseguridad del ecosistema" (incluidas las partes interesadas internas y externas); "Protección" incluye "Arquitectura de seguridad de TI", "Administración de seguridad de TI", "Gestión de identidad y acceso", "Mantenimiento de seguridad de TI" y "Seguridad física y ambiental"; "Defensa" incluye "Detección" y "Gestión de incidentes de seguridad informática"; "Resiliencia" incluye "Continuidad de las operaciones" y "Gestión de crisis". Los valores de atributo consisten en Gobernabilidad_y_Ecosistema, Protección, Defensa y Resiliencia.

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

Los atributos dados en este Proyecto de Norma Mexicana se seleccionan porque se consideran lo suficientemente genéricos como para ser utilizados por diferentes tipos de organizaciones. Las organizaciones pueden optar por ignorar uno o más de los atributos dados en este Proyecto de Norma Mexicana. También pueden crear atributos propios (con los valores de atributo correspondientes) para crear sus propias vistas organizativas. El inciso A.2 incluye ejemplos de tales atributos.

4.3 Diseño de control

El diseño de cada control contiene lo siguiente:

- **Título del control:** nombre corto del control.
- **Tabla de atributos:** una tabla muestra los valores de cada atributo para el control dado.
- **Control:** qué es el control.
- **Finalidad:** por qué se recomienda implementar el control.
- **Orientación:** cómo se recomienda implementar el control;
- **Otros datos:** texto explicativo o referencias a otros documentos relacionados.

Se utilizan los subtítulos en el texto de orientación para algunos controles para facilitar la legibilidad cuando la orientación es larga y aborda varios temas. Estos encabezamientos no se utilizan necesariamente en todos los textos de orientación. Se subrayan los subtítulos.

5 Controles organizativos

5.1 políticas de seguridad de la información

Tipo de control	Propiedades de Seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Identificar	#Gobernabilidad	#Gobernabilidad_y_Ecosistema #Resiliencia

Control

Se recomienda que la política de seguridad de la información y las políticas específicas del tema sean definidas, aprobadas por la administración, publicadas, comunicadas y reconocidas por el personal pertinente y las partes interesadas pertinentes, y revisadas a intervalos planificados y si se producen cambios significativos.

Propósito

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

Garantizar la idoneidad continua, la adecuación, la eficacia de la dirección de gestión y el apoyo a la seguridad de la información de acuerdo con los requisitos comerciales, legales, estatutarios, reglamentarios y contractuales.

Orientación

Al más alto nivel, se recomienda que la organización defina una "política de seguridad de la información" que sea aprobada por la alta gerencia y que establezca el enfoque de la organización para administrar su seguridad de la información.

Es conveniente que la política de seguridad de la información tenga en cuenta los requisitos derivados de:

a) estrategia y requisitos empresariales;

b) reglamentos, legislación y contratos;

c) los riesgos y amenazas actuales y proyectados para la seguridad de la información.

Se recomienda que la política de seguridad de la información contenga declaraciones relativas a:

a) definición de seguridad de la información;

b) los objetivos de seguridad de la información o el marco para establecer objetivos de seguridad de la información;

c) principios para orientar todas las actividades relacionadas con la seguridad de la información;

d) compromiso de satisfacer los requisitos aplicables relacionados con la seguridad de la información;

e) compromiso con la mejora continua del sistema de gestión de la seguridad de la información;

f) asignación de responsabilidades para la gestión de la seguridad de la información a funciones definidas;

g) procedimientos para tramitar exenciones y excepciones.

Se recomienda que la alta dirección apruebe cualquier cambio en la política de seguridad de la información.

En un nivel inferior, es conveniente que la política de seguridad de la información este respaldada por políticas temáticas específicas según sea necesario, para exigir aún más la implementación de controles de seguridad de la información. Las políticas específicas de cada tema suelen estar estructuradas para abordar las necesidades de ciertos grupos objetivo dentro de una organización o para cubrir ciertas áreas de seguridad. Es conveniente que las políticas específicas de cada tema estén alineadas y ser complementarias a la política de seguridad de la información de la organización.

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

Ejemplos de tales temas incluyen:

a) control de acceso;

b) seguridad física y medioambiental;

c) gestión de activos;

d) transferencia de información;

e) configuración y manipulación seguras de los dispositivos de punto final del usuario;

f) seguridad de las redes;

g) gestión de incidentes de seguridad de la información;

h) copia de seguridad;

i) criptografía y gestión de claves;

j) clasificación y manipulación de la información;

k) gestión de vulnerabilidades técnicas;

l) desarrollo seguro.

Se recomienda que la responsabilidad de la elaboración, revisión y aprobación de las políticas relativas a temas específicos se asignen al personal pertinente en función de su nivel apropiado de autoridad y competencia técnica. Se recomienda que la revisión incluya la evaluación de oportunidades de mejora de la política de seguridad de la información de la organización y las políticas específicas del tema y la gestión de la seguridad de la información en respuesta a los cambios para:

a) la estrategia empresarial de la organización;

b) el entorno técnico de la organización;

c) reglamentos, estatutos, legislación y contratos;

d) riesgos para la seguridad de la información;

e) el entorno actual y proyectado de amenazas a la seguridad de la información;

f) lecciones aprendidas de eventos e incidentes de seguridad de la información.

Se recomienda que la revisión de la política de seguridad de la información y las políticas temáticas específicas tengan en cuenta los resultados de las revisiones y auditorías de la administración. Se recomienda considerar la revisión y actualización de otras políticas relacionadas cuando se cambia una política para mantener la coherencia.

Es conveniente que la política de seguridad de la información y las políticas temáticas específicas se comuniquen al personal pertinente y a las partes interesadas en una forma

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

que sea pertinente, accesible y comprensible para el lector previsto. Se recomienda exigir a los destinatarios de las políticas que reconozcan que entienden y aceptan cumplir con las políticas cuando corresponda. La organización puede determinar los formatos y nombres de estos documentos de directiva que satisfagan las necesidades de la organización. En algunas organizaciones, la directiva de seguridad de la información y las directivas específicas del tema pueden estar en un solo documento. La organización puede nombrar estas políticas específicas del tema como estándares, directivas, políticas u otras.

Si la política de seguridad de la información o cualquier política específica del tema se distribuye fuera de la organización, se recomienda tener cuidado de no divulgar indebidamente información confidencial.

La Tabla 1 ilustra las diferencias entre la política de seguridad de la información y la política de temas específicos.

Tabla 1 - Diferencias entre la política de seguridad de la información y la política de temas específicos

	Política de seguridad de la información	**Política específica del tema**
Nivel de detalle	General o de alto nivel	Específico y detallado
Documentado y aprobado formalmente por	Alta dirección	Nivel adecuado de gestión

Otros datos

Las directivas específicas de cada tema pueden variar de una organización a otra.

5.2 Funciones y responsabilidades de seguridad de la información

Tipo de control	**Propiedades de Seguridad de la información**	**Conceptos de ciberseguridad**	**Capacidades operativas**	**Dominios de seguridad**
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Identificar	#Gobernabilidad	#Gobernabilidad_y_Ecosistema #Protección #Resiliencia

Control

Es conveniente que las funciones y responsabilidades de seguridad de la información sean definidas y asignadas de acuerdo con las necesidades de la organización.

Propósito

Establecer una estructura definida, aprobada y entendida para la implementación, operación y gestión de la seguridad de la información dentro de la organización.

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

Orientación

Se recomienda que la asignación de funciones y responsabilidades de seguridad de la información se haga de acuerdo con la política de seguridad de la información y las políticas específicas del tema (ver inciso 5.1). Se recomienda que la organización defina y gestione las responsabilidades de:

a) protección de la información y otros activos asociados;

b) llevar a cabo procesos específicos de seguridad de la información;

c) actividades de gestión de riesgos para la seguridad de la información y, en particular, aceptación de riesgos residuales (por ejemplo, para los propietarios de riesgos);

d) todo el personal que utilice la información de una organización y otros activos asociados.

Se recomienda que las responsabilidades se complementen, cuando sea necesario, con una orientación más detallada para sitios específicos e instalaciones de procesamiento de información. Las personas con responsabilidades de seguridad de la información asignadas pueden asignar tareas de seguridad a otros. Sin embargo, se recomienda que sigan siendo responsables y determinen que las tareas delegadas se han realizado correctamente.

Se recomienda que cada área de seguridad de la que son responsables las personas sea definida, documentada y comunicada. Es conveniente que los niveles de autorización se definan y documenten. Se sugiere que las personas que asuman una función específica de seguridad de la información sean competentes en cuanto a los conocimientos y habilidades requeridos por la función y se recomienda reciban apoyo para mantenerse al día con los desarrollos relacionados con la función y necesarias para cumplir con las responsabilidades de la función.

Otros datos

Muchas organizaciones designan a un gerente de seguridad de la información para que asuma la responsabilidad general del desarrollo y la implementación de la seguridad de la información y para apoyar la identificación de riesgos y los controles de mitigación.

Sin embargo, la responsabilidad de los recursos y la implementación de los controles a menudo recae en los gerentes individuales. Una práctica común es nombrar un propietario para cada activo que luego se convierte en responsable de su protección diaria.

Dependiendo del tamaño y los recursos de una organización, la seguridad de la información puede estar cubierta por roles o tareas dedicadas llevadas a cabo además de los roles existentes.

5.3 Segregación de funciones

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

Tipo de control	Propiedades de Seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Gobernanza #Identidad_y_control_de_acceso	#Gobernabilidad_y_Ecosistema

Control

Se recomienda segregarse los deberes contradictorios y las esferas de responsabilidad en conflicto.

Propósito

Reducir el riesgo de fraude, error y elusión de los controles de seguridad de la información.

Orientación

La segregación de deberes y áreas de responsabilidad tiene como objetivo separar los deberes en conflicto entre diferentes individuos para evitar que un individuo ejecute posibles deberes conflictivos por su cuenta.

Se recomienda que la organización determine qué deberes y áreas de responsabilidad se sugiere sean segregados. Los siguientes son ejemplos de actividades que pueden requerir segregación:

a) iniciar, aprobar y ejecutar un cambio;

b) solicitar, aprobar y aplicar los derechos de acceso;

c) diseñar, aplicar y revisar el código;

d) desarrollar programas informáticos y administrar sistemas de producción;

e) utilizar y administrar aplicaciones;

f) el uso de aplicaciones y la administración de bases de datos;

g) diseñar, auditar y garantizar los controles de seguridad de la información.

Se recomienda que la posibilidad de colusión se tenga en cuenta al diseñar los controles de segregación. Las organizaciones pequeñas pueden encontrar difícil lograr la segregación de funciones, se sugiere el principio se aplique en la medida de lo posible y factible. Siempre que sea difícil segregar, se sugiere se consideren otros controles, como el seguimiento de las actividades, los registros de auditoría y la supervisión de la gestión.

Se recomienda tener cuidado al utilizar sistemas de control de acceso basados en roles para garantizar que a las personas no se les otorguen roles conflictivos. Cuando hay un gran número de roles, se sugiere que la organización considere el uso de herramientas automatizadas para identificar conflictos y facilitar su eliminación. Se recomienda que

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

los roles se definan y asignen cuidadosamente para minimizar los problemas de acceso si se quita o reasigna un rol.

Otros datos

No hay otra información.

5.4 Responsabilidades de gestión

Tipo de control	Propiedades de Seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Identificar	#Gobernabilidad	#Gobernabilidad_y_Ecosistema

Control

Se sugiere que la administración requiera que todo el personal aplique la seguridad de la información de acuerdo con la política de seguridad de la información establecida, las políticas y procedimientos específicos del tema de la organización.

Propósito

Garantizar que la administración comprenda su papel en la seguridad de la información y emprenda acciones destinadas a garantizar que todo el personal conozca y cumpla con sus responsabilidades de seguridad de la información.

Orientación

Se recomienda que la administración demuestre el apoyo a la política de seguridad de la información, las políticas específicas del tema, los procedimientos y los controles de seguridad de la información.

Se recomienda que las responsabilidades de gestión incluyan garantizar que el personal:

a) estén debidamente informados sobre sus funciones y responsabilidades en materia de seguridad de la información antes de que se les conceda acceso a la información de la organización y otros activos asociados;

b) se les proporcionan directrices que establecen las expectativas de seguridad de la información de su papel dentro de la organización;

c) tienen el mandato de cumplir la política de seguridad de la información y las políticas temáticas específicas de la organización;

d) lograr un nivel de conciencia de la seguridad de la información pertinente para sus funciones y responsabilidades dentro de la organización (ver el inciso 6.3);

e) el cumplimiento de los términos y condiciones de empleo, contrato o acuerdo, incluida la política de seguridad de la información de la organización y los métodos de trabajo apropiados;

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

f) seguir teniendo las competencias y cualificaciones adecuadas en materia de seguridad de la información a través de una formación profesional continua;

g) cuando sea posible, se les proporciona un canal confidencial para denunciar violaciones de la política de seguridad de la información, políticas temáticas específicas o procedimientos para la seguridad de la información ("denuncia de irregularidades"). Esto puede permitir la denuncia anónima, o tener disposiciones para garantizar que el conocimiento de la identidad del denunciante sea conocida solo por aquellos que necesitan lidiar con tales informes;

h) se les proporcionan los recursos adecuados y el tiempo de planificación del proyecto para implementar los procesos y controles relacionados con la seguridad de la organización.

Otros datos

No hay otra información.

5.5 Contacto con las autoridades

Tipo de control	Propiedades de Seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Identificar #Proteger #Responder #Recuperación	#Gobernabilidad	#Defensa #Resiliencia

Control

Se recomienda que la organización establezca y mantenga contacto con las autoridades pertinentes.

Propósito

Garantizar que se produzca un flujo adecuado de información con respecto a la seguridad de la información entre la organización y las autoridades legales, reglamentarias y de supervisión pertinentes.

Orientación

Se recomienda que la organización especifique cuándo y por quién se sugiere poner en contacto con las autoridades (por ejemplo, las fuerzas del orden, los organismos reguladores, las autoridades de supervisión) y cómo es conveniente informar oportunamente los incidentes de seguridad de la información identificados.

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

Se recomienda que los contactos con las autoridades también se utilicen para facilitar la comprensión de las expectativas actuales y futuras de estas autoridades (por ejemplo, las normas de seguridad de la información aplicables).

Otros datos

Las organizaciones atacadas pueden solicitar a las autoridades que tomen medidas contra la fuente del ataque.

El mantenimiento de estos contactos puede ser un requisito para apoyar la gestión de incidentes de seguridad de la información (ver el subinciso 5.24 al subinciso 5.28) o los procesos de planificación de contingencias y continuidad del negocio (ver el subinciso 5.29 y el subinciso 5.30). Los contactos con los organismos reguladores también son útiles para anticipar y prepararse para los próximos cambios en las leyes o regulaciones relevantes que afectan a la organización. Los contactos con otras autoridades incluyen servicios públicos, servicios de emergencia, proveedores de electricidad y salud y seguridad [por ejemplo, departamentos de bomberos (en relación con la continuidad de las actividades), proveedores de telecomunicaciones (en relación con el enrutamiento y la disponibilidad de líneas) y proveedores de agua (en relación con las instalaciones de refrigeración para equipos)].

5.6 Contacto con grupos de interés especial

Tipo de control	Propiedades de Seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo #Correctivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger #Responder #Recuperar	#Gobernabilidad	#Defensa

Control

Se recomienda que la organización establezca y mantenga contacto con grupos de interés especial u otros foros especializados en seguridad y asociaciones profesionales.

Propósito

Garantizar que el flujo adecuado de información tenga lugar con respecto a la seguridad de la información.

Orientación

Se recomienda que la pertenencia a grupos o foros de interés especial se consideren como un medio para:

a) mejorar el conocimiento sobre las mejores prácticas y mantenerse al día con la información de seguridad pertinente;

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

b) garantizar que la comprensión del entorno de seguridad de la información sea actual;

c) recibir alertas tempranas de alertas, avisos y parches relacionados con ataques y vulnerabilidades;

d) obtener acceso a asesoramiento especializado en seguridad de la información;

e) compartir e intercambiar información sobre nuevas tecnologías, productos, servicios, amenazas o vulnerabilidades;

f) proporcionar puntos de enlace adecuados cuando se trate de incidentes de seguridad de la información (ver el subinciso 5.24 al subinciso 5.28).

Otros datos

No hay otra información.

5.7 Inteligencia de amenazas

Tipo de control	Propiedades de Seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo #Detectivo #Correctivo	#Confidencialidad #Integridad #Disponibilidad	#Identificar #Detectar #Responder	#Amenazas_y_gestión_de_vulnerabilidades	#Defensa #Resiliencia

Control

Se recomienda que la información relacionada con las amenazas a la seguridad de la información se recopile y analice para producir inteligencia sobre amenazas.

Propósito

Proporcionar conciencia sobre el entorno de amenazas de la organización para que se puedan tomar las medidas de mitigación apropiadas.

Orientación

La información sobre las amenazas existentes o emergentes se recopila y analiza con el fin de:

a) facilitar acciones informadas para evitar que las amenazas causen daño a la organización;

b) reducir el impacto de tales amenazas.

Se recomienda que la inteligencia de amenazas se puede dividir en tres capas, que considere:

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

a) inteligencia estratégica sobre amenazas: intercambio de información de alto nivel sobre el cambiante panorama de amenazas (por ejemplo, tipos de atacantes o tipos de ataques);

b) inteligencia táctica de amenazas: información sobre las metodologías, herramientas y tecnologías de los atacantes implicados;

c) inteligencia operativa sobre amenazas: detalles sobre ataques específicos, incluidos indicadores técnicos.

Se recomienda que la inteligencia de amenazas sea:

a) pertinente (es decir, relacionado con la protección de la organización);

b) perspicaz (es decir, proporcionar a la organización una comprensión precisa y detallada del panorama de amenazas);

c) contextual, para proporcionar conciencia situacional (es decir, agregar contexto a la información basada en el momento de los eventos, dónde ocurren, experiencias previas y prevalencia en organizaciones similares);
d) accionable (es decir, la organización puede actuar sobre la información de forma rápida y eficaz).

Se recomienda que las actividades de inteligencia de amenazas incluyan:

a) establecer objetivos para la producción de inteligencia sobre amenazas;

b) identificar, examinar y seleccionar las fuentes de información internas y externas que sean necesarias y apropiadas para proporcionar la información necesaria para la producción de inteligencia sobre amenazas;

c) recopilar información de fuentes seleccionadas, que pueden ser internas y externas;

d) procesar la información recopilada para prepararla para el análisis (por ejemplo, traduciendo, formateando o corroborando información);

e) analizar la información para comprender cómo se relaciona y es significativa para la organización;

f) comunicarlo y compartirlo con las personas pertinentes en un formato que pueda entenderse.

Se recomienda que la inteligencia de amenazas analice y utilice posteriormente:

a) mediante la implementación de procesos para incluir la información recopilada de fuentes de inteligencia de amenazas en los procesos de gestión de riesgos de seguridad de la información de la organización;

b) como entrada adicional a los controles técnicos preventivos y de detección como firewalls, sistemas de detección de intrusos o soluciones antimalware;

c) como entrada a los procesos y técnicas de prueba de seguridad de la información.

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

Se recomienda que la organización comparta la inteligencia de amenazas con otras organizaciones de forma mutua para mejorar la inteligencia general de amenazas.

Otros datos

Las organizaciones pueden usar la inteligencia de amenazas para prevenir, Detectar o Responder a las amenazas. Las organizaciones pueden producir inteligencia de amenazas, pero más típicamente reciben y hacen uso de la inteligencia de amenazas producida por otras fuentes.

La inteligencia de amenazas a menudo es proporcionada por proveedores o asesores independientes, agencias gubernamentales o grupos colaborativos de inteligencia de amenazas.

La efectividad de controles como el subinciso 5.25, el inciso 8.7, el inciso 8.16 u el inciso 8.23, depende de la calidad de la inteligencia de amenazas disponible.

5.8 Seguridad de la información en la gestión de proyectos

Tipo de control	Propiedades de Seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Identificar #Proteger	#Gobernabilidad	#Gobernabilidad_y_Ecosistema #Protección

Control

Se recomienda que la seguridad de la información se integre en la gestión de proyectos.

Propósito

Garantizar que los riesgos de seguridad de la información relacionados con los proyectos y entregables se aborden de manera efectiva en la gestión de proyectos a lo largo del ciclo de vida del proyecto.

Orientación

Se recomienda que la seguridad de la información se integre en la gestión de proyectos para garantizar que los riesgos de seguridad de la información se aborden como parte de la gestión del proyecto. Esto se puede aplicar a cualquier tipo de proyecto independientemente de su complejidad, tamaño, duración, disciplina o área de aplicación (por ejemplo, un proyecto para un proceso de negocio central, TIC, gestión de instalaciones u otros procesos de apoyo).

Se recomienda que la gestión del proyecto en uso requiera que:

a) los riesgos para la seguridad de la información se evalúan y tratan en una fase temprana y periódicamente como parte de los riesgos del proyecto a lo largo del ciclo de vida del proyecto;

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

b) los requisitos de seguridad de la información [por ejemplo, los requisitos de seguridad de las aplicaciones (ver inciso 8.26), los requisitos para cumplir los derechos de propiedad intelectual (ver inciso 5.32), etc.] se abordan en las primeras etapas de los proyectos;

c) los riesgos de seguridad de la información asociados a la ejecución de proyectos, como la seguridad de los aspectos de comunicación interna y externa, se consideren y traten a lo largo del ciclo de vida del proyecto;

d) se revisa el progreso en el tratamiento del riesgo de seguridad de la información y se evalúa y prueba la efectividad del tratamiento.

Se recomienda que la idoneidad de las consideraciones y actividades de seguridad de la información sea objeto de seguimiento en etapas predefinidas por personas u órganos de gobierno adecuados, como el comité directivo del proyecto.

Se recomienda que las responsabilidades y autoridades para la seguridad de la información relevantes para el proyecto se definan y asignen a roles específicos.

Se recomienda que los requisitos de seguridad de la información para los productos o servicios que entrega el proyecto se determinen utilizando varios métodos, incluido el derivado de los requisitos de cumplimiento de la política de seguridad de la información, las políticas y regulaciones específicas del tema. Otros requisitos de seguridad de la información pueden derivarse de actividades como la modelización de amenazas, las revisiones de incidentes, el uso de umbrales de vulnerabilidad o la planificación de contingencias, asegurando así que la arquitectura y el diseño de los sistemas de información estén protegidos contra amenazas conocidas basadas en el entorno operativo.

Se recomienda que los requisitos de seguridad de la información se determinen para todos los tipos de proyectos, no sólo para los proyectos de desarrollo de las TIC. También se sugiere tener en cuenta lo siguiente al determinar estos requisitos:

a) qué información se trata (determinación de la información), cuáles son las necesidades de seguridad de la información correspondientes (clasificación; ver inciso 5.12) y el posible impacto negativo en el negocio que puede resultar de la falta de seguridad adecuada;

b) las necesidades de protección requeridas de la información y otros activos asociados implicados, en particular en términos de confidencialidad, integridad y disponibilidad;

c) el nivel de confianza o seguridad requerido con respecto a la identidad reivindicada de las entidades para derivar los requisitos de autenticación;

d) los procesos de aprovisionamiento y autorización de acceso, para clientes y otros usuarios empresariales potenciales, así como para usuarios privilegiados o técnicos, como los miembros pertinentes del proyecto, el personal potencial de la operación o los proveedores externos;

e) informar a los usuarios de sus deberes y responsabilidades;

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

f) los requisitos derivados de los procesos empresariales, como el registro y la supervisión de las transacciones, los requisitos de no repudio;

g) requisitos exigidos por otros controles de seguridad de la información (por ejemplo, interfaces para sistemas de registro y seguimiento o detección de fugas de datos);

h) el cumplimiento del entorno legal, estatutario, reglamentario y contractual en el que opera la organización;

i) el nivel de confianza o seguridad requerido para que terceros cumplan con la política de seguridad de la información de la organización y las políticas específicas del tema, incluidos los capítulos de seguridad relevantes en cualquier acuerdo o contrato.

Otros datos

El enfoque de desarrollo del proyecto, como el ciclo de vida en cascada o el ciclo de vida ágil, se recomienda apoyar la seguridad de la información de una manera estructurada que se pueda adaptar para adaptarse a la gravedad evaluada de los riesgos de seguridad de la información, en función del carácter del proyecto. La consideración temprana de los requisitos de seguridad de la información para el producto o servicio (por ejemplo, en las etapas de planificación y diseño) puede conducir a soluciones más efectivas y rentables para la calidad y la seguridad de la información. La norma que se indica en el inciso 10.10 y en el inciso 10.11 proporcionan orientación sobre conceptos y procesos de gestión de proyectos que son importantes para el desempeño de los proyectos.

La NMX-I-27005-NYCE-2019 proporciona orientación sobre el uso de procesos de gestión de riesgos para identificar controles que cumplan con los requisitos de seguridad de la información.

5.9 Inventario de información y otros activos asociados

Tipo de control	Propiedades de Seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Identificar	#Gestión_de_activos	#Gobernabilidad_y_Ecosistema #Protección

Control

Se recomienda elaborar y mantener un inventario de la información y otros activos asociados, incluidos los propietarios.

Propósito

Identificar la información de la organización y otros activos asociados con el fin de preservar su seguridad de la información y asignar la propiedad adecuada.

Orientación

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

Inventario

Se recomienda que la organización identifique su información y otros activos asociados y determinar su importancia en términos de seguridad de la información. Se sugiere que la documentación se mantenga en inventarios dedicados o existentes, según corresponda.

El inventario de información y otros activos asociados se sugiere sean precisos, actualizado, coherente y alineado con otros inventarios. Las opciones para garantizar la exactitud de un inventario de información y otros activos asociados incluyen:

a) la realización de revisiones periódicas de la información identificada y otros activos asociados en relación con el inventario de activos;

b) hacer cumplir automáticamente una actualización de inventario en el proceso de instalación, cambio o eliminación de un activo.

Se recomienda que la ubicación de un activo se incluya en el inventario, según proceda.

El inventario no necesita ser una sola lista de información y otros activos asociados. Se recomienda tener en cuenta que el inventario sea mantenido por las funciones pertinentes, puede verse como un conjunto de inventarios dinámicos, como inventarios de activos de información, hardware, software, máquinas virtuales (VM), instalaciones, personal, competencia, capacidades y registros.

Se recomienda que cada activo sea clasificado de acuerdo con la clasificación de la información (ver el inciso 5.12) asociada a ese activo.

La granularidad del inventario de información y otros activos asociados se sugiere estén en un nivel apropiado para las necesidades de la organización. A veces, no es factible documentar instancias específicas de activos en el ciclo de vida de la información debido a la naturaleza del activo. Un ejemplo de un activo de corta duración es una instancia de máquina virtual cuyo ciclo de vida puede ser de corta duración.

Propiedad

Para la información identificada y otros activos asociados, se sugiere que la propiedad del activo se asigne a un individuo o un grupo y se recomienda que la clasificación se pueda identificar (ver inciso 5.12 y el inciso 5.13). Se recomienda implementar un proceso para garantizar la asignación oportuna de la propiedad de los activos. Se sugiere que la propiedad se asigne cuando se crean activos o cuando los activos se transfieren a la organización. Se recomienda que la propiedad de activos se reasigne según sea necesario cuando los propietarios de activos actuales abandonan o cambian de puesto de trabajo.

Deberes del propietario

Se recomienda que el propietario del activo sea responsable de la gestión adecuada de un activo a lo largo de todo el ciclo de vida del activo, garantizando que:

a) la información y otros activos asociados están inventariados;

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

b) la información y otros activos asociados estén debidamente clasificados y protegidos;

c) la clasificación se revisa periódicamente;

d) los componentes que soportan los activos tecnológicos se enumeran y vinculan, como la base de datos, el almacenamiento, los componentes de software y los subcomponentes;

e) se establezcan requisitos para el uso aceptable de la información y otros activos asociados (ver el inciso 5.10);

f) que las restricciones de acceso se correspondan con la clasificación y que sean eficaces y se revisen periódicamente;

g) la información y otros activos asociados, cuando se eliminan o retiran, se manejan de manera segura y se eliminan del inventario;

h) participen en la identificación y gestión de los riesgos asociados a su(s) activo(s);

i) apoyan al personal que tiene las funciones y responsabilidades de administrar su información.

Otros datos

Los inventarios de información y otros activos asociados a menudo son necesarios para garantizar la protección efectiva de la información y pueden ser necesarios para otros fines, como salud y seguridad, seguros o razones financieras. Los inventarios de información y otros activos asociados también respaldan la gestión de riesgos, las actividades de auditoría, la gestión de vulnerabilidades, la respuesta a incidentes y la planificación de la recuperación.

Las tareas y responsabilidades se pueden delegar (por ejemplo, a un custodio que cuida de los activos a diario), pero la persona o el grupo que los delegó sigue siendo responsable.

Puede ser útil designar grupos de información y otros activos asociados que actúen juntos para proporcionar un servicio en particular. En este caso, el propietario de este servicio es responsable de la prestación del servicio, incluida la operación de sus activos.

Consulte la norma que se indica en el inciso 10.12 para obtener información adicional sobre la gestión de activos de tecnología de la información (TI). Consulte la NMX-J-SAST-55001-ANCE-IMNC-2015 para obtener información adicional sobre la gestión de activos.

5.10 Uso aceptable de la información y otros activos asociados

Tipo de control	Propiedades de Seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad	#Proteger	#Gestión_de_activos#Protección_	#Gobernabilidad_y_Ecosistema #Protección

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

	#Disponibilidad		de_la_información	

Control

Se recomienda identificar, documentar y aplicar normas para el uso aceptable y procedimientos para el tratamiento de la información y otros activos asociados.

Propósito

Para garantizar que la información y otros activos asociados estén adecuadamente protegidos, utilizados y manejados.

Orientación

Se recomienda que el personal y los usuarios externos que utilizan o tienen acceso a la información de la organización y otros activos asociados sean conscientes de los requisitos de seguridad de la información para proteger y manejar la información de la organización y otros activos asociados. Se recomienda sean responsables de su uso de cualquier instalación de procesamiento de información.

Se recomienda que la organización establezca una política temática específica sobre el uso aceptable de la información y otros activos asociados y comunicarla a cualquier persona que use o maneje información y otros activos asociados. Se recomienda que la política sobre el uso aceptable proporcione una dirección clara sobre cómo se espera que las personas utilicen la información y otros activos asociados. Es conveniente que la política específica del tema indique:

a) comportamientos esperados e inaceptables de las personas desde una perspectiva de seguridad de la información;

b) el uso permitido y prohibido de la información y otros activos asociados;

c) supervisar las actividades que realiza la organización.

Se recomienda elaborar procedimientos de uso aceptable para el ciclo de vida completo de la información de acuerdo con su clasificación (ver inciso 5.12) y los riesgos determinados. Se sugiere considerar los siguientes elementos:

a) restricciones de acceso que respalden los requisitos de protección para cada nivel de clasificación;

b) mantenimiento de un registro de los usuarios autorizados de la información y otros activos asociados;

c) la protección de las copias temporales o permanentes de la información a un nivel compatible con la protección de la información original;

d) almacenamiento de activos asociados a la información de conformidad con las especificaciones de los fabricantes (ver inciso 7.8);

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

e) marcado claro de todas las copias de los soportes de almacenamiento (electrónicos o físicos) para la atención del destinatario autorizado (ver inciso 7.10);

f) autorización de enajenación de información y otros activos asociados y método(s) de supresión admitido(s) (ver inciso 8.10).

Otros datos

Puede darse el caso de que los activos en cuestión no pertenezcan directamente a la organización, como los servicios de nube pública. El uso de dichos activos de terceros y cualquier activo de la organización asociado con dichos activos externos (por ejemplo, información, software) se sugiere ser identificados como aplicables y controlados, por ejemplo, a través de acuerdos con proveedores de servicios en la nube. También se sugiere tener cuidado cuando se utiliza un entorno de trabajo colaborativo.

5.11 Devolución de activos

Tipo de control	Propiedades de Seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Gestión_de_activos	#Preventivo

Control

El personal y otras partes interesadas, según corresponda, se sugiere devuelvan todos los activos de la organización en su posesión al cambiar o terminar su empleo, contrato o acuerdo.

Propósito

Para proteger los activos de la organización como parte del proceso de cambio o terminación de empleo, contrato o acuerdo.

Orientación

Se recomienda que el proceso de cambio o terminación se formalice para incluir la devolución de todos los activos físicos y electrónicos emitidos anteriormente propiedad de la organización o confiados a ella.

En los casos en que el personal y otras partes interesadas compren el equipo de la organización o utilicen su propio equipo personal, se sugiere seguir procedimientos para garantizar que toda la información pertinente se rastree y transfiera a la organización y se elimine de forma segura del equipo (ver inciso 7.14).

En los casos en que el personal y otras partes interesadas tienen conocimientos que son importantes para las operaciones en curso, se sugiere que esa información se documente y transfiera a la organización.

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

Durante el período de notificación y posteriormente, se sugiere que la organización evite la copia no autorizada de información relevante (por ejemplo, propiedad intelectual) por parte del personal bajo notificación de terminación.

Se recomienda que la organización identifique y documente claramente toda la información y otros activos asociados que son devueltos, que pueden incluir:

a) dispositivos de punto final de usuario;

b) dispositivos de almacenamiento portátiles;

c) equipo especializado;

d) hardware de autenticación (por ejemplo, claves mecánicas, fichas físicas y tarjetas inteligentes) para sistemas de información, sitios y archivos físicos;

e) copias físicas de la información.

Otros datos

Puede ser difícil devolver la información contenida en activos que no son propiedad de la organización. En tales casos, es necesario restringir el uso de la información utilizando otros controles de seguridad de la información, como la gestión de derechos de acceso (ver inciso 5.18) o el uso de criptografía (ver inciso 8.24).

5.12 Clasificación de la información

Tipo de control	Propiedades de Seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Identificar	#Protección_de_la_información	#Protección#Defensa

Control

Se recomienda que la información se clasifique de acuerdo con las necesidades de seguridad de la información de la organización en función de la confidencialidad, la integridad, la disponibilidad y los requisitos pertinentes de las partes interesadas.

Propósito

Asegurar la identificación y comprensión de las necesidades de protección de la información de acuerdo con su importancia para la organización.

Orientación

Se recomienda que la organización establezca una política temática específica sobre la clasificación de la información y comunicarla a todas las partes interesadas pertinentes.

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

Se recomienda que la organización tenga en cuenta los requisitos de confidencialidad, integridad y disponibilidad en el esquema de clasificación.

Las clasificaciones y los controles de protección asociados de la información se sugiere tengan en cuenta las necesidades de las empresas para compartir o restringir la información, proteger la integridad de la información y garantizar la disponibilidad, así como los requisitos legales relativos a la confidencialidad, integridad o disponibilidad de la información. Los activos que no sean información también se pueden clasificar de conformidad con la clasificación de la información, que se almacena, procesa o maneja o protege de otra manera por el activo.

Se recomienda que los propietarios de la información sean responsables de su clasificación.

Se recomienda que el sistema de clasificación incluya convenios para la clasificación y criterios para la revisión de la clasificación a lo largo del tiempo. Se sugiere que los resultados de la clasificación se actualicen de acuerdo con los cambios en el valor, la sensibilidad y la criticidad de la información a lo largo de su ciclo de vida.

Se recomienda que el esquema este alineado con la política específica del tema sobre control de acceso (ver inciso 5.1) y se sugiere ser capaz de abordar las necesidades comerciales específicas de la organización.

La clasificación puede determinarse por el nivel de impacto que el compromiso de la información tenga para la organización. Se recomienda a cada nivel definido en el régimen se le dé un nombre que tenga sentido en el contexto de la aplicación del sistema de clasificación.

Se recomienda el esquema sea consistente en toda la organización e incluido en sus procedimientos para que todos clasifiquen la información y los otros activos asociados aplicables de la misma manera. De esta manera, todos tienen un entendimiento común de los requisitos de protección y aplican la protección adecuada.

El esquema de clasificación utilizado dentro de la organización puede ser diferente de los esquemas utilizados por otras organizaciones, incluso si los nombres de los niveles son similares. Además, la información que se mueve entre organizaciones puede variar en clasificación dependiendo de su contexto en cada organización, incluso si sus esquemas de clasificación son idénticos. Por lo tanto, los acuerdos con otras organizaciones que incluyan el intercambio de información se sugiere incluyan procedimientos para identificar la clasificación de esa información e interpretar los niveles de clasificación de otras organizaciones. La correspondencia entre los diferentes esquemas puede determinarse buscando la equivalencia en los métodos de manipulación y protección asociados.

Otros datos

La clasificación proporciona a las personas que tratan con información una indicación concisa de cómo manejarla y protegerla. Crear grupos de información con necesidades de protección similares y especificar procedimientos de seguridad de la información que se apliquen a toda la información de cada grupo facilita esto. Este enfoque reduce la necesidad de una evaluación de riesgos caso por caso y un diseño personalizado de los controles.

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

La información puede dejar de ser sensible o crítica después de un cierto período de tiempo. Por ejemplo, cuando la información se ha hecho pública, ya no tiene requisitos de confidencialidad, pero aún puede requerir protección para sus propiedades de integridad y disponibilidad. Se recomienda que estos aspectos se tengan en cuenta, ya que la clasificación excesiva puede dar lugar a la aplicación de controles innecesarios que den lugar a gastos adicionales o, por el contrario, la clasificación insuficiente puede dar lugar a controles insuficientes para proteger la información del compromiso.

A modo de ejemplo, un sistema de clasificación de la confidencialidad de la información puede basarse en cuatro niveles de la siguiente manera:

a) la divulgación no causa ningún daño;

b) la divulgación cause daños menores a la reputación o un impacto operativo menor;

c) la divulgación de información tiene un impacto significativo a corto plazo en las operaciones o en los objetivos empresariales;

d) la divulgación tiene un grave impacto en los objetivos comerciales a largo plazo o pone en riesgo la supervivencia de la organización.

5.13 Etiquetado de a información

Tipo de control	Propiedades de Seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Protección_de_la_información	#Defensa#Protección

Control

Se recomienda elaborar y aplicar un conjunto adecuado de procedimientos para el etiquetado de la información de conformidad con el sistema de clasificación de la información adoptado por la organización.

Propósito

Facilitar la comunicación de la clasificación de la información y apoyar la automatización del procesamiento y la gestión de la información.

Orientación

Se recomienda que los procedimientos de etiquetado de la información abarquen la información y otros activos asociados en todos los formatos. Se sugiere que el etiquetado refleje el sistema de clasificación establecido en el inciso 5.12. Se recomienda que las

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

etiquetas sean fácilmente reconocibles. Se recomienda que los procedimientos proporcionen orientación sobre dónde y cómo se adjuntan las etiquetas teniendo en cuenta cómo se accede a la información o se manejan los activos en función de los tipos de medios de almacenamiento. Los procedimientos pueden definir:

a) los casos en que se omite el etiquetado (por ejemplo, el etiquetado de información no confidencial para reducir la carga de trabajo);

b) cómo etiquetar la información enviada o almacenada en medios electrónicos o físicos, o en cualquier otro formato;

c) cómo gestionar los casos en los que el etiquetado no es posible (por ejemplo, debido a restricciones técnicas).

Ejemplos de técnicas de etiquetado incluyen:

a) etiquetas físicas;

b) encabezados y pies de página;

c) metadatos;

d) marca de agua;

e) sellos de goma.

Se recomienda que la información digital utilice metadatos para identificar, gestionar y controlar la información, especialmente en lo que respecta a la confidencialidad. Se sugiere que los metadatos también permitan una búsqueda eficiente y correcta de información. Los metadatos deberían facilitar que los sistemas interactúen y tomen decisiones basadas en las etiquetas de clasificación asociadas.

Se recomienda que los procedimientos describan cómo adjuntar metadatos a la información, qué etiquetas usar y se sugiere cómo se manejan los datos, en línea con el modelo de información de la organización y la arquitectura de las TIC.

Se recomienda que los sistemas agreguen metadatos adicionales relevantes cuando procesan información en función de sus propiedades de seguridad de la información.

Se recomienda que el personal y otras partes interesadas sean informados de los procedimientos de etiquetado. Se sugiere que todo el personal reciba la formación necesaria para garantizar que la información se etiquete correctamente y se maneje en consecuencia.

Los resultados de los sistemas que contienen información clasificada como sensible o crítica se sugiere lleven una etiqueta de clasificación adecuada.

Otros datos

El etiquetado de la información clasificada es un requisito clave para el intercambio de información.

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

Otros metadatos útiles que se pueden adjuntar a la información es qué proceso organizativo creó la información y en qué momento.

El etiquetado de la información y otros activos asociados a veces puede tener efectos negativos. Los activos clasificados pueden ser más fáciles de identificar por actores maliciosos para un posible uso indebido.

Algunos sistemas no etiquetan archivos individuales o registros de bases de datos con su clasificación, sino que protegen toda la información al más alto nivel de clasificación de cualquiera de la información que contiene o se le permite contener. Es habitual en tales sistemas determinar y luego etiquetar la información cuando se exporta.

5.14 Transferencia de información

Tipo de control	Propiedades de Seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Gestión_de_activos#Protección_de_la_información	#Protección

Control

Se recomienda que las reglas, procedimientos o acuerdos de transferencia de información estén vigentes para todos los tipos de instalaciones de transferencia dentro de la organización y entre la organización y otras partes.

Propósito

Mantener la seguridad de la información transferida dentro de una organización y con cualquier parte interesada externa.

Orientación

General

Se recomienda que la organización establezca y comunique una política temática específica sobre la transferencia de información a todas las partes interesadas pertinentes. Las normas, procedimientos y acuerdos para proteger la información en tránsito se sugiere reflejen la clasificación de la información de que se trate. Cuando se transfiera información entre la organización y terceros, se recomienda establecer y mantener acuerdos de transferencia (incluida la autenticación del destinatario) para proteger la información en todas las formas en tránsito (ver inciso 5.10).

La transferencia de información puede ocurrir a través de transferencia electrónica, transferencia de medios de almacenamiento físico y transferencia verbal.

Para todos los tipos de transferencia de información, las reglas, procedimientos y acuerdos se sugiere incluir:

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

a) controles diseñados para proteger la información transferida de la interceptación, el acceso no autorizado, la copia, la modificación, el desvío, la destrucción y la denegación de servicio, incluidos los niveles de control de acceso proporcionales a la clasificación de la información de que se trate y cualquier control especial que se requiera para proteger la información sensible, como el uso de técnicas criptográficas (ver inciso 8.24);

b) controles para garantizar la trazabilidad y el no repudio, incluido el mantenimiento de una cadena de custodia de la información durante el tránsito;

c) identificación de los contactos adecuados relacionados con la transferencia, incluidos los propietarios de la información, los propietarios de riesgos, los responsables de seguridad y los custodios de la información, según proceda;

d) responsabilidades y responsabilidades en caso de incidentes de seguridad de la información, como la pérdida de medios de almacenamiento físicos o datos;

e) el uso de un sistema de etiquetado acordado para la información sensible o crítica, garantizando que se comprenda inmediatamente el significado de las etiquetas y que la información esté debidamente protegida (ver inciso 5.13);

f) fiabilidad y disponibilidad del servicio de traslado;

g) la política o las directrices sobre el uso aceptable de los servicios de transferencia de información (ver inciso 5.10);

h) directrices de retención y eliminación de todos los registros comerciales, incluidos los mensajes;

Nota: La legislación y las regulaciones locales pueden existir con respecto a la retención y eliminación de registros comerciales.

i) la consideración de cualquier otro requisito legal, reglamentario y contractual pertinente (ver inciso 5.31, inciso 5.32, inciso 5.33 y el inciso 5.34) relacionados con la transferencia de información (por ejemplo, requisitos para firmas electrónicas).

Transferencia electrónica

Se recomienda que las normas, procedimientos y acuerdos también tengan en cuenta los siguientes elementos al utilizar los servicios de comunicación electrónica para la transferencia de información:

a) detección y protección contra malware que pueda transmitirse mediante el uso de comunicaciones electrónicas (ver inciso 8.7);

b) la protección de la información electrónica sensible comunicada en forma de anexo;

c) prevención contra el envío de documentos y mensajes en las comunicaciones a la dirección o número incorrectos;

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

d) obtener la aprobación antes de utilizar servicios públicos externos como la mensajería instantánea, las redes sociales, el intercambio de archivos o el almacenamiento en la nube;

e) niveles más estrictos de autenticación al transferir información a través de redes de acceso público;

f) restricciones asociadas a los medios de comunicación electrónica (por ejemplo, impedir el reenvío automático de correo electrónico a direcciones de correo externas);

g) aconsejar al personal y otras partes interesadas que no envíen mensajes cortos (SMS) o mensajes instantáneos con información crítica, ya que estos pueden ser leídos en lugares públicos (y por lo tanto por personas no autorizadas) o almacenados en dispositivos no adecuadamente protegidos;

h) asesorar al personal y a otras partes interesadas sobre los problemas de la utilización de máquinas o servicios de fax, a saber:

1) acceso no autorizado a los almacenes de mensajes incorporados para recuperar mensajes;

2) programación deliberada o accidental de máquinas para enviar mensajes a números específicos.

Transferencia de medios de almacenamiento físico

Al transferir medios de almacenamiento físico (incluido el papel), las reglas, procedimientos y acuerdos también se sugiere incluyan:

a) responsabilidades de controlar y notificar la transmisión, el envío y la recepción;

b) garantizar la correcta dirección y transporte del mensaje;

c) envases que protejan el contenido de cualquier daño físico que pueda surgir durante el tránsito y de conformidad con las especificaciones de cualquier fabricante, por ejemplo, protegiendo contra cualquier factor medioambiental que pueda reducir la eficacia de la restauración de los medios de almacenamiento, como la exposición al calor, la humedad o los campos electromagnéticos; la utilización de normas técnicas mínimas para el envasado y la transmisión (por ejemplo, el uso de sobres opacos);

d) una lista de mensajeros fiables autorizados acordados por la dirección;

e) normas de identificación de mensajería;

f) en función del nivel de clasificación de la información en el medio de almacenamiento que vaya a transportarse, utilice controles a prueba de manipulaciones o resistentes a la manipulación (por ejemplo, bolsas, contenedores);

g) procedimientos para verificar la identificación de los mensajeros;

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

h) lista aprobada de terceros que prestan servicios de transporte o mensajería en función de la clasificación de la información;

i) mantener registros para identificar el contenido de los medios de almacenamiento, la protección aplicada, así como registrar la lista de destinatarios autorizados, los tiempos de transferencia a los custodios de tránsito y la recepción en el lugar de destino.

Transferencia verbal

Para proteger la transferencia verbal de información, se recomienda recordar al personal y a otras partes interesadas que:

a) no tener conversaciones verbales confidenciales en lugares públicos o a través de canales de comunicación inseguros, ya que estos pueden ser escuchados por personas no autorizadas;

b) no dejar mensajes que contengan información confidencial en contestadores automáticos o mensajes de voz, ya que estos pueden ser reproducidos por personas no autorizadas, almacenados en sistemas comunales o almacenados incorrectamente como resultado de una mala manipulación;

c) ser examinados al nivel apropiado para escuchar la conversación;

d) garantizar que se apliquen los controles de sala adecuados (por ejemplo, insonorización, puerta cerrada);

e) comenzar cualquier conversación delicada con un descargo de responsabilidad para que los presentes conozcan el nivel de clasificación y los requisitos de manejo de lo que están a punto de escuchar.

Otros datos

No hay otra información.

5.15 Control de acceso

Tipo de control	Propiedades de Seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Identidad_y_control_de_acceso	#Protección

Control

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

Se recomienda que las reglas para controlar el acceso físico y lógico a la información y otros activos asociados establezcan e implementen en función de los requisitos comerciales y de seguridad de la información.

Propósito

Para garantizar el acceso autorizado y evitar el acceso no autorizado a la información y otros activos asociados.

Orientación

Se recomienda que los propietarios de información y otros activos asociados determinen la seguridad de la información y los requisitos comerciales relacionados con el control de acceso. Se sugiere definir una política temática específica sobre el control de acceso que tenga en cuenta estos requisitos y que se comunique a todas las partes interesadas pertinentes.

Se recomienda que estos requisitos y la política específica del tema tenga en cuenta lo siguiente:

a) determinar qué entidades requieren qué tipo de acceso a la información y otros activos asociados;

b) la seguridad de las solicitudes (ver inciso 8.26);

c) el acceso físico, se sugiere este respaldado por controles físicos de entrada adecuados (ver el inciso 7.2, el inciso 7.3 y el inciso 7.4);

d) difusión y autorización de la información (por ejemplo, el principio de necesidad de conocer) y niveles de seguridad de la información y clasificación de la información (ver el inciso 5.10, el inciso 5.12 y el inciso 5.13);

e) restricciones al acceso privilegiado (ver el inciso 8.2);

f) la separación de funciones (ver el inciso 5.3);

g) la legislación pertinente, los reglamentos y cualquier obligación contractual relativa a la limitación del acceso a los datos o servicios (ver el inciso 5.31, el inciso 5.32, el inciso 5.33, el inciso 5.34 y el inciso 8.3);

h) segregación de las funciones de control de acceso (por ejemplo, solicitud de acceso, autorización de acceso, administración de acceso);

i) autorización formal de las solicitudes de acceso (ver el inciso 5.16 y el inciso 5.18);

j) la gestión de los derechos de acceso (ver el inciso 5.18);

k) registro (ver el inciso 8.15).

Se recomienda que las normas de control de acceso se apliquen definiendo y asignando derechos y restricciones de acceso adecuados a las entidades pertinentes (ver inciso 5.16). Una entidad puede representar a un usuario humano, así como a un elemento

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

técnico o lógico (por ejemplo, una máquina, un dispositivo o un servicio). Para simplificar la administración del control de acceso, se pueden asignar roles específicos a los grupos de entidades.

Al definir y aplicar las normas de control de acceso, se sugiere tenerse en cuenta:

a) coherencia entre los derechos de acceso y la clasificación de la información;

b) coherencia entre los derechos de acceso y las necesidades y requisitos de seguridad del perímetro físico;

c) considerar todos los tipos de conexiones disponibles en entornos distribuidos, de modo que las entidades solo tengan acceso a la información y otros activos asociados, incluidas las redes y los servicios de red, que estén autorizadas a utilizar;

d) considerar cómo pueden reflejarse los elementos o factores pertinentes para el control dinámico del acceso.

Otros datos

A menudo se utilizan principios generales en el contexto del control de acceso. Dos de los principios más utilizados son:

a) necesidad de saber: a una entidad solo se le concede acceso a la información que esa entidad necesita para llevar a cabo sus tareas (diferentes tareas o roles significan diferente información de necesidad de conocer y, por lo tanto, diferentes perfiles de acceso);

b) necesidad de uso: a una entidad solo se le asigna acceso a la infraestructura de tecnología de la información cuando existe una necesidad clara.

Se recomienda tener cuidado al especificar las reglas de control de acceso a considerar:

a) establecer reglas basadas en la premisa del mínimo privilegio, "Todo está generalmente prohibido a menos que esté expresamente permitido", en lugar de la regla más débil, "Todo está generalmente permitido a menos que esté expresamente prohibido";
b) los cambios en las etiquetas de información (ver inciso 5.13) iniciados automáticamente por los centros de tratamiento de la información y los iniciados a discreción de un usuario;

c) los cambios en los permisos de usuario iniciados automáticamente por el sistema de información y los iniciados por un administrador;

d) cuando definir y revisar periódicamente la aprobación.

Se recomienda que las reglas de control de acceso estén respaldadas por procedimientos documentados (ver inciso 5.16, inciso 5.17, inciso 5.18, inciso 8.2, inciso 8.3, inciso 8.4, inciso 8.5 y el inciso 8.18) y responsabilidades definidas (ver inciso 5.2 y el inciso 5.17).

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

Hay varias formas de implementar el control de acceso, como MAC (control de acceso obligatorio), DAC (control de acceso discrecional), RBAC (control de acceso basado en roles) y ABAC (control de acceso basado en atributos).

Las reglas de control de acceso también pueden contener elementos dinámicos (por ejemplo, una función que evalúa accesos pasados o valores de entorno específicos). Las reglas de control de acceso se pueden implementar en diferentes granularidades, que van desde cubrir redes o sistemas completos hasta campos de datos específicos y también pueden considerar propiedades como la ubicación del usuario o el tipo de conexión de red que se utiliza para el acceso. Estos principios y cómo se define el control de acceso granular pueden tener un impacto significativo en los costos. Las reglas más estrictas y la granularidad generalmente conducen a un mayor costo. Los requisitos empresariales y las consideraciones de riesgo se sugiere se utilicen para definir qué reglas de control de acceso se aplican y qué granularidad se requiere.

5.16 Gestión de identidades

Tipo de control	Propiedades de Seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Identidad_y_control_de_acceso	#Protección

Control

Se recomienda gestionar el ciclo de vida completo de las identidades.

Propósito

Permitir la identificación única de las personas y los sistemas que acceden a la información de la organización y otros activos asociados y permitir la asignación adecuada de derechos de acceso.

Orientación

Se recomienda que los procesos utilizados en el contexto de la gestión de identidades garantice que:

a) en el caso de las identidades asignadas a personas, una identidad específica solo está vinculada a una sola persona para poder responsabilizar a la persona por las acciones realizadas con esta identidad específica;

b) las identidades asignadas a varias personas (por ejemplo, identidades compartidas) solo se permiten cuando son necesarias por razones comerciales u operativas y están sujetas a una aprobación y documentación específicas;

c) las identidades asignadas a entidades no humanas están sujetas a una aprobación debidamente segregada y a una supervisión independiente y continua;

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

d) las identidades se desactivan o eliminan de manera oportuna si ya no son necesarias (por ejemplo, si sus entidades asociadas se eliminan o ya no se utilizan, o si la persona vinculada a una identidad ha abandonado la organización o ha cambiado el rol);

e) en un dominio específico, se asigna una sola identidad a una sola entidad, [es decir, se evita la asignación de múltiples identidades a la misma entidad dentro del mismo contexto (identidades duplicadas)];

f) se mantengan registros de todos los acontecimientos significativos relacionados con el uso y la gestión de las identidades de los usuarios y de la información de autenticación.

Se recomienda que la organización cuente con un proceso de apoyo para manejar los cambios en la información relacionada con las identidades de los usuarios. Estos procesos pueden incluir la re-verificación de documentos de confianza relacionados con una persona.

Al utilizar identidades proporcionadas o emitidas por terceros (por ejemplo, credenciales de redes sociales), se sugiere que la organización se asegure de que las identidades de terceros proporcionen el nivel de confianza requerido y que cualquier riesgo asociado sea conocido y suficientemente tratado. Esto puede incluir controles relacionados con terceros (ver inciso 5.19), así como controles relacionados con la información de autenticación asociada (ver inciso 5.17).

Otros datos

Proporcionar o revocar el acceso a la información y otros activos asociados suele ser un procedimiento de varios pasos:

a) confirmar los requisitos empresariales para el establecimiento de una identidad;

b) verificar la identidad de una entidad antes de asignarle una identidad lógica;

c) establecer una identidad;

d) configurar y activar la identidad. Esto también incluye la configuración y la configuración inicial de los servicios de autenticación relacionados;

e) proporcionar o revocar derechos de acceso específicos a la identidad, sobre la base de decisiones de autorización o derechos apropiadas (ver inciso 5.18).

5.17 Información de autenticación

Tipo de control	Propiedades de Seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Identidad_y_control_de_acceso	#Protección

Control

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

La asignación y gestión de la información de autenticación se sugiere se controle mediante un proceso de gestión, que incluya asesorar al personal sobre el manejo adecuado de la información de autenticación.

Propósito

Para garantizar la autenticación adecuada de la entidad y evitar fallos en los procesos de autenticación.

Orientación

Asignación de información de autenticación

Se recomienda que el proceso de asignación y gestión garantice que:

a) las contraseñas personales o los números de identificación personal (PIN) generados automáticamente durante los procesos de inscripción como información de autenticación secreta temporal no son adivinables y únicas para cada persona, y que los usuarios deberían cambiarlas después del primer uso;

b) se establezcan procedimientos para verificar la identidad de un usuario antes de proporcionar información nueva, de sustitución o de autenticación temporal;

c) la información de autenticación, incluida la información de autenticación temporal, se transmite a los usuarios de forma segura (por ejemplo, a través de un canal autenticado y protegido) y se evita el uso de mensajes de correo electrónico no protegidos (texto sin cifrar) para este fin;

d) los usuarios acusan recibo de la información de autenticación;

e) la información de autenticación predeterminada predefinida o proporcionada por los proveedores se cambia inmediatamente después de la instalación de los sistemas o el software;

f) se mantengan registros de acontecimientos significativos relativos a la asignación y gestión de la información de autenticación y se conceda su confidencialidad, y se apruebe el método de mantenimiento de registros (por ejemplo, mediante el uso de una herramienta de bóveda de contraseñas aprobada).

Responsabilidades del usuario

Se recomienda advertir a cualquier persona que tenga acceso a la información de autenticación o que utilice la información de autenticación que se asegure de que:

a) la información secreta de autenticación, como las contraseñas, se mantiene confidencial. Se recomienda que la información de autenticación secreta personal no se comparte con nadie. La información secreta de autenticación utilizada en el contexto de identidades vinculadas a múltiples usuarios o vinculadas a entidades no personales se comparte únicamente con personas autorizadas;

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

b) la información de autenticación afectada o comprometida se cambia inmediatamente después de la notificación o cualquier otra indicación de un compromiso;

c) cuando se utilizan contraseñas como información de autenticación, se seleccionan contraseñas seguras de acuerdo con las recomendaciones de mejores prácticas, por ejemplo:

1) las contraseñas no se basan en nada que alguien más pueda adivinar u obtener fácilmente utilizando información relacionada con la persona (por ejemplo, nombres, números de teléfono y fechas de nacimiento);

2) las contraseñas no se basan en palabras del diccionario o combinaciones de estas;

3) use frases de contraseña fáciles de recordar y trate de incluir caracteres alfanuméricos y especiales;

4) las contraseñas tienen una longitud mínima;

d) no se utilicen las mismas contraseñas en distintos servicios y sistemas;

e) la obligación de seguir estas normas también se incluye en las condiciones de empleo (ver inciso 6.2).

Sistema de gestión de contraseñas

Cuando las contraseñas se utilizan como información de autenticación, el sistema de gestión de contraseñas sugiere:

a) permita a los usuarios seleccionar y cambiar sus propias contraseñas e incluir un procedimiento de confirmación para corregir los errores de entrada;

b) haga cumplir contraseñas seguras de acuerdo con las recomendaciones de buenas prácticas [ver inciso c) de "Responsabilidades del usuario];

c) obligue a los usuarios a cambiar sus contraseñas en el primer inicio de sesión;

d) haga cumplir los cambios de contraseña según sea necesario, por ejemplo, después de un incidente de seguridad, o tras la terminación o el cambio de empleo cuando un usuario tenga contraseñas conocidas para identidades que permanecen activas (por ejemplo, identidades compartidas);

e) impida la reutilización de contraseñas anteriores;

f) evite el uso de contraseñas de uso común y nombres de usuario comprometidos, combinaciones de contraseñas de sistemas pirateados;

g) no muestre contraseñas en la pantalla cuando se introduzcan;

h) almacene y transmitir contraseñas en forma protegida.

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

Se recomienda que el cifrado de contraseñas y el hash realice de acuerdo con las técnicas criptográficas aprobadas para las contraseñas (ver inciso 8.24).

Otros datos

Las contraseñas o frases de contraseña son un tipo de información de autenticación de uso común y son un medio común para verificar la identidad de un usuario. Otros tipos de información de autenticación son las claves criptográficas, los datos almacenados en tokens de hardware (por ejemplo, tarjetas inteligentes) que producen códigos de autenticación y datos biométricos como escaneos de iris o huellas dactilares. Puede encontrar información adicional en la serie de normas que se indica en el inciso 10.24.

Requerir el cambio frecuente de contraseñas puede ser problemático porque los usuarios pueden molestarse por los cambios frecuentes, olvidar nuevas contraseñas, anotarlas en lugares inseguros o elegir contraseñas inseguras. La provisión de inicio de sesión único (SSO) u otras herramientas de administración de autenticación (por ejemplo, bóvedas de contraseñas) reduce la cantidad de información de autenticación que los usuarios se sugiere protejan y, por lo tanto, puede aumentar la efectividad de este control. Sin embargo, estas herramientas también pueden aumentar el impacto de la divulgación de información de autenticación.

Algunas aplicaciones requieren que las contraseñas de usuario sean asignadas por una autoridad independiente. En tales casos, el inciso a), el inciso c) y el inciso d) de "Sistema de gestión de contraseñas" no se aplican.

5.18 Derechos de acceso

Tipo de control	Propiedades de Seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Identidad_y_control_de_acceso	#Protección

Control

Se recomienda que los derechos de acceso a la información y otros activos asociados se aprovisione, revise, modifique y elimine de conformidad con la política y las normas específicas del tema de la organización para el control de acceso.

Propósito

Para garantizar que el acceso a la información y otros activos asociados se defina y autorice de acuerdo con los requisitos del negocio.

Orientación

Provisión y revocación de derechos de acceso

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

El proceso de aprovisionamiento para asignar o revocar los derechos de acceso físico y lógico concedidos a la identidad autenticada de una entidad se sugiere incluya:

a) obtener la autorización del propietario de la información y otros activos asociados para el uso de la información y otros activos asociados (ver inciso 5.9). La aprobación separada de los derechos de acceso por parte de la administración también puede ser apropiada;

b) teniendo en cuenta los requisitos empresariales y la política y las normas sobre control de acceso sobre el control de acceso por temas específicos de la organización;

c) considerar la segregación de funciones, incluida la segregación de las funciones de aprobación y aplicación de los derechos de acceso y la separación de funciones en conflicto;

d) garantizar que se eliminen los derechos de acceso cuando alguien no necesite acceder a la información y otros activos asociados, en particular garantizando que los derechos de acceso de los usuarios que han abandonado la organización se eliminen de manera oportuna;

e) considerar la posibilidad de conceder derechos de acceso temporal por un período de tiempo limitado y revocarlos en la fecha de expiración, en particular para el personal temporal o el acceso temporal requerido por el personal;

f) verificar que el nivel de acceso concedido se ajusta a las políticas específicas del tema sobre control de acceso (ver inciso 5.15) y es coherente con otros requisitos de seguridad de la información, como la separación de funciones (ver inciso 5.3);

g) garantizar que los derechos de acceso se activen (por ejemplo, por parte de los proveedores de servicios) solo después de que los procedimientos de autorización se hayan completado con éxito;

h) mantener un registro central de los derechos de acceso concedidos a un identificador de usuario (ID, lógico o físico) para acceder a la información y otros activos asociados;

i) modificar los derechos de acceso de los usuarios que han cambiado de roles o trabajos;

j) eliminar o ajustar los derechos de acceso físico y lógico, lo que puede hacerse mediante la eliminación, revocación o sustitución de claves, información de autenticación, tarjetas de identificación o suscripciones;

k) mantener un registro de los cambios en los derechos de acceso lógico y físico de los usuarios.

Revisión de los derechos de acceso

Las revisiones periódicas de los derechos de acceso físico y lógico se sugiere consideren lo siguiente:

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

a) los derechos de acceso de los usuarios después de cualquier cambio dentro de la misma organización (por ejemplo, cambio de empleo, promoción, degradación) o terminación del empleo (ver el inciso 6.1 al inciso 6.5);

b) autorizaciones de derechos de acceso privilegiado.

Consideración antes del cambio o terminación del empleo

Se recomienda que los derechos de acceso de un usuario a la información y otros activos asociados se revisen y ajusten o eliminen antes de cualquier cambio o terminación del empleo en función de la evaluación de factores de riesgo tales como:

a) si la terminación o el cambio es iniciado por el usuario o por la administración y el motivo de la terminación;

b) las responsabilidades actuales del usuario;

c) el valor de los activos actualmente accesibles.

Otros datos

Se recomienda considerar la posibilidad de establecer roles de acceso de usuario basados en los requisitos empresariales que resuman una serie de derechos de acceso en perfiles de acceso de usuario típicos. Las solicitudes de acceso y las revisiones de los derechos de acceso se gestionan más fácilmente a nivel de dichos roles que a nivel de derechos particulares.

Se recomienda considerar la posibilidad de incluir cláusulas en los contratos de personal y en los contratos de servicios que especifiquen sanciones si el personal intenta acceder sin autorización (ver el inciso 5.20, el inciso 6.2, el inciso 6.4 y el inciso 6.6).

En los casos de despido iniciado por la administración, el personal descontento o los usuarios externos pueden corromper deliberadamente la información o sabotear las instalaciones de procesamiento de información. En los casos de personas que renuncian o son despedidas, pueden verse tentadas a recopilar información para su uso futuro.

La clonación es una forma eficiente para que las organizaciones asignen acceso a los usuarios. Sin embargo, se sugiere hacer con cuidado basado en roles distintos identificados por la organización en lugar de simplemente clonar una identidad con todos los derechos de acceso asociados. La clonación tiene un riesgo inherente de resultar en derechos de acceso excesivos a la información y otros activos asociados.

5.19 Seguridad de la información en las relaciones con los proveedores

Tipo de control	Propiedades de Seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Identificar	#Seguridad_en_la_relación_con_proveedores	#Gobernabilidad_y_Ecosistema #Protección

Control

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

Se recomienda que los procesos y procedimientos se definan e implementen para gestionar los riesgos de seguridad de la información asociados con el uso de los productos o servicios del proveedor.

Propósito

Mantener un nivel acordado de seguridad de la información en las relaciones con los proveedores.

Orientación

Se recomienda que la organización establezca y comunique una política temática específica sobre las relaciones con los proveedores a todas las partes interesadas pertinentes.

Se sugiere que la organización identifique e implemente procesos y procedimientos para abordar los riesgos de seguridad asociados con el uso de productos y servicios proporcionados por los proveedores. Se sugiere que esto también aplique al uso de los recursos de los proveedores de servicios en la nube por parte de la organización. Se recomienda que estos procesos y procedimientos incluyan aquellos que deben ser implementados por la organización, así como aquellos que la organización requiere que el proveedor implemente para el inicio del uso de los productos o servicios de un proveedor o para la terminación del uso de los productos y servicios de un proveedor, tales como:

a) identificar y documentar los tipos de proveedores (por ejemplo, servicios de TIC, logística, servicios públicos, servicios financieros, componentes de infraestructura de TIC) que pueden afectar a la confidencialidad, integridad y disponibilidad de la información de la organización;

b) establecer cómo evaluar y seleccionar a los proveedores de acuerdo con la sensibilidad de la información, los productos y los servicios (por ejemplo, con análisis de mercado, referencias de clientes, revisión de documentos, evaluaciones in situ, certificaciones);

c) evaluar y seleccionar los productos o servicios del proveedor que cuenten con controles adecuados de seguridad de la información y revisarlos; en particular, la exactitud e integridad de los controles implementados por el proveedor que garantizan la integridad de la información del proveedor y el procesamiento de la información y, por lo tanto, la seguridad de la información de la organización;

d) definir la información de la organización, los servicios de TIC y la infraestructura física a la que los proveedores pueden acceder, supervisar, controlar o utilizar;

e) definir los tipos de componentes y servicios de infraestructura de TIC prestados por los proveedores que pueden afectar a la confidencialidad, integridad y disponibilidad de la información de la organización;

f) evaluar y gestionar los riesgos para la seguridad de la información asociados a:

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

1) el uso por parte de los proveedores de la información de la organización y otros activos asociados, incluidos los riesgos originados por posible personal de proveedores malintencionados;

2) mal funcionamiento o vulnerabilidades de los productos (incluidos los componentes de software y los subcomponentes utilizados en estos productos) o los servicios prestados por los proveedores;

g) supervisar el cumplimiento de los requisitos de seguridad de la información establecidos para cada tipo de proveedor y tipo de acceso, incluida la revisión por terceros y la validación del producto;

h) mitigar el incumplimiento de un proveedor, ya sea que se haya detectado mediante supervisión o por otros medios;

i) el manejo de incidentes y contingencias asociadas con los productos y servicios de los proveedores, incluidas las responsabilidades tanto de la organización como de los proveedores;

j) resiliencia y, si es necesario, medidas de recuperación y contingencia para garantizar la disponibilidad de la información del proveedor y el procesamiento de la información y, por lo tanto, la disponibilidad de la información de la organización;

k) sensibilización y capacitación del personal de la organización que interactúa con el personal de los proveedores en relación con las normas de compromiso adecuadas, las políticas, los procesos y los procedimientos específicos del tema y el comportamiento basados en el tipo de proveedor y el nivel de acceso de los proveedores a los sistemas y la información de la organización;

l) gestionar la transferencia necesaria de información, otros activos asociados y cualquier otra cosa que deba modificarse y garantizar que se mantenga la seguridad de la información durante todo el período de transferencia;

m) requisitos para garantizar una terminación segura de la relación con el proveedor, incluidos:

1) desaprovisionamiento de los derechos de acceso;

2) manejo de información;

3) determinar la propiedad de la propiedad intelectual desarrollada durante el compromiso;

4) portabilidad de la información en caso de cambio de proveedor o contratación interna;

5) gestión de registros;

6) devolución de activos;

7) la eliminación segura de la información y otros activos asociados;

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

8) requisitos de confidencialidad continuos;

n) nivel de seguridad del personal y seguridad física que se espera del personal y las instalaciones del proveedor.

Los procedimientos para continuar el procesamiento de la información en caso de que el proveedor no pueda suministrar sus productos o servicios (por ejemplo, debido a un incidente, porque el proveedor ya no está en el negocio o ya no proporciona algunos componentes debido a los avances tecnológicos) se recomienda considerar para evitar cualquier retraso en la organización de productos o servicios de reemplazo (por ejemplo, identificar un proveedor alternativo por adelantado o siempre utilizando proveedores alternativos).

Otros datos

En los casos en que no sea posible que una organización imponga requisitos a un proveedor, se sugiere la organización:

a) tener en cuenta la orientación dada en este control al tomar decisiones sobre la elección de un proveedor y su producto o servicio;

b) aplicar controles compensatorios según sea necesario sobre la base de una evaluación del riesgo.

La información puede ser puesta en riesgo por proveedores con una gestión inadecuada de la seguridad de la información. Se sugiere que los controles determinarse y aplicarse para gestionar el acceso del proveedor a la información y otros activos asociados. Por ejemplo, si existe una necesidad especial de confidencialidad de la información, se pueden utilizar acuerdos de no divulgación o técnicas criptográficas. Otro ejemplo son los riesgos de protección de datos personales cuando el acuerdo con el proveedor implica la transferencia o el acceso a la información a través de las fronteras. Se recomienda que la organización sea consciente de que la responsabilidad legal o contractual de proteger la información sigue siendo de la organización.

Los riesgos también pueden deberse a controles inadecuados de los componentes de la infraestructura de TIC o a los servicios prestados por los proveedores. El mal funcionamiento o los componentes o servicios vulnerables pueden causar violaciones de la seguridad de la información en la organización o a otra entidad (por ejemplo, pueden causar infección de malware, ataques u otros daños en entidades que no sean la organización).

Consulte la norma que se indica en el inciso 10.36 para obtener más detalles.

5.20 Abordar la seguridad de la información dentro de los acuerdos con proveedores

Tipo de control	Propiedades de Seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Identificar	#Seguridad_en_la_relación_con_proveedores	#Gobernabilidad_y_Ecosistema #Protección

Control

Los requisitos pertinentes de seguridad de la información se sugiere establezcan y acuerden con cada proveedor en función del tipo de relación con el proveedor.

Propósito

Mantener un nivel acordado de seguridad de la información en las relaciones con los proveedores.

Orientación

Se recomienda que los acuerdos con los proveedores establezcan y documenten para garantizar que haya un entendimiento claro entre la organización y el proveedor con respecto a las obligaciones de ambas partes de cumplir con los requisitos de seguridad de la información pertinentes.

Los siguientes términos pueden considerarse para su inclusión en los acuerdos con el fin de satisfacer los requisitos de seguridad de la información identificados:

a) descripción de la información que se proporciona o se accede y los métodos para proporcionar o acceder a la información;

b) clasificación de la información según el sistema de clasificación de la organización (ver inciso 5.10, inciso 5.12 y el inciso 5.13);

c) la correspondencia entre el propio sistema de clasificación de la organización y el sistema de clasificación del proveedor;

d) los requisitos legales, legales, reglamentarios y contractuales, incluida la protección de datos, el tratamiento de la información de identificación personal (PII), los derechos de propiedad intelectual y los derechos de autor, así como una descripción de cómo se garantiza su cumplimiento;

e) obligación de cada parte contractual de implementar un conjunto acordado de controles, incluido el control de acceso, la revisión del rendimiento, el monitoreo, la presentación de informes y la auditoría, y las obligaciones del proveedor de cumplir con los requisitos de seguridad de la información de la organización;

f) normas de uso aceptable de la información y otros activos asociados, incluido el uso inaceptable si es necesario;

g) procedimientos o condiciones para la autorización y eliminación de la autorización para el uso de la información de la organización y otros activos asociados por parte del personal proveedor (por ejemplo, a través de una lista explícita del personal proveedor autorizado para utilizar la información de la organización y otros activos asociados);

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

h) requisitos de seguridad de la información relativos a la infraestructura de TIC del proveedor; en particular, los requisitos mínimos de seguridad de la información para cada tipo de información y tipo de acceso sirvan de base para los acuerdos de proveedores individuales basados en las necesidades comerciales y los criterios de riesgo de la organización;

i) indemnizaciones y medidas correctivas por incumplimiento de los requisitos por parte del contratista;

j) requisitos y procedimientos de gestión de incidentes (especialmente notificación y colaboración durante la reparación de incidentes);

k) requisitos de formación y sensibilización para procedimientos específicos y requisitos de seguridad de la información (por ejemplo, para la respuesta a incidentes, procedimientos de autorización);

l) disposiciones pertinentes para la subcontratación, incluidos los controles que necesitan implementarse, como un acuerdo sobre el uso de subproveedores (por ejemplo, exigir que tengan las mismas obligaciones que el proveedor, exigir tener una lista de subproveedores y notificación antes de cualquier cambio);

m) contactos pertinentes, incluida una persona de contacto para cuestiones de seguridad de la información;

n) cualquier requisito de control, cuando sea legalmente permisible, para el personal del proveedor, incluidas las responsabilidades de llevar a cabo los procedimientos de detección y notificación si el control no se ha completado o si los resultados dan motivo de duda o preocupación;

o) las pruebas y los mecanismos de garantía de las certificaciones de terceros para los requisitos pertinentes de seguridad de la información relacionados con los procesos de los proveedores y un informe independiente sobre la eficacia de los controles;

p) derecho a auditar los procesos y controles de los proveedores relacionados con el acuerdo;

q) la obligación del proveedor de presentar periódicamente un informe sobre la eficacia de los controles y un acuerdo sobre la corrección oportuna de las cuestiones pertinentes planteadas en el informe;

r) procesos de resolución de defectos y resolución de conflictos;

s) proporcionar copias de seguridad alineadas con las necesidades de la organización (en términos de frecuencia, tipo y ubicación de almacenamiento);

t) garantizar la disponibilidad de una instalación alternativa (es decir, un sitio de recuperación ante desastres) que no esté sujeta a las mismas amenazas que la instalación principal y consideraciones para los controles alternativos (controles alternativos) en caso de fallo de los controles primarios;

u) tener un proceso de gestión del cambio que garantice la notificación anticipada a la organización y la posibilidad de que la organización no acepte cambios;

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

v) controles de seguridad física acordes con la clasificación de la información;

w) controles de transferencia de información para proteger la información durante la transferencia física o la transmisión lógica;

x) cláusulas de rescisión tras la celebración del acuerdo, incluida la gestión de registros, la devolución de activos, la enajenación segura de información y otros activos asociados, y cualquier obligación de confidencialidad en curso;

y) la provisión de un método para destruir de forma segura la información de la organización almacenada por el proveedor tan pronto como ya no sea necesaria;

z) garantizar, al final del contrato, el apoyo a otro proveedor o a la propia organización.

Se sugiere que la organización establezca y mantenga un registro de acuerdos con partes externas (por ejemplo, contratos, memorandos de entendimiento, acuerdos de intercambio de información) para realizar un seguimiento de hacia dónde va su información. Se recomienda que la organización también revise, valide y actualice regularmente sus acuerdos con partes externas para garantizar que sigan siendo necesarios y adecuados para el propósito con los capítulos de seguridad de la información relevantes.

Otros datos

Los acuerdos pueden variar considerablemente para diferentes organizaciones y entre los diferentes tipos de proveedores. Por lo tanto, se sugiere tener cuidado de incluir todos los requisitos pertinentes para abordar los riesgos de seguridad de la información.

Para obtener más información sobre los acuerdos con los proveedores, consulte la serie de normas que se indica en el inciso 10.35. Para conocer los acuerdos de servicio en la nube, consulte la serie de normas que se indica en el inciso 10.9.

5.21 Gestión de la seguridad de la información en la cadena de suministro de las TIC

Tipo de control	Propiedades de Seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Identificar	#Seguridad_en_la_relación_con_proveedores	#Gobernabilidad_y_Ecosistema #Protección

Control

Se recomienda definir e implementar procesos y procedimientos para gestionar los riesgos de seguridad de la información asociados con la cadena de suministro de productos y servicios de TIC.

Propósito

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

Mantener un nivel acordado de seguridad de la información en las relaciones con los proveedores.

Orientación

Se recomienda considerar los siguientes temas para abordar la seguridad de la información dentro de la seguridad de la cadena de suministro de las TIC, además de los requisitos generales de seguridad de la información para las relaciones con los proveedores:

a) definir los requisitos de seguridad de la información que se aplicaran a la adquisición de productos o servicios de TIC;

b) exigir que los proveedores de servicios de TIC propaguen los requisitos de seguridad de la organización a lo largo de la cadena de suministro si subcontratan partes del servicio de TIC prestado a la organización;

c) exigir que los proveedores de productos tic propaguen prácticas de seguridad adecuadas a lo largo de toda la cadena de suministro si estos productos incluyen componentes comprados o adquiridos a otros proveedores u otras entidades (por ejemplo, desarrolladores de software subcontratados y proveedores de componentes de hardware);

d) solicitar que los proveedores de productos tic faciliten información que describa los componentes informáticos utilizados en los productos;

e) solicitar que los proveedores de productos TIC faciliten información que describa las funciones de seguridad implementadas de su producto y la configuración necesaria para su funcionamiento seguro;

f) implementar un proceso de monitoreo y métodos aceptables para validar que los productos y servicios de TIC entregados cumplen con los requisitos de seguridad establecidos. Ejemplos de tales métodos de revisión de proveedores pueden incluir pruebas de penetración y pruebas o validaciones de atestaciones de terceros para las operaciones de seguridad de la información del proveedor;

g) implementar un proceso para identificar y documentar los componentes de productos o servicios que son críticos para mantener la funcionalidad y, por lo tanto, requieren una mayor atención, escrutinio y seguimiento adicional cuando se construyen fuera de la organización, especialmente si el proveedor subcontrata aspectos de los componentes de productos o servicios a otros proveedores;

h) obtener garantías de que los componentes críticos y su origen pueden rastrearse a lo largo de la cadena de suministro;

i) obtener garantías de que los productos TIC suministrados funcionan según lo esperado sin características inesperadas o no deseadas;

j) implementar procesos para garantizar que los componentes de los proveedores sean genuinos e inalterados de sus especificaciones. Las medidas de ejemplo incluyen etiquetas anti-manipulación, verificaciones criptográficas de hash o firmas digitales. El monitoreo del rendimiento fuera de especificación puede ser

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

un indicador de manipulación o falsificaciones. Se recomienda la prevención y detección de manipulaciones implementarse durante múltiples etapas del ciclo de vida de desarrollo del sistema, incluido el diseño, el desarrollo, la integración, las operaciones y el mantenimiento;

k) obtener garantías de que los productos de TIC alcanzan los niveles de seguridad requeridos, por ejemplo, mediante una certificación formal o un sistema de evaluación como el Acuerdo de Reconocimiento de Criterios Comunes;

l) definir normas para el intercambio de información sobre la cadena de suministro y cualquier posible problema y compromiso entre la organización y los proveedores;

m) la aplicación de procesos específicos para la gestión del ciclo de vida y la disponibilidad de los componentes de TIC y los riesgos de seguridad asociados. Esto incluye la gestión de los riesgos de que los componentes ya no estén disponibles debido a que los proveedores ya no están en el negocio o los proveedores ya no proporcionan estos componentes debido a los avances tecnológicos. Se sugiere considerar la identificación de un proveedor alternativo y el proceso para transferir el software y la competencia al proveedor alternativo.

Otros datos

Las prácticas específicas de gestión de riesgos de la cadena de suministro de las TIC se basan en las prácticas generales de seguridad de la información, calidad, gestión de proyectos e ingeniería de sistemas, pero no las reemplazan.

Se aconseja a las organizaciones que trabajen con los proveedores para comprender la cadena de suministro de las TIC y cualquier asunto que tenga un efecto importante en los productos y servicios que se proporcionan. La organización puede influir en las prácticas de seguridad de la información de la cadena de suministro de las TIC dejando claro en los acuerdos con sus proveedores las cuestiones que deberían abordar otros proveedores de la cadena de suministro de las TIC.

Se sugiere que las TIC se adquieran de fuentes acreditadas. La fiabilidad del software y el hardware es una cuestión de control de calidad. Si bien generalmente no es posible que una organización inspeccione los sistemas de control de calidad de sus proveedores, puede hacer juicios confiables basados en la reputación del proveedor.

La cadena de suministro de TIC, tal como se aborda aquí, incluye servicios en la nube.

Ejemplos de cadenas de suministro de TIC son:

a) el aprovisionamiento de servicios en la nube, cuando el proveedor de servicios en la nube se base en los desarrolladores de software, los proveedores de servicios de telecomunicaciones y los proveedores de hardware;

b) IoT, cuando el servicio involucra a los fabricantes de dispositivos, los proveedores de servicios en la nube (por ejemplo, los operadores de plataformas IoT), los desarrolladores de aplicaciones móviles y web, el proveedor de bibliotecas de software;

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

c) servicios de alojamiento, cuando el proveedor dependa de mesas de servicio externas, incluidos los niveles de soporte primero, segundo y tercero.

Consulte la norma que se indica en el inciso 10.37 para obtener más detalles, incluida la guía de evaluación de riesgos.

Las etiquetas de identificación de software (SWID) también pueden ayudar a lograr una mejor seguridad de la información en la cadena de suministro, al proporcionar información sobre la procedencia del software. Consulte la norma que se indica en el inciso 10.13 para obtener más detalles.

5.22 Seguimiento, revisión y gestión del cambio de los servicios de los proveedores

Tipo de control	Propiedades de Seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Identificar	#Seguridad_en_la_relación_con_proveedores#Aseguramiento_de_seguridad_de_la_información	#Gobernabilidad_y_Ecosistema #Protección#Defensa

Control

Es conveniente que la organización monitoreé, revise, evalué y gestione regularmente el cambio en las prácticas de seguridad de la información de los proveedores y la prestación de servicios.

Propósito

Mantener un nivel acordado de seguridad de la información y prestación de servicios en línea con los acuerdos con los proveedores.

Orientación

Se recomienda que el seguimiento, la revisión y la gestión del cambio de los servicios de los proveedores garanticen que se cumplan los términos y condiciones de seguridad de la información de los acuerdos, que los incidentes y problemas de seguridad de la información se gestionen adecuadamente y que los cambios en los servicios de los proveedores o en el estado de las empresas no afecten a la prestación de servicios.

Es conveniente que esto implique un proceso para gestionar la relación entre la organización y el proveedor para:

a) supervisar los niveles de rendimiento del servicio para verificar el cumplimiento de los acuerdos;

b) supervisar los cambios realizados por los proveedores, incluidos:

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

1) mejoras a los servicios actuales ofrecidos;

2) desarrollo de nuevas aplicaciones y sistemas;

3) modificaciones o actualizaciones de las políticas y procedimientos del proveedor;

4) controles nuevos o modificados para resolver incidentes de seguridad de la información y mejorar la seguridad de la información;

c) supervisar los cambios en los servicios de los proveedores, incluidos:

1) cambios y mejora de las redes;

2) uso de nuevas tecnologías;

3) adopción de nuevos productos o nuevas versiones o lanzamientos;

4) nuevas herramientas y entornos de desarrollo;

5) cambios en la ubicación física de las instalaciones de servicio;

6) cambio de subproveedores;

7) subcontratación a otro proveedor;

d) revisar los informes de servicio elaborados por el proveedor y organizar reuniones periódicas sobre la marcha de los trabajos, según lo exijan los acuerdos;

e) realizar auditorías de proveedores y subproveedores, junto con la revisión de los informes de los auditores independientes, si están disponibles, y el seguimiento de los problemas identificados;

f) proporcionar información sobre incidentes de seguridad de la información y revisar esta información según lo exijan los acuerdos y las directrices y procedimientos de apoyo;

g) revisar las pistas de auditoría de los proveedores y los registros de eventos de seguridad de la información, problemas operativos, fallas, rastreo de fallas e interrupciones relacionadas con el servicio prestado;

h) Responder y gestionar cualquier evento o incidente de seguridad de la información identificado;

i) identificar las vulnerabilidades de seguridad de la información y gestionarlas;

j) revisar los aspectos de seguridad de la información de las relaciones del proveedor con sus propios proveedores;

k) garantizar que el proveedor mantenga una capacidad de servicio suficiente junto con planes viables diseñados para garantizar que se mantengan los niveles de continuidad del servicio acordados tras fallas importantes del servicio o desastres

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

(ver inciso 5.29, ver inciso 5.30, ver inciso 5.35, ver inciso 5.36 y ver inciso 8.14);

l) garantizar que los proveedores asignen responsabilidades para revisar el cumplimiento y hacer cumplir los requisitos de los acuerdos;

m) evaluar periódicamente que los proveedores mantienen niveles adecuados de seguridad de la información.

La responsabilidad de gestionar las relaciones con los proveedores es conveniente se asigne a una persona o equipo designado. Se recomienda ponerse a disposición conocimientos técnicos y recursos suficientes para supervisar que se cumplen los requisitos del acuerdo, en particular los requisitos de seguridad de la información. Se sugiere tomar las medidas apropiadas cuando se observen deficiencias en la prestación de servicios.

Otros datos

Consulte la norma que se indica en el inciso 10.37 para obtener más detalles.

5.23 Seguridad de la información para el uso de servicios en la nube

Tipo de control	Propiedades de Seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Seguridad_en_la_relación_con_proveedores	#Gobernabilidad_y_Ecosistema #Protección

Control

Es conveniente que los procesos de adquisición, uso, gestión y salida de los servicios en la nube establezcan de acuerdo con los requisitos de seguridad de la información de la organización.

Propósito

Especificar y gestionar la seguridad de la información para el uso de servicios en la nube.

Orientación

Se recomienda que la organización establezca y comunique una política temática específica sobre el uso de los servicios en la nube a todas las partes interesadas pertinentes.

Se sugiere que la organización defina y comunique cómo pretende gestionar los riesgos de seguridad de la información asociados con el uso de servicios en la nube. Puede ser una extensión o parte del enfoque existente sobre cómo una organización gestiona los servicios prestados por partes externas (ver el inciso 5.21 y el inciso 5.22).

El uso de servicios en la nube puede implicar la responsabilidad compartida de la seguridad de la información y el esfuerzo de colaboración entre el proveedor de servicios

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

en la nube y la organización que actúa como cliente del servicio en la nube. Es esencial que las responsabilidades tanto para el proveedor de servicios en la nube como para la organización, que actúa como cliente del servicio en la nube, se definan e implementen adecuadamente.

Se recomienda que la organización defina:

a) todos los requisitos pertinentes de seguridad de la información asociados al uso de los servicios en la nube;

b) criterios de selección de servicios en la nube y alcance del uso de los servicios en la nube;

c) funciones y responsabilidades relacionadas con el uso y la gestión de los servicios en la nube;

d) qué controles de seguridad de la información son gestionados por el proveedor de servicios en la nube y cuáles son gestionados por la organización como cliente del servicio en la nube;

e) cómo obtener y utilizar las capacidades de seguridad de la información proporcionadas por el proveedor de servicios en la nube;

f) cómo obtener garantías sobre los controles de seguridad de la información implementados por los proveedores de servicios en la nube;

g) cómo gestionar los controles, las interfaces y los cambios en los servicios cuando una organización utiliza múltiples servicios en la nube, en particular de diferentes proveedores de servicios en la nube;

h) procedimientos para gestionar los incidentes de seguridad de la información que se produzcan en relación con el uso de los servicios en la nube;

i) su enfoque para supervisar, revisar y evaluar el uso continuo de los servicios en la nube para gestionar los riesgos de seguridad de la información;

j) cómo cambiar o detener el uso de los servicios en la nube, incluidas las estrategias de salida de los servicios en la nube.

Los acuerdos de servicios en la nube a menudo están predefinidos y no están abiertos a negociación. Para todos los servicios en la nube, es conveniente que la organización revise los acuerdos de servicios en la nube con los proveedores de servicios en la nube. Se sugiere un acuerdo de servicio en la nube aborde los requisitos de confidencialidad, integridad, disponibilidad y manejo de la información de la organización, con objetivos de nivel de servicio en la nube apropiados y objetivos cualitativos de servicio en la nube. Se recomienda que la organización también realice evaluaciones de riesgos relevantes para identificar los riesgos asociados con el uso del servicio en la nube. Cualquier riesgo residual relacionado con el uso del servicio en la nube se sugiere sea claramente identificado y aceptado por la administración adecuada de la organización.

Un acuerdo entre el proveedor de servicios en la nube y la organización, que actúa como cliente del servicio en la nube, es conveniente incluir las siguientes disposiciones para la protección de los datos de la organización y la disponibilidad de los servicios:

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

a) proporcionar soluciones basadas en normas aceptadas por la industria para la arquitectura y la infraestructura;

b) gestionar los controles de acceso del servicio en la nube para cumplir con los requisitos de la organización;

c) implementar soluciones de monitoreo y protección contra malware;

d) procesar y almacenar la información confidencial de la organización en lugares aprobados (por ejemplo, un país o región en particular) o dentro o sujeto a una jurisdicción en particular;

e) proporcionar soporte específico en caso de un incidente de seguridad de la información en el entorno de servicios en la nube;

f) garantizar que se cumplen los requisitos de seguridad de la información de la organización en caso de que los servicios en la nube se subcontraten a un proveedor externo (o prohibir que los servicios en la nube se subcontraten);

g) apoyar a la organización en la recopilación de pruebas digitales, teniendo en cuenta las leyes y reglamentos relativos a las pruebas digitales en diferentes jurisdicciones;

h) proporcionar soporte adecuado y disponibilidad de servicios durante un período de tiempo adecuado cuando la organización desee salir del servicio en la nube;

i) proporcionar la copia de seguridad requerida de los datos y la información de configuración y gestionar de forma segura las copias de seguridad, según corresponda, en función de las capacidades del proveedor de servicios en la nube utilizado por la organización, que actúa como cliente del servicio en la nube;

j) proporcionar y devolver información como archivos de configuración, código fuente y datos que son propiedad de la organización, actuando como el cliente del servicio en la nube, cuando se solicita durante la prestación del servicio o al finalizar el servicio.

La organización, actuando como el cliente del servicio en la nube, es conveniente considerar si el acuerdo requiere que los proveedores de servicios en la nube proporcionen una notificación anticipada antes de que se realicen cambios sustanciales que afecten al cliente en la forma en que se entrega el servicio a la organización, que incluyen:

a) cambios en la infraestructura técnica (por ejemplo, reubicación, reconfiguración o cambios en el hardware o software) que afecten o cambien la oferta de servicios en la nube;

b) procesar o almacenar información en una nueva jurisdicción geográfica o legal;

c) el uso de proveedores de servicios en la nube homólogos u otros subcontratistas (incluido el cambio de partes existentes o el uso de nuevas partes).

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

Se recomienda que la organización que utiliza servicios en la nube mantenga un estrecho contacto con sus proveedores de servicios en la nube. Estos contactos permiten el intercambio mutuo de información sobre seguridad de la información para el uso de los servicios en la nube, incluido un mecanismo para que tanto el proveedor de servicios en la nube como la organización, actuando como cliente del servicio en la nube, supervisen cada característica del servicio e informen de los incumplimientos de los compromisos contenidos en los acuerdos.

Otros datos

Este control considera la seguridad en la nube desde la perspectiva del cliente del servicio en la nube.

Puede encontrar información adicional relacionada con los servicios en la nube en la norma que se indica en el inciso 10.7, en el inciso 10.8 y el inciso 10.18. Los detalles relacionados con la portabilidad de la nube en apoyo de las estrategias de salida se pueden encontrar en el inciso 10.14. Los detalles relacionados con la seguridad de la información y los servicios de nube pública se describen en el inciso 10.29. Los detalles relacionados con la protección de PII en nubes públicas que actúan como procesador de PII se describen en la NMX-I-27018-NYCE-2021. Las relaciones con los proveedores de servicios en la nube están cubiertas por el inciso 10.38 y acuerdos de servicios en la nube y su contenido se trata en la serie de normas que se indican en el inciso 10.9, con seguridad y privacidad específicamente cubiertas por la norma que se indica en el inciso 10.10.

5.24 Planificación y preparación de la gestión de incidentes de seguridad de la información

Tipo de control	Propiedades de Seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Correctivo	#Confidencialidad #Integridad #Disponibilidad	#Responder #Recuperación	#Gobernanza#Gestión_de_eventos_de_seguridad_de_la_información	#Defensa

Control

Se sugiere que la organización planifique y prepare para la gestión de incidentes de seguridad de la información mediante la definición, el establecimiento y la comunicación de procesos, roles y responsabilidades de gestión de incidentes de seguridad de la información.

Propósito

Garantizar una respuesta rápida, eficaz, coherente y ordenada a los incidentes de seguridad de la información, incluida la comunicación sobre eventos de seguridad de la información.

Orientación

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

Funciones y responsabilidades

Se recomienda que la organización establezca procesos apropiados de gestión de incidentes de seguridad de la información. Las funciones y responsabilidades para llevar a cabo los procedimientos de gestión de incidentes deberían determinarse y comunicarse de manera efectiva a las partes interesadas internas y externas pertinentes.

Se sugiere considerar lo siguiente:

a) establecer un método común para notificar acontecimientos de seguridad de la información, incluidos los puntos de contacto (ver inciso 6.8);

b) establecer un proceso de gestión de incidentes para proporcionar a la organización la capacidad de gestionar incidentes de seguridad de la información, incluida la administración, la documentación, la detección, el triaje, la priorización, el análisis, la comunicación y la coordinación de las partes interesadas;

c) establecer un proceso de respuesta a incidentes para proporcionar a la organización la capacidad de evaluar, responder y aprender de los incidentes de seguridad de la información;

d) solo permitir que el personal competente maneje los problemas relacionados con incidentes de seguridad de la información dentro de la organización. Se recomienda que dicho personal reciba documentación sobre los procedimientos y capacitación periódica;

e) establecer un proceso para identificar la capacitación, la certificación y el desarrollo profesional continuo requeridos para el personal de respuesta a incidentes.

Procedimientos de gestión de incidencias

Se sugiere que los objetivos para la gestión de incidentes de seguridad de la información se acuerden con la administración y se recomienda garantizar que los responsables de la gestión de incidentes de seguridad de la información comprendan las prioridades de la organización para manejar incidentes de seguridad de la información, incluido el marco de tiempo de resolución basado en las posibles consecuencias y gravedad. Es conveniente implementar procedimientos de gestión de incidentes para cumplir con estos objetivos y prioridades.

Es conveniente que la administración se asegure de que se cree un plan de gestión de incidentes de seguridad de la información teniendo en cuenta los diferentes escenarios y procedimientos que se desarrollan e implementan para las siguientes actividades:

a) evaluación de eventos de seguridad de la información de acuerdo con criterios para lo que constituye un incidente de seguridad de la información;

b) seguimiento (ver el inciso 8.15 y el inciso 8.16), detección (ver el inciso 8.16), clasificación (ver el inciso 5.25), análisis y notificación (ver el inciso 6.8) de acontecimientos e incidentes de seguridad de la información (por medios humanos o automáticos);

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

c) gestionar los incidentes de seguridad de la información hasta su conclusión, incluida la respuesta y la escalada (ver el inciso 5.26), según el tipo y la categoría del incidente, la posible activación de la gestión de crisis y la activación de planes de continuidad, la recuperación controlada de un incidente y la comunicación a las partes interesadas internas y externas;

d) coordinación con las partes interesadas internas y externas, como autoridades, grupos de interés y foros externos, proveedores y clientes (ver el inciso 5.5 y el inciso 5.6);

e) el registro de actividades de gestión de incidentes;

f) tratamiento de las pruebas (ver el inciso 5.28);

g) análisis de la causa raíz o procedimientos post mortem;

h) identificación de las lecciones aprendidas y cualquier mejora en los procedimientos de gestión de incidentes o controles de seguridad de la información en general que se requieran.

Procedimientos de presentación de informes

Los procedimientos de presentación de informes se sugiere incluya:

a) las medidas que se adoptan en caso de que se produzca un evento de seguridad de la información (por ejemplo, anotar todos los detalles pertinentes de inmediato, como el mal funcionamiento y los mensajes en pantalla, informar inmediatamente al punto de contacto y solo tomar medidas coordinadas);

b) uso de formularios de incidentes para ayudar al personal a realizar todas las acciones necesarias al informar de incidentes de seguridad de la información;

c) procesos de retroalimentación adecuados para garantizar que las personas que informan de acontecimientos de seguridad de la información sean notificadas, en la medida de lo posible, de los resultados después de que se haya abordado y cerrado la cuestión;

d) creación de informes de incidentes.

Cualquier requisito externo sobre la notificación de incidentes a las partes interesadas pertinentes dentro del plazo definido (por ejemplo, los requisitos de notificación de infracciones a los reguladores) se sugiere tener en cuenta al aplicar los procedimientos de gestión de incidentes.

Otros datos

Los incidentes de seguridad de la información pueden trascender las fronteras organizacionales y nacionales. Para responder a tales incidentes, es beneficioso coordinar la respuesta y compartir información sobre estos incidentes con organizaciones externas según corresponda.

En la serie de normas que se indican en el inciso 10.34 se proporciona una guía detallada sobre la gestión de incidentes de seguridad de la información.

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

5.25 Evaluación y decisión sobre eventos de seguridad de la información

Tipo de control	Propiedades de Seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Detectivo	#Confidencialidad #Integridad #Disponibilidad	#Detectar #Responder	#Gestión_de_eventos_de_seguridad_de_la_información	#Defensa

Control

Es conveniente que la organización evalué los eventos de seguridad de la información y decidir si se clasifican como incidentes de seguridad de la información.

Propósito

Asegurar la categorización efectiva y la priorización de eventos de seguridad de la información.

Orientación

Se sugiere acordar un esquema de categorización y priorización de incidentes de seguridad de la información para la identificación de las consecuencias y la prioridad de un incidente. Es conveniente que el esquema incluya los criterios para categorizar los eventos como incidentes de seguridad de la información. Se recomienda que el punto de contacto evaluar cada evento de seguridad de la información utilizando el esquema acordado.

Se sugiere que el personal responsable de coordinar y responder a los incidentes de seguridad de la información realice la evaluación y tomar una decisión sobre los eventos de seguridad de la información.

Se recomienda que los resultados de la evaluación y la decisión se registren en detalle a efectos de futuras referencias y verificaciones.

Otros datos

La serie de normas que se indica en el inciso 10.34 proporciona más orientación sobre la gestión de incidentes.

5.26 Respuesta a incidentes de seguridad de la información

Tipo de control	Propiedades de Seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Correctivo	#Confidencialidad #Integridad	#Responder #Recuperación	#Gestión_de_eventos_de_seguri	#Defensa

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

	#Disponibilidad		dad_de_la_infor mación	

Control

Se recomienda que los incidentes de seguridad de la información respondan de acuerdo con los procedimientos documentados.

Propósito

Garantizar una respuesta eficiente y eficaz a los incidentes de seguridad de la información.

Orientación

Se sugiere que la organización establezca y comunique procedimientos sobre la respuesta a incidentes de seguridad de la información a todas las partes interesadas pertinentes.

Se sugiere que los incidentes de seguridad de la información sean respondidos por un equipo designado con la competencia requerida (ver el inciso 5.24).

Es conveniente que la respuesta incluya lo siguiente:

a) que contengan, si las consecuencias del incidente pueden propagarse, los sistemas afectados por el incidente;

b) la recogida de pruebas (ver el inciso 5.28) tan pronto como sea posible después de la ocurrencia;

c) la intensificación, según sea necesario, incluidas las actividades de gestión de crisis y posiblemente invocando planes de continuidad de las actividades (ver el inciso 5.29 y el inciso 5.30);

d) garantizar que todas las actividades de respuesta implicadas se registren correctamente para su posterior análisis;

e) comunicar la existencia del incidente de seguridad de la información o cualquier detalle relevante del mismo a todas las partes interesadas internas y externas pertinentes siguiendo el principio de necesidad de conocer;

f) coordinarse con las partes internas y externas, como autoridades, grupos de interés y foros externos, proveedores y clientes, para mejorar la eficacia de la respuesta y ayudar a minimizar las consecuencias para otras organizaciones;

g) una vez que el incidente se haya abordado con éxito, cerrarlo formalmente y registrarlo;

h) realizar análisis forenses de seguridad de la información, según sea necesario (ver el inciso 5.28);

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

i) realizar análisis posteriores al incidente para identificar la causa raíz. Asegurarse de que se documente y comunique de acuerdo con los procedimientos definidos (ver el inciso 5.27);

j) identificar y gestionar las vulnerabilidades y debilidades de la seguridad de la información, incluidas las relacionadas con los controles que han causado, contribuido o no han evitado el incidente.

Otros datos

La serie de normas que se indica en el inciso 10.34 proporciona más orientación sobre la gestión de incidentes.

5.27 Aprender de los incidentes de seguridad de la información

Tipo de control	Propiedades de Seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Identificar #Proteger	#Gestión_de_eventos_de_seguridad_de_la_información	#Defensa

Control

Se recomienda que los conocimientos adquiridos de los incidentes de seguridad de la información se utilicen para fortalecer y mejorar los controles de seguridad de la información.

Propósito

Para reducir la probabilidad o las consecuencias de futuros incidentes.

Orientación

Se sugiere que la organización establezca procedimientos para cuantificar y monitorear los tipos, volúmenes y costos de los incidentes de seguridad de la información.

Se sugiere que la información obtenida de la evaluación de incidentes de seguridad de la información se utilice para:

a) mejorar el plan de gestión de incidentes, incluidos los escenarios y procedimientos de incidentes (ver el inciso 5.24);

b) identificar incidentes recurrentes o graves y sus causas para actualizar la evaluación de riesgos de seguridad de la información de la organización y determinar e implementar los controles adicionales necesarios para reducir la probabilidad o las consecuencias de futuros incidentes similares. Los mecanismos para permitir eso incluyen la recopilación, cuantificación y monitoreo de información sobre tipos de incidentes, volúmenes y costos;

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

c) mejorar la sensibilización y la formación de los usuarios (ver el inciso 6.3) proporcionando ejemplos de lo que puede suceder, cómo responder ante tales incidentes y cómo evitarlos en el futuro.

Otros datos

La serie de normas que se indica en el inciso 10.34 proporciona más orientación.

5.28 Recopilación de pruebas

Tipo de control	Propiedades de Seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Correctivo	#Confidencialidad #Integridad #Disponibilidad	#Detectar #Responder	#Gestión_de_eventos_de_seguridad_de_la_información	#Defensa

Control

Se sugiere que la organización establecer e implementar procedimientos para la identificación, recolección, adquisición y preservación de evidencia relacionada con eventos de seguridad de la información.

Propósito

Garantizar una gestión coherente y eficaz de las pruebas relacionadas con incidentes de seguridad de la información a efectos de acciones disciplinarias y legales.

Orientación

Se recomienda desarrollar y seguir procedimientos internos cuando se trate de pruebas relacionadas con eventos de seguridad de la información a los efectos de acciones disciplinarias y legales. Se sugiere que los requisitos de las diferentes jurisdicciones se consideren para maximizar las posibilidades de admisión en las jurisdicciones pertinentes.

En general, estos procedimientos para la gestión de las pruebas se sugiere proporcionen instrucciones para la identificación, recopilación, adquisición y conservación de pruebas de conformidad con los diferentes tipos de medios de almacenamiento, dispositivos y estado de los dispositivos (es decir, encendidos o apagados). Por lo general, las pruebas necesitan recopilarse de manera que sean admisibles en los tribunales nacionales de justicia apropiados u otro foro disciplinario. Se sugiere que de ser posible demostrar que:

a) los registros están completos y no han sido manipulados de ninguna manera;

b) las copias de las pruebas electrónicas son probablemente idénticas a las originales;

c) cualquier sistema de información del que se hayan obtenido pruebas funcionaba correctamente en el momento en que se registraron las pruebas.

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

Cuando esté disponible, se sugiere buscar la certificación u otros medios pertinentes de cualificación del personal y las herramientas, a fin de reforzar el valor de las pruebas conservadas.

La evidencia digital puede trascender los límites organizacionales o jurisdiccionales. En tales casos, se recomienda garantizar que la organización tenga derecho a recopilar la información requerida como evidencia digital.

Otros datos

Cuando se detectara por primera vez un evento de seguridad de la información, no siempre es obvio si el evento dará lugar o no a una acción judicial. Por lo tanto, existe el peligro de que la evidencia necesaria se destruya intencional o accidentalmente antes de que se realice la gravedad del incidente. Es aconsejable involucrar el asesoramiento legal o la aplicación de la ley al principio de cualquier acción legal contemplada y asesorar sobre la evidencia requerida.

La NMX-I-27037-NYCE-2015 proporciona definiciones y directrices para la identificación, recopilación, adquisición y preservación de pruebas digitales.

La serie de normas que se indica en el inciso 10.40 se ocupa del descubrimiento electrónico, que implica el procesamiento de información almacenada electrónicamente como evidencia.

5.29 Seguridad de la información

Tipo de control	Propiedades de Seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo #Correctivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger #Responder	#Contiunidad	#Protección#Resilienci a

Control

Se sugiere que la organización planifique cómo mantener la seguridad de la información en un nivel apropiado durante la interrupción.

Propósito

Para proteger la información y otros activos asociados durante la interrupción.

Orientación

Es conveniente que la organización determine sus requisitos para adaptar los controles de seguridad de la información durante la interrupción. Se sugiere que los requisitos de seguridad de la información se incluyan en los procesos de gestión de la continuidad del negocio.

Se sugiere que los planes se desarrollen, implementarse, probarse, revisarse y evaluarse para mantener o restaurar la seguridad de la información de los procesos críticos del

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

negocio después de una interrupción o falla. Se sugiere que la seguridad de la información se restablezca en el nivel requerido y en los plazos requeridos.

Se recomienda que la organización implemente y mantenga:

a) controles de seguridad de la información, sistemas y herramientas de apoyo dentro de los planes de continuidad de las actividades y continuidad de las TIC;

b) procesos para mantener los controles de seguridad de la información existentes durante la interrupción;

c) compensar los controles de seguridad de la información que no puedan mantenerse durante la interrupción.

Otros datos

En el contexto de la continuidad del negocio y la planificación de la continuidad de las TIC, puede ser necesario adaptar los requisitos de seguridad de la información en función del tipo de interrupción, en comparación con las condiciones operativas normales. Como parte del análisis de impacto en el negocio y la evaluación de riesgos realizada dentro de la gestión de la continuidad del negocio, se sugiere considerar y priorizar las consecuencias de la pérdida de confidencialidad e integridad de la información, además de la necesidad de mantener la disponibilidad.

La información sobre los sistemas de gestión de la continuidad del negocio se puede encontrar en la NMX-I-22301-NYCE-2021 y en la norma que se indica en el inciso 10.19. Se puede encontrar más orientación sobre el análisis de impacto en el negocio (BIA) en la norma que se indica en el inciso 10.20.

5.30 Preparación de las TIC para la continuidad de las actividades

Tipo de control	Propiedades de Seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Correctivo	#Disponibilidad	#Responder	#Contiunidad	#Resiliencia

Control

La preparación para las TIC se sugiere se planifique, aplique, mantenga y pruebe sobre la base de los objetivos de continuidad de las actividades y los requisitos de continuidad de las TIC.

Propósito

Asegurar la disponibilidad de la información de la organización y otros activos asociados durante la interrupción.

Orientación

La preparación de las TIC para la continuidad de las actividades es un componente importante de la gestión de la continuidad de las actividades y la gestión de la seguridad

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

de la información para garantizar que los objetivos de la organización puedan seguir cumpliéndose durante la disrupción.

Los requisitos de continuidad de las TIC son el resultado del análisis de impacto en el negocio (BIA). Se sugiere que el proceso BIA utilice tipos y criterios de impacto para evaluar los impactos a lo largo del tiempo resultantes de la interrupción de las actividades comerciales que ofrecen productos y servicios. Es conveniente que la magnitud y la duración del impacto resultante se utilice para identificar las actividades priorizadas a las que se sugiere asignar un objetivo de tiempo de recuperación (RTO). Se recomienda que el BIA determine qué recursos se necesitan para apoyar las actividades priorizadas. También se sugiere especificar un RTO para estos recursos. Un subconjunto de estos recursos debería incluir los servicios de TIC.

El BIA que involucra servicios de TIC puede ampliarse para definir los requisitos de rendimiento y capacidad de los sistemas de TIC y los objetivos de punto de recuperación (RPO) de la información requerida para apoyar las actividades durante la interrupción.

Sobre la base de los resultados del BIA y la evaluación de riesgos que involucran a los servicios de TIC, se recomienda que la organización identifique y seleccione estrategias de continuidad de las TIC que consideren opciones para antes, durante y después de la interrupción. Las estrategias de continuidad del negocio pueden comprender una o más soluciones. Sobre la base de las estrategias, se sugiere elaborar, aplicar y ensayar planes para cumplir con el nivel de disponibilidad requerido de los servicios de TIC y en los plazos requeridos después de la interrupción o el fracaso de los procesos críticos.

Se recomienda que la organización vele porque:

a) exista una estructura organizativa adecuada para prepararse, mitigar y responder a una interrupción apoyada por personal con la responsabilidad, autoridad y competencia necesarias;

b) los planes de continuidad de las TIC, incluidos los procedimientos de respuesta y recuperación que detallan cómo la organización está planeando gestionar una interrupción del servicio de TIC, son:

   1) evaluado regularmente a través de ejercicios y pruebas;

   2) aprobado por la dirección;

c) los planes de continuidad de las TIC incluyen la siguiente información sobre la continuidad de las TIC:

   1) especificaciones de rendimiento y capacidad para cumplir los requisitos y objetivos de continuidad del negocio especificados en el BIA;

   2) RTO de cada servicio de TIC priorizado y los procedimientos para restaurar esos componentes;

   3) RPO de los recursos TIC priorizados definidos como información y los procedimientos para restaurar la información.

Otros datos

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

La gestión de la continuidad de las TIC constituye una parte clave de los requisitos de continuidad de las actividades en relación con la disponibilidad para poder:

a) responder y recuperarse de la interrupción de los servicios de TIC, independientemente de la causa;

b) garantizar que la continuidad de las actividades prioritarias cuente con el apoyo de los servicios de TIC necesarios;

c) responder antes de que se produzca una interrupción de los servicios de TIC, y tras la detección de al menos un incidente que pueda dar lugar a una interrupción de los servicios de TIC.

En la NMX-I-27031-NYCE-2019 se puede encontrar más orientación sobre la preparación de las TIC para la continuidad del negocio.

Se puede encontrar más orientación sobre los sistemas de gestión de la continuidad del negocio en la NMX-I-22301-NYCE-2019 y en la norma que se indica en el inciso 10.19.

Se puede encontrar más orientación sobre BIA en la norma que se indica en el inciso 10.20.

5.31 Requisitos legales, reglamentarios y contractuales

Tipo de control	Propiedades de Seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Identificar	#Cumplimiento_y_legal	#Gobernabilidad_y_Ecosistema #Protección

Control

Los requisitos legales, estatutarios, reglamentarios y contractuales relevantes para la seguridad de la información y el enfoque de la organización para cumplir con estos requisitos deberían identificarse, documentarse y mantenerse actualizados.

Propósito

Garantizar el cumplimiento de los requisitos legales, estatutarios, reglamentarios y contractuales relacionados con la seguridad de la información.

Orientación

General

Los requisitos externos, incluidos los requisitos legales, legales, reglamentarios o contractuales, es conveniente tener en cuenta cuando:

a) desarrollar políticas y procedimientos de seguridad de la información;

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

b) diseñar, aplicar o modificar controles de seguridad de la información;

c) clasificar la información y otros activos asociados como parte del proceso para establecer requisitos de seguridad de la información para las necesidades internas o para los acuerdos con los proveedores;

d) realizar evaluaciones de riesgos de seguridad de la información y determinar las actividades de tratamiento de riesgos de seguridad de la información;

e) determinar los procesos junto con las funciones y responsabilidades relacionadas con la seguridad de la información;

f) determinar los requisitos contractuales de los proveedores pertinentes para la organización y el alcance del suministro de productos y servicios.

Legislación y reglamentos

Se recomienda que la organización:

a) identificar toda la legislación y normativa pertinente a la seguridad de la información de la organización con el fin de conocer los requisitos para su tipo de negocio;

b) tener en cuenta el cumplimiento en todos los países pertinentes, si la organización:

- realiza negocios en otros países;
- utiliza productos y servicios de otros países donde las leyes y regulaciones pueden afectar a la organización;
- transfiere información a través de las fronteras jurisdiccionales donde las leyes y regulaciones pueden afectar a la organización;

c) revisar periódicamente la legislación y el reglamento identificados a fin de mantenerse al día con los cambios e identificar nueva legislación;

d) definir y documentar los procesos específicos y las responsabilidades individuales para cumplir estos requisitos.

Criptografía

La criptografía es un área que a menudo tiene requisitos legales específicos. Se recomienda tener en cuenta el cumplimiento de los acuerdos, leyes y reglamentos pertinentes relativos a los siguientes puntos:

a) restricciones a la importación o exportación de equipos y programas informáticos para la realización de funciones criptográficas;

b) restricciones a la importación o exportación de equipos y programas informáticos diseñados para que se le añadan funciones criptográficas;

c) restricciones en el uso de la criptografía;

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

d) métodos obligatorios o discrecionales de acceso de las autoridades de los países a la información cifrada;

e) validez de las firmas, sellos y certificados digitales.

Se recomienda buscar asesoramiento legal para garantizar el cumplimiento de la legislación y las regulaciones pertinentes, especialmente cuando la información cifrada o las herramientas de criptografía se mueven a través de las fronteras jurisdiccionales.

Contratos

Los requisitos contractuales relacionados con la seguridad de la información se sugiere incluyan los establecidos en:

a) contratos con clientes;

b) contratos con proveedores (ver inciso 5.20);

c) contratos de seguro.

Otros datos

No hay otra información.

5.32 Derechos de propiedad intelectual

Tipo de control	Propiedades de Seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Identificar	#Cumplimiento_y_legal	#Gobernabilidad_y_Ecosistema

Control

Se sugiere que la organización implemente procedimientos apropiados para proteger los derechos de propiedad intelectual.

Propósito

Garantizar el cumplimiento de los requisitos legales, legales, reglamentarios y contractuales relacionados con los derechos de propiedad intelectual y el uso de productos patentados.

Orientación

Se recomienda considerar las siguientes pautas para proteger cualquier material que pueda considerarse propiedad intelectual:

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

a) definir y comunicar una política temática específica sobre la protección de los derechos de propiedad intelectual;

b) procedimientos de publicación para el cumplimiento de los derechos de propiedad intelectual que definan el uso conforme de los programas informáticos y los productos de información;

c) adquirir software solo a través de fuentes conocidas y de buena reputación, para garantizar que no se infrinjan los derechos de autor;

d) mantener registros de activos adecuados e identificar todos los activos con requisitos para proteger los derechos de propiedad intelectual;

e) mantener pruebas y pruebas de la propiedad de licencias, manuales, etc.;

f) garantizar que no se supere el número máximo de usuarios o recursos [por ejemplo, unidades centrales de tratamiento (CPU)] permitidos en la licencia;

g) llevar a cabo revisiones para garantizar que solo se instalen software autorizado y productos con licencia;

h) establecer procedimientos para mantener unas condiciones de licencia adecuadas;

i) proporcionar procedimientos para eliminar o transferir software a otros;

j) cumplir con los términos y condiciones para el software y la información obtenida de redes públicas y fuentes externas;

k) no duplicar, convertir a otro formato o extraer de grabaciones comerciales (vídeo, audio) que no sean las permitidas por la legislación de derechos de autor o las licencias aplicables;

l) no copiar, total o parcialmente, normas (por ejemplo, las normas que se indican en el inciso 10.1 y el inciso 10.2), libros, artículos, informes u otros documentos, que no estén permitidos por la ley de derechos de autor o las licencias aplicables.

Otros datos

Los derechos de propiedad intelectual incluyen derechos de autor de software o documentos, derechos de diseño, marcas comerciales, patentes y licencias de código fuente.

Los productos de software propietario generalmente se suministran bajo un acuerdo de licencia que especifica los términos y condiciones de la licencia, por ejemplo, limitando el uso de los productos a máquinas específicas o limitando la copia a la creación de copias de seguridad solamente. Consulte la serie de normas que se indica en el inciso 10.11 para obtener detalles sobre la gestión de activos de TI.

Los datos se pueden adquirir de fuentes externas. Por lo general, dichos datos se obtienen en virtud de los términos de un acuerdo de intercambio de datos o un instrumento jurídico similar. Dichos acuerdos de intercambio de datos se sugiere dejar claro qué tratamiento está permitido para los datos adquiridos. También es aconsejable

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

que se indique claramente la procedencia de los datos. Consulte la norma que se indica en el inciso 10.23 para obtener detalles sobre los acuerdos de intercambio de datos.

Los requisitos legales, legales, reglamentarios y contractuales pueden imponer restricciones a la copia de material patentado. En particular, pueden requerir que solo se pueda utilizar material desarrollado por la organización o que sea licenciado o proporcionado por el desarrollador a la organización. La infracción de los derechos de autor puede dar lugar a acciones legales, que pueden implicar multas y procedimientos penales.

Además de que la organización necesite cumplir con sus obligaciones con respecto a los derechos de propiedad intelectual de terceros, también se recomienda gestionarse los riesgos de que el personal y los terceros no respeten los derechos de propiedad intelectual propios de la organización.

5.33 Protección de registros

Tipo de control	Propiedades de Seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Identificar #Proteger	#Cumplimiento_y_legal#Gestión_de_activos#Protección_de_la_información	#Defensa

Control

Se recomienda que los registros se protejan contra pérdida, destrucción, falsificación, acceso no autorizado y liberación no autorizada.

Propósito

Garantizar el cumplimiento de los requisitos legales, legales, reglamentarios y contractuales, así como las expectativas de la comunidad o la sociedad relacionadas con la protección y disponibilidad de los registros.

Orientación

Es conveniente que la organización tome las siguientes medidas para proteger la autenticidad, confiabilidad, integridad y usabilidad de los registros, ya que su contexto comercial y los requisitos para su administración cambian con el tiempo:

a) emitir directrices sobre el almacenamiento, la manipulación de la cadena de custodia y la eliminación de registros, lo que incluye la prevención de la manipulación de registros. Se sugiere que estas directrices estén alineadas con

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

la política temática específica de la organización sobre la gestión de registros y otros requisitos de registros;

b) elaborar un calendario de conservación en el que se definan los registros y el período de tiempo durante el cual es conveniente conservar.

Se sugiere que el sistema de almacenamiento y manipulación garantice la identificación de los registros y de su período de conservación, teniendo en cuenta la legislación o los reglamentos nacionales o regionales, así como las expectativas de la comunidad o la sociedad, si procede. Se recomienda que este sistema permita la destrucción adecuada de los registros después de ese período si la organización no los necesita.

Al decidir sobre la protección de registros organizacionales específicos, se recomienda considerar su clasificación de seguridad de la información correspondiente, basada en el esquema de clasificación de la organización. Es conveniente que los registros se clasifiquen en tipos de registros (por ejemplo, registros contables, registros de transacciones comerciales, registros de personal, registros legales), cada uno con detalles de los períodos de retención y el tipo de medios de almacenamiento permitidos que pueden ser físicos o electrónicos.

Se recomienda que los sistemas de almacenamiento de datos elijan de manera que los registros requeridos puedan recuperarse en un plazo y formato aceptables, en función de los requisitos que deban cumplirse.

Cuando se elijan medios de almacenamiento electrónico, se sugiere establecer procedimientos para garantizar la capacidad de acceder a los registros (tanto a los medios de almacenamiento como a la legibilidad del formato) durante todo el período de conservación para protegerlos contra pérdidas debidas a futuros cambios tecnológicos. Se sugiere que todas las claves criptográficas relacionadas y los programas asociados con archivos cifrados o firmas digitales también se conserven para permitir el descifrado de los registros durante el tiempo que se conserven los registros (ver el inciso 8.24).

Se recomienda que los procedimientos de almacenamiento y manipulación apliquen de conformidad con las recomendaciones proporcionadas por los fabricantes de medios de almacenamiento. Se sugiere considerar la posibilidad de deterioro de los medios utilizados para el almacenamiento de registros.

Otros datos

Los registros documentan eventos o transacciones individuales o pueden formar agregaciones que han sido diseñadas para documentar procesos de trabajo, actividades o funciones. Ambos son evidencia de la actividad comercial y los activos de información. Cualquier conjunto de información, independientemente de su estructura o forma, se puede gestionar como un registro. Esto incluye información en forma de documento, una colección de datos u otros tipos de información digital o analógica que se crean, capturan y gestionan en el curso de los negocios.

En la gestión de registros, los metadatos son datos que describen el contexto, el contenido y la estructura de los registros, así como su gestión a lo largo del tiempo. Los metadatos son un componente esencial de cualquier registro.

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

Puede ser necesario conservar algunos registros de forma segura para cumplir con los requisitos legales, legales, reglamentarios o contractuales, así como para respaldar las actividades comerciales esenciales. La legislación o el reglamento nacional pueden establecer el período de tiempo y el contenido de los datos para la retención de la información. Puede encontrar más información sobre la gestión de registros en la norma que se indica en el inciso 10.5.

5.34 Privacidad y protección de la PII

Tipo de control	Propiedades de Seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Identificar #Proteger	#Protección_de_la_información# Cumplimiento_y_legal	#Protección

Control

Se recomienda que la organización identifique y cumpla con los requisitos relacionados con la preservación de la privacidad y la protección de la PII de acuerdo con las leyes y regulaciones aplicables y los requisitos contractuales.

Propósito

Garantizar el cumplimiento de los requisitos legales, legales, reglamentarios y contractuales relacionados con los aspectos de seguridad de la información de la protección de la PII.

Orientación

Es conveniente que la organización establezca y comunique una política temática específica sobre privacidad y protección de la PII a todas las partes interesadas relevantes.

Se recomienda que la organización desarrolle e implemente procedimientos para la preservación de la privacidad y la protección de la PII. Se sugiere que estos procedimientos se comuniquen a todas las partes interesadas pertinentes que participen en el tratamiento de la información de identificación personal.

El cumplimiento de estos procedimientos y de toda la legislación y normativa pertinente relativa a la preservación de la privacidad y la protección de la PII requiere funciones, responsabilidades y controles adecuados. A menudo, esto se logra mejor mediante el nombramiento de una persona responsable, se recomienda como un oficial de privacidad, que proporcione orientación al personal, los proveedores de servicios y otras partes interesadas sobre sus responsabilidades individuales y los procedimientos específicos que se sugiere seguir.

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

La responsabilidad de manejar la PII se sugiere aborde teniendo en cuenta la legislación y los reglamentos pertinentes.

Se recomienda implementar medidas técnicas y organizativas apropiadas para proteger la PII.

Otros datos

Varios países han introducido legislación que establece controles sobre la recopilación, el procesamiento, la transmisión y la eliminación de la PII. Dependiendo de la legislación nacional respectiva, dichos controles pueden imponer derechos a quienes recopilan, procesan y difunden PII y también pueden restringir la autoridad para transferir PII a otros países.
La norma que se indica en el inciso 10.43 proporciona un marco de alto nivel para la protección de la PII dentro de los sistemas de TIC. Puede encontrar más información sobre los sistemas de gestión de la información de privacidad en la NMX-I-27701-NYCE-2021. Puede encontrar información específica sobre la gestión de la información de privacidad para nubes públicas que actúan como procesadores de PII en la NMX-I-27018-NYCE-2021.

La norma que se indica en el inciso 10.45 proporciona directrices para la evaluación del impacto en la privacidad (PIA) y ofrece un ejemplo de la estructura y el contenido de un informe PIA. En comparación con la NMX-I-27005-NYCE-2019, esto se centra en el procesamiento de PII y es relevante para aquellas organizaciones que procesan PII. Esto puede ayudar a identificar los riesgos de privacidad y las posibles mitigaciones para reducir estos riesgos a niveles aceptables.

5.35 Revisión independiente de la seguridad de la información

Tipo de control	Propiedades de Seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo #Correctivo	#Confidencialidad #Integridad #Disponibilidad	#Identificar #Proteger	#Aseguramiento_de_seguridad_de_la_información	#Gobernabilidad_y_Ecosistema

Control

El enfoque de la organización para administrar la seguridad de la información y su implementación, incluidas las personas, los procesos y las tecnologías, se sugiere revisar de forma independiente a intervalos planificados o cuando se producen cambios significativos.

Propósito

Asegurar la idoneidad, adecuación y eficacia continuas del enfoque de la organización para gestionar la seguridad de la información.

Orientación

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

Se recomienda que la organización tenga procesos para realizar revisiones independientes.

Se sugiere que la administración planifique e inicie revisiones periódicas independientes. Se recomienda que las revisiones incluyan la evaluación de oportunidades de mejora y la necesidad de cambios en el enfoque de la seguridad de la información, incluida la política de seguridad de la información, las políticas específicas del tema y otros controles.

Es conveniente que dichos exámenes sean realizados por personas independientes de la esfera objeto de examen (por ejemplo, la función de auditoría interna, un administrador independiente o una organización externa especializada en esos exámenes). Se sugiere que las personas que lleven a cabo estas revisiones tengan la competencia adecuada. La persona que realiza las revisiones no debería estar en la línea de autoridad para garantizar que tenga la independencia para hacer una evaluación.

Los resultados de las revisiones independientes se sugiere se comuniquen a la administración que inició las revisiones y, si procede, a la alta gerencia. Estos registros deberían mantenerse.

Si las revisiones independientes identifican que el enfoque y la implementación de la organización para administrar la seguridad de la información son inadecuados [por ejemplo, los objetivos y requisitos documentados no se cumplen o no cumplen con la dirección para la seguridad de la información establecida en la política de seguridad de la información y las políticas específicas del tema (ver el inciso 5.1)], se que la administración inicie acciones correctivas.

Además de los exámenes periódicos independientes, se sugiere que la organización considere la posibilidad de realizar exámenes independientes cuando:

a) las leyes y reglamentos que afectan a la organización cambian;

b) se producen incidentes significativos;

c) la organización inicia un nuevo negocio o cambia un negocio actual;

d) la organización comienza a utilizar un nuevo producto o servicio, o cambia el uso de un producto o servicio actual;

e) la organización cambia significativamente los controles y procedimientos de seguridad de la información.

Otros datos

La norma que se indica en el inciso 10.25 y el inciso 10.26 proporcionan orientación para llevar a cabo revisiones independientes.

5.36 Cumplimiento de políticas, reglas y estándares de seguridad de la información

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

Tipo de control	Propiedades de Seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Identificar #Proteger	#Cumplimiento_y_legal#Aseguramiento_de_seguridad_de_la_información	#Gobernabilidad_y_Ecosistema

Control

El cumplimiento de la política de seguridad de la información de la organización, las políticas específicas del tema, las reglas y los estándares se sugiere se revisen regularmente.

Propósito

Garantizar que la seguridad de la información se implemente y opere de acuerdo con la política de seguridad de la información de la organización, las políticas, reglas y estándares específicos del tema.

Orientación

Los gerentes, propietarios de servicios, productos o información deberían identificar cómo revisar que se cumplan los requisitos de seguridad de la información definidos en la política de seguridad de la información, las políticas específicas del tema, las reglas, los estándares y otras regulaciones aplicables. Se recomienda considerar herramientas automáticas de medición e informes para una revisión periódica eficiente.

Si se encuentra algún incumplimiento como resultado de la revisión, se sugiere que los gerentes:

a) identifiquen las causas del incumplimiento;

b) evalúen la necesidad de medidas correctivas para lograr el cumplimiento;

c) apliquen las medidas correctivas adecuadas;

d) revisen las medidas correctivas adoptadas para verificar su eficacia e identificar cualquier deficiencia o debilidad.

Los resultados de las revisiones y acciones correctivas llevadas a cabo por los gerentes, los propietarios de servicios, productos o información se sugiere se registren y estos registros es conveniente mantenerlos. Se recomienda que los administradores informen de los resultados a las personas que llevan a cabo exámenes independientes (ver el inciso 5.35) cuando se lleve a cabo un examen independiente en el ámbito de su responsabilidad.

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

Se sugiere que las acciones correctivas se completen de manera oportuna según corresponda al riesgo. Si no se completa en el próximo examen programado, es conveniente que los progresos al menos lo aborden en ese examen.

Otros datos

El monitoreo operacional del uso del sistema se cubre en el inciso 8.15, en el inciso 8.16 y el inciso 8.17.

5.37 Procedimientos operativos documentados

Tipo de control	Propiedades de Seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo #Correctivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger #Recuperación	#Gestión_de_activos#Seguridad_física#Seguridad_de_sistemas_y_redes#Seguridad_de_aplicaciones#Configuración_segura#Identidad_y_control_de_acceso#Amenazas_y_gestión_de_vulnerabilidades#Continuidad#Gestión_de_eventos_de_seguridad_de_la_información	#Gobernabilidad_y_Ecosistema #Protección#Defensa

Control

Se sugiere que los procedimientos operativos para las instalaciones de procesamiento de información se documenten y pongan a disposición del personal que los necesite.

Propósito

Asegurar el correcto y seguro funcionamiento de las instalaciones de tratamiento de la información.

Orientación

Se recomienda preparar procedimientos documentados para las actividades operativas de la organización asociadas con la seguridad de la información, por ejemplo:

a) cuando la actividad deba ser realizada de la misma manera por muchas personas;

b) cuando la actividad se realiza raramente y cuando se realiza la próxima vez, es probable que el procedimiento se haya olvidado;

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

c) cuando la actividad sea nueva y presente un riesgo si no se realiza correctamente;

d) antes de entregar la actividad al nuevo personal.

Es conveniente que los procedimientos operativos especifiquen:

a) las personas responsables;

b) la instalación y configuración seguras de los sistemas;

c) procesamiento y manejo de la información, tanto automatizado como manual;

d) copia de seguridad (ver el inciso 8.13) y resiliencia;

e) requisitos de programación, incluidas las interdependencias con otros sistemas;

f) instrucciones para gestionar errores u otras condiciones excepcionales [por ejemplo, restricciones en el uso de programas de utilidad (ver el inciso 8.18)], que pueden surgir durante la ejecución del trabajo;

g) contactos de soporte y escalamiento, incluidos los contactos de apoyo externo en caso de dificultades operativas o técnicas inesperadas;

h) instrucciones de manipulación de los soportes de almacenamiento (ver el inciso 7.10 y el inciso 7.14);

i) procedimientos de reinicio y recuperación del sistema para su uso en caso de fallo del sistema;

j) la gestión de la información de seguimiento de auditoría y registro del sistema (ver el inciso 8.15 y el inciso 8.17) y de los sistemas de seguimiento por vídeo (ver el inciso 7.4);

k) procedimientos de supervisión como la capacidad, el rendimiento y la seguridad (ver el inciso 8.6 y el inciso 8.16);

l) instrucciones de mantenimiento.

Los procedimientos operativos documentados se sugiere se revisen y actualicen cuando sea necesario. Es conveniente autorizar cambios en los procedimientos operativos documentados. Cuando sea técnicamente factible, se sugiere que los sistemas de información se gestionen de manera coherente, utilizando los mismos procedimientos, herramientas y utilidades.

Otros datos

No hay otra información.

6 Controles de personas

6.1 Chequeo

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

Tipo de control	Propiedades de Seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Seguridad_de_los_recursos_humanos	#Gobernabilidad_y_Ecosistema

Control

Las verificaciones de antecedentes de todos los candidatos para convertirse en personal se sugiere se lleven a cabo antes de unirse a la organización y de forma continúa teniendo en cuenta las leyes, regulaciones y ética aplicables y ser proporcionales a los requisitos comerciales, se recomienda que la clasificación de la información a la que se accede y los riesgos percibidos.

Propósito

Garantizar que todo el personal sea elegible y adecuado para los roles para los que se considera y siga siendo elegible y adecuado durante su empleo.

Orientación

Es conveniente llevar a cabo un proceso de selección para todo el personal, incluido el personal a tiempo completo, a tiempo parcial y temporal. Cuando estas personas son contratadas a través de proveedores de servicios, se sugiere que los requisitos de selección se incluyan en los acuerdos contractuales entre la organización y los proveedores.

Se recomienda que la información sobre todos los candidatos que se están considerando para puestos dentro de la organización se recopilen y manejen teniendo en cuenta cualquier legislación apropiada existente en la jurisdicción pertinente. En algunas jurisdicciones, la organización puede estar legalmente obligada a informar a los candidatos de antemano sobre las actividades de selección.

Se sugiere que la verificación tenga en cuenta toda la privacidad pertinente, la protección de la PII y la legislación basada en el empleo y, cuando esté permitida, se recomienda incluya lo siguiente:

a) disponibilidad de referencias satisfactorias (por ejemplo, referencias comerciales y personales);

b) una verificación (para su exhaustividad y exactitud) del currículum vitae del solicitante;

c) confirmación de las cualificaciones académicas y profesionales reivindicadas;

d) verificación de identidad independiente (por ejemplo, pasaporte u otro documento aceptable expedido por las autoridades competentes);

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

e) verificación más detallada, como la revisión de crédito o la revisión de antecedentes penales si el candidato asume un papel crítico.

Cuando se contrata a una persona para un rol específico de seguridad de la información, se recomienda que la organización se asegure de que el candidato:

a) tiene la competencia necesaria para desempeñar la función de seguridad;

b) se puede confiar en que asuma el rol, especialmente si el rol es crítico para la organización.

Cuando un trabajo, ya sea en el nombramiento inicial o en la promoción, involucra a la persona que tiene acceso a las instalaciones de procesamiento de información y, en particular, si esto implica el manejo de información confidencial (por ejemplo, información financiera, información personal o información de atención médica), se sugiere que la organización también considere verificaciones adicionales y más detalladas.

Se recomienda que los procedimientos definan criterios y limitaciones para las revisiones de verificación (por ejemplo, quién es elegible para evaluar a las personas y cómo, cuándo y por qué se llevan a cabo las revisiones de verificación).

En situaciones en las que la verificación no pueda completarse a tiempo, se sugiere implementar controles de mitigación hasta que finalice la revisión, por ejemplo:

a) retraso en la incorporación;

b) retraso en el despliegue de activos corporativos;

c) incorporación con acceso reducido;

d) terminación del empleo.

Es conveniente que los controles de verificación se repitan periódicamente para confirmar la idoneidad continua del personal, dependiendo de la criticidad del papel de una persona.

Otros datos

No hay otra información.

6.2 Términos y condiciones de empleo

Tipo de control	Propiedades de Seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Seguridad_de_los_recursos_humanos	#Gobernabilidad_y_Ecosistema

Control

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

Es conveniente que los acuerdos contractuales de empleo establezcan las responsabilidades del personal y de la organización para la seguridad de la información.

Propósito

Asegurar que el personal comprenda sus responsabilidades de seguridad de la información para los roles para los que son considerados.

Orientación

Se recomienda que las obligaciones contractuales para el personal tengan en cuenta la política de seguridad de la información de la organización y las políticas relevantes para temas específicos. Además, se pueden aclarar y enunciar los siguientes puntos:

a) acuerdos de confidencialidad o no divulgación que el personal al que se da acceso a información confidencial se sugiere firmen antes de que se le dé acceso a la información y otros activos asociados (ver inciso 6.6);

b) responsabilidades y derechos legales [por ejemplo, en relación con las leyes de derechos de autor o la legislación de protección de datos (ver el inciso 5.32 y el inciso 5.34)];

c) responsabilidades para la clasificación de la información y la gestión de la información de la organización y otros activos asociados, las instalaciones de procesamiento de información y los servicios de información manejados por el personal (ver el inciso 5.9 al inciso 5.13);

d) responsabilidades en el tratamiento de la información recibida de las partes interesadas;

e) es conveniente que las medidas que se adopten si el personal hace caso omiso de los requisitos de seguridad de la organización (ver inciso 6.4).

Se recomienda que los roles y responsabilidades de seguridad de la información se comuniquen a los candidatos durante el proceso previo al empleo.

Es conveniente que la organización se asegure de que el personal acepte los términos y condiciones relativos a la seguridad de la información. Se recomienda que estos términos y condiciones sean apropiados a la naturaleza y el alcance del acceso que tienen a los activos de la organización asociados con los sistemas y servicios de información. Los términos y condiciones relacionados con la seguridad de la información se sugiere se revisen cuando cambien las leyes, reglamentos, la política de seguridad de la información o las políticas específicas del tema.

Cuando proceda, se sugiere que las responsabilidades contenidas en las condiciones de empleo continúen durante un período definido después de la finalización del empleo (ver el inciso 6.5).

Otros datos

Se puede utilizar un código de conducta para establecer las responsabilidades de seguridad de la información del personal con respecto a la confidencialidad, la protección

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

de la PII, la ética, el uso apropiado de la información de la organización y otros activos asociados, así como las prácticas de buena reputación esperadas por la organización.

Se puede requerir que una parte externa, con la que está asociado el personal del proveedor, celebre acuerdos contractuales en nombre de la persona contratada.

Si la organización no es una entidad legal y no tiene empleados, el equivalente del acuerdo contractual y los términos y condiciones se puede considerar de acuerdo con la orientación de este control.

6.3 Sensibilización, educación y formación en materia de seguridad de la información

Tipo de control	Propiedades de Seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Seguridad_de_los_recursos_humanos	#Gobernabilidad_y_Ecosistema

Control

Es conveniente que el personal de la organización y las partes interesadas pertinentes reciban información adecuada sobre la seguridad de la información, educación y capacitación y actualizaciones periódicas de la política de seguridad de la información de la organización, políticas y procedimientos específicos del tema, según sea pertinente para su función laboral.

Propósito

Garantizar que el personal y las partes interesadas pertinentes conozcan y cumplan con sus responsabilidades de seguridad de la información.

Orientación

General

Se recomienda establecer un programa de sensibilización, educación y capacitación en materia de seguridad de la información de conformidad con la política de seguridad de la información de la organización, las políticas temáticas específicas y los procedimientos pertinentes sobre seguridad de la información, teniendo en cuenta la información de la organización que es conveniente proteger y los controles de seguridad de la información que se han aplicado para proteger la información.

Se sugiere que la sensibilización, la educación y la formación en materia de seguridad de la información se lleve a cabo periódicamente. La concienciación inicial, la educación y la capacitación pueden aplicarse al nuevo personal y a aquellos que se transfieren a nuevos puestos o roles con requisitos de seguridad de la información sustancialmente diferentes.

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

Se recomienda que la comprensión del personal se evalúe al final de una actividad de sensibilización, educación o formación para poner a prueba la transferencia de conocimientos y la eficacia del programa de sensibilización, educación y formación.

Conciencia

Un programa de sensibilización sobre la seguridad de la información se sugiere tenga por objeto sensibilizar al personal sobre sus responsabilidades en materia de seguridad de la información y los medios por los que se cumplen esas responsabilidades.

Es conveniente que el programa de sensibilización se planifique teniendo en cuenta las funciones del personal de la organización, incluido el personal interno y externo (por ejemplo, consultores externos, personal de proveedores). Las actividades del programa de sensibilización se sugiere se programen a lo largo del tiempo, preferiblemente con regularidad, de modo que las actividades se repitan y abarquen al nuevo personal. Se recomienda también basarse en las lecciones aprendidas de los incidentes de seguridad de la información.

El programa de sensibilización se sugiere incluya una serie de actividades de sensibilización a través de canales físicos o virtuales apropiados, como campañas, folletos, carteles, boletines, sitios web, sesiones informativas, sesiones informativas, módulos de aprendizaje electrónico y correos electrónicos.

Es conveniente que la concienciación sobre la seguridad de la información abarque aspectos generales como:

a) el compromiso de la dirección con la seguridad de la información en toda la organización;

b) las necesidades de familiaridad y cumplimiento en relación con las normas y obligaciones de seguridad de la información aplicables, teniendo en cuenta la política de seguridad de la información y las políticas, normas, leyes, estatutos, reglamentos, contratos y acuerdos específicos del tema;

c) la responsabilidad personal por las propias acciones e inacciones, y las responsabilidades generales para asegurar o proteger la información perteneciente a la organización y a las partes interesadas;

d) procedimientos básicos de seguridad de la información [por ejemplo, notificación de sucesos de seguridad de la información (ver el inciso 6.8)] y controles de referencia [por ejemplo, seguridad de contraseñas (ver el inciso 5.17)];

e) puntos de contacto y recursos para obtener información y asesoramiento adicionales sobre cuestiones de seguridad de la información, incluidos otros materiales de sensibilización sobre la seguridad de la información.

Educación y formación

Se sugiere que la organización identifique, prepare e implemente un plan de capacitación apropiado para los equipos técnicos cuyos roles requieren conjuntos de habilidades y experiencia específicas. Se sugiere que los equipos técnicos tengan las habilidades para configurar y mantener el nivel de seguridad requerido para dispositivos, sistemas,

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

aplicaciones y servicios. Si faltan habilidades, se sugiere que la organización tome medidas y las adquiera.

El programa de educación y capacitación se sugiere considere diferentes formas [por ejemplo, conferencias o autoestudios, ser asesorado por personal experto o consultores (capacitación en el trabajo), rotar a los miembros del personal para seguir diferentes actividades, reclutar personas ya calificadas y contratar consultores]. Puede utilizar diferentes medios de entrega, incluidos el aula, el aprendizaje a distancia, el basado en la web, a su propio ritmo y otros. Se recomienda que el personal técnico mantenga sus conocimientos actualizados suscribiéndose a boletines y revistas o asistiendo a conferencias y eventos destinados a la mejora técnica y profesional.

Otros datos

Al componer un programa de sensibilización, es importante no solo centrarse en el "qué" y el "cómo", sino también en el "por qué", cuando sea posible. Es importante que el personal comprenda el objetivo de la seguridad de la información y el efecto potencial, positivo y negativo, en la organización de su propio comportamiento.

La sensibilización, la educación y la formación en materia de seguridad de la información pueden formar parte de otras actividades, por ejemplo, la gestión general de la información, las TIC, la seguridad, la privacidad o la formación en materia de seguridad, o llevarse a cabo en colaboración con ellas.

6.4 Proceso disciplinario

Tipo de control	Propiedades de Seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo #Correctivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger #Responder	#Seguridad_de_los_recursos_humanos	#Gobernabilidad_y_Ecosistema

Control

Se sugiere formalizar y comunicar un proceso disciplinario para tomar medidas contra el personal y otras partes interesadas relevantes que hayan cometido una violación de la política de seguridad de la información.

Propósito

Para garantizar que el personal y otras partes interesadas relevantes entiendan las consecuencias de la violación de la política de seguridad de la información, para disuadir y tratar adecuadamente con el personal y otras partes interesadas relevantes que cometieron la violación.

Orientación

Se recomienda que el proceso disciplinario no inicie sin la verificación previa de que se ha producido una violación de la política de seguridad de la información (ver el inciso 5.28).

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

Se sugiere que el proceso disciplinario formal prevea una respuesta gradual que tenga en cuenta factores tales como:

a) la naturaleza (quién, qué, cuándo, cómo) y la gravedad de la infracción y sus consecuencias;

b) si el delito fue intencional (malicioso) o no intencional (accidental);

c) si se trata o no de una primera infracción o de una reincidencia;

d) si el infractor estaba o no debidamente formado.

Se sugiere que la respuesta tenga en cuenta los requisitos legales, estatutarios, reglamentarios, contractuales y comerciales pertinentes, así como otros factores según sea necesario. Se recomienda que el proceso disciplinario también utilice como elemento disuasorio para evitar que el personal y otras partes interesadas pertinentes violen la política de seguridad de la información, las políticas específicas del tema y los procedimientos para la seguridad de la información. Las violaciones deliberadas de la política de seguridad de la información pueden requerir acciones inmediatas.

Otros datos

Es conveniente que siempre que sea posible, la identidad de las personas sujetas a medidas disciplinarias se proteja de conformidad con los requisitos aplicables.

Cuando las personas demuestran un comportamiento excelente con respecto a la seguridad de la información, pueden ser recompensadas para promover la seguridad de la información y fomentar el buen comportamiento.

6.5 Responsabilidades después de la terminación o cambio de empleo

Tipo de control	Propiedades de Seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Seguridad_de_los_recursos_humanos#Gestión_de_activos	#Gobernabilidad_y_Ecosistema

Control

Las responsabilidades y deberes de seguridad de la información que siguen siendo válidos después de la terminación o el cambio de empleo se sugiere se definan, hacerse cumplir y comunicarse al personal pertinente y otras partes interesadas.

Propósito

Para proteger los intereses de la organización como parte del proceso de cambio o terminación de empleo o contratos.

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

Orientación

Se recomienda que el proceso para gestionar la terminación o el cambio de empleo se defina qué responsabilidades y deberes de seguridad de la información se sugiere seguir siendo válidos después de la terminación o el cambio. Esto puede incluir la confidencialidad de la información, la propiedad intelectual y otros conocimientos obtenidos, así como las responsabilidades contenidas en cualquier otro acuerdo de confidencialidad (ver el inciso 6.6). Las responsabilidades y deberes que siguen siendo válidos después de la terminación del empleo o contrato deberían estar contenidos en los términos y condiciones de empleo del individuo (ver el inciso 6.2), contrato o acuerdo. Otros contratos o acuerdos que continúan durante un período definido después del final del empleo del individuo también pueden contener responsabilidades de seguridad de la información.

Los cambios de responsabilidad o empleo se recomienda gestionar como la terminación de la responsabilidad o empleo actual combinado con el inicio de la nueva responsabilidad o empleo.

Los roles y responsabilidades de seguridad de la información que tiene cualquier persona que deje o cambie de trabajo deberían identificarse y transferirse a otra persona.

Es conveniente establecer un proceso para la comunicación de los cambios y de los procedimientos operativos al personal, otras partes interesadas y las personas de contacto pertinentes (por ejemplo, a clientes y proveedores).

El proceso para la terminación o cambio de empleo se recomienda también sea aplicado al personal externo (es decir, proveedores) cuando se produce una terminación del personal, el contrato o el trabajo con la organización, o cuando hay un cambio del trabajo dentro de la organización.

Otros datos

En muchas organizaciones, la función de recursos humanos es generalmente responsable del proceso general de terminación y trabaja junto con el gerente supervisor de la persona en transición para administrar los aspectos de seguridad de la información de los procedimientos relevantes. En el caso del personal proporcionado a través de una parte externa (por ejemplo, a través de un proveedor), este proceso de terminación es llevado a cabo por la parte externa de acuerdo con el contrato entre la organización y la parte externa.

6.6 Acuerdos de confidencialidad o no divulgación

Tipo de control	Propiedades de Seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo	#Confidencialidad	#Proteger	#Seguridad_de_los_recursos_humanos#Protección_de_la_información#Supplier_relationships	#Gobernabilidad_y_Ecosistema

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

Control

Los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la organización para la protección de la información se sugiere sean identificados, documentados, revisados y firmados periódicamente por el personal y otras partes interesadas pertinentes.

Propósito

Mantener la confidencialidad de la información accesible por personal o partes externas.

Orientación

Se recomienda que los acuerdos de confidencialidad o no divulgación aborden el requisito de proteger la información confidencial utilizando términos legalmente exigibles. Los acuerdos de confidencialidad o no divulgación son aplicables a las partes interesadas y al personal de la organización. Sobre la base de los requisitos de seguridad de la información de una organización, se sugiere que los términos de los acuerdos determinen teniendo en cuenta el tipo de información que se maneja, su nivel de clasificación, su uso y el acceso permisible por parte de la otra parte. Para identificar los requisitos para los acuerdos de confidencialidad o no divulgación, se sugiere considerar los siguientes elementos:

a) una definición de la información que se recomienda proteger (por ejemplo, información confidencial);

b) la duración prevista de un acuerdo, incluidos los casos en que pueda ser necesario mantener la confidencialidad indefinidamente o hasta que la información esté a disposición del público;

c) las acciones requeridas cuando se rescinde un acuerdo;

d) las responsabilidades y acciones de los signatarios para evitar la divulgación no autorizada de información;

e) la propiedad de la información, los secretos comerciales y la propiedad intelectual, y cómo se relaciona esto con la protección de la información confidencial;

f) el uso permitido de la información confidencial y los derechos del firmante a utilizar la información;

g) el derecho a auditar y supervisar las actividades que impliquen información confidencial en circunstancias muy delicadas;

h) el proceso de notificación y notificación de la divulgación no autorizada o la fuga de información confidencial;

i) los términos para que la información sea devuelta o destruida al finalizar el acuerdo;

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

j) las medidas previstas que deban adoptarse en caso de incumplimiento del acuerdo.

Es conveniente que la organización tenga en cuenta el cumplimiento de los acuerdos de confidencialidad y no divulgación para la jurisdicción a la que se aplican (ver el inciso 5.31, el inciso 5.32, el inciso 5.33 y el inciso 5.34).

Los requisitos para los acuerdos de confidencialidad y no divulgación se sugiere revisar periódicamente y cuando se produzcan cambios que influyan en estos requisitos.

Otros datos

Los acuerdos de confidencialidad y no divulgación protegen la información de la organización e informan a los signatarios de su responsabilidad de proteger, usar y divulgar la información de manera responsable y autorizada.

6.7 Trabajo remoto

Tipo de control	Propiedades de Seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Gestión_de_activos#Protección_de_la_información#Seguridad_física#Seguridad_de_sistemas_y_redes	#Protección

Control

Se recomienda que las medidas de seguridad se implementen cuando el personal trabaja de forma remota para proteger la información a la que se accede, procesa o almacena fuera de las instalaciones de la organización.

Propósito

Garantizar la seguridad de la información cuando el personal trabaja de forma remota.

Orientación

El trabajo remoto ocurre cuando el personal de la organización trabaja desde una ubicación fuera de las instalaciones de la organización, accediendo a la información ya sea en papel o electrónicamente a través de equipos de TIC. Los entornos de trabajo remoto incluyen aquellos denominados "teletrabajo", "teletrabajo", "lugar de trabajo flexible", "entornos de trabajo virtuales" y "mantenimiento remoto".

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

Nota: Es posible que no todas las recomendaciones de este Proyecto de Norma Mexicana se puedan aplicar debido a la legislación y regulaciones locales en diferentes jurisdicciones.

Las organizaciones que permiten actividades de trabajo remoto se sugiere emitan una política específica sobre el trabajo remoto que defina las condiciones y restricciones relevantes. Se recomienda cuando se considere aplicable, tener en cuenta las siguientes cuestiones:

a) la seguridad física existente o propuesta del lugar de trabajo remoto, teniendo en cuenta la seguridad física de la ubicación y el entorno local, incluidas las diferentes jurisdicciones donde se encuentra el personal;

b) normas y mecanismos de seguridad para el entorno físico remoto, como archivadores con cerradura, transporte seguro entre ubicaciones y normas para el acceso remoto, escritorio transparente, impresión y eliminación de información y otros activos asociados, e informes de eventos de seguridad de la información (ver el inciso 6.8);

c) los entornos físicos de trabajo a distancia previstos;

d) los requisitos de seguridad de las comunicaciones, teniendo en cuenta la necesidad de acceso remoto a los sistemas de la organización, se recomienda la sensibilidad de la información a la que se accede y transmite a través del enlace de comunicación y la sensibilidad de los sistemas y aplicaciones;

e) el uso del acceso remoto, como el acceso a escritorios virtuales, que admite el procesamiento y almacenamiento de información en equipos de propiedad privada;

f) la amenaza de acceso no autorizado a la información o los recursos de otras personas en el lugar de trabajo remoto (por ejemplo, familiares y amigos);

g) la amenaza de acceso no autorizado a información o recursos de otras personas en lugares públicos;

h) el uso de redes domésticas y redes públicas, y los requisitos o restricciones en la configuración de los servicios de redes inalámbricas;

i) uso de medidas de seguridad, como cortafuegos y protección contra malware;

j) mecanismos seguros para desplegar e inicializar sistemas a distancia;

k) mecanismos seguros para la autenticación y habilitación de privilegios de acceso teniendo en cuenta la vulnerabilidad de los mecanismos de autenticación de un solo factor en los que se permite el acceso remoto a la red de la organización.

Las directrices y medidas que se recomienda considerar incluyen:

a) el suministro de equipos y muebles de almacenamiento adecuados para las actividades de trabajo a distancia, cuando no se permita el uso de equipos de propiedad privada que no estén bajo el control de la organización;

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

b) una definición del trabajo permitido, la clasificación de la información que puede conservarse y los sistemas y servicios internos a los que el trabajador remoto está autorizado a acceder;

c) la formación de las personas que trabajan a distancia y las que prestan apoyo. Es conveniente incluir cómo realizar negocios de manera segura mientras se trabaja de forma remota;

d) el suministro de equipos de comunicación adecuados, incluidos los métodos para garantizar el acceso remoto, como los requisitos relativos a los bloqueos de pantalla de los dispositivos y los temporizadores de inactividad; la habilitación del seguimiento de la ubicación del dispositivo; instalación de capacidades de borrado remoto;

e) seguridad física;

f) normas y orientaciones sobre el acceso de la familia y los visitantes al equipo y la información;

g) la prestación de soporte y mantenimiento de hardware y software;

h) la prestación de seguros;

i) los procedimientos de copia de seguridad y continuidad de las actividades;

j) auditoría y supervisión de la seguridad;

k) la revocación de la autoridad y los derechos de acceso y la devolución de los equipos cuando finalicen las actividades de trabajo a distancia.

Otros datos

No hay otra información.

6.8 Informe de eventos de seguridad de la información

Tipo de control	Propiedades de Seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Detectivo	#Confidencialidad #Integridad #Disponibilidad	#Detectar	#Gestión_de_eventos_de_seguridad_de_la_información	#Defensa

Control

Se sugiere que la organización proporcione un mecanismo para que el personal informe oportunamente de los acontecimientos de seguridad de la información observados o sospechosos a través de los canales apropiados.

Propósito

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

Apoyar la presentación oportuna, consistente y efectiva de informes de eventos de seguridad de la información que puedan ser identificados por el personal.

Orientación

Es conveniente que todo el personal y los usuarios sean conscientes de su responsabilidad de informar los eventos de seguridad de la información lo más rápido posible para prevenir o minimizar el efecto de los incidentes de seguridad de la información. Se sugiere conocer el procedimiento para informar de los acontecimientos de seguridad de la información y el punto de contacto al que es conveniente notificar de los acontecimientos. Se recomienda que el mecanismo de presentación de informes sea lo más fácil, accesible y disponible posible. Los eventos de seguridad de la información incluyen incidentes, infracciones y vulnerabilidades.

Las situaciones que se sugiere considerar para la notificación de eventos de seguridad de la información incluyen:

a) controles ineficaces de la seguridad de la información;

b) incumplimiento de las expectativas de confidencialidad, integridad o disponibilidad de la información;

c) errores humanos;

d) el incumplimiento de la política de seguridad de la información, las políticas temáticas específicas o las normas aplicables;

e) violaciones de las medidas de seguridad física;

f) cambios en el sistema que no han pasado por el proceso de gestión del cambio;

g) mal funcionamiento u otro comportamiento anómalo del sistema de software o hardware;

h) violaciones de acceso;

i) vulnerabilidades;

j) sospecha de infección de malware.

Se recomienda advertir al personal y a los usuarios que no intenten probar presuntas vulnerabilidades de seguridad de la información. Las vulnerabilidades de prueba pueden interpretarse como un posible uso indebido del sistema y también pueden causar daños al sistema o servicio de información, y pueden corromper u oscurecer la evidencia digital. En última instancia, esto puede resultar en responsabilidad legal para la persona que realiza la prueba.

Otros datos

Consulte la serie de normas que se indica en el inciso 10.34 para obtener información adicional.

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

7 Controles físicos

7.1 Perímetros de seguridad física

Tipo de control	Propiedades de Seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Seguridad_física	#Protección

Control

Se sugiere que los perímetros de seguridad se definan y utilicen para proteger las áreas que contienen información y otros activos asociados.

Propósito

Para evitar el acceso físico no autorizado, daños e interferencias a la información de la organización y otros activos asociados.

Orientación

Se sugiere que las siguientes directrices se consideren e implementen cuando sea apropiado para los perímetros de seguridad física:

a) definir los perímetros de seguridad y la ubicación y la solidez de cada uno de los perímetros de conformidad con los requisitos de seguridad de la información relacionados con los activos dentro del perímetro;

b) tener perímetros físicamente sólidos para un edificio o emplazamiento que contenga instalaciones de tratamiento de información (es decir, no se recomienda halla huecos en el perímetro o en las zonas en las que pueda producirse fácilmente un robo). Los techos exteriores, paredes, techos y pisos del sitio se sugiere sea de construcción sólida y es conveniente que todas las puertas externas estén adecuadamente protegidas contra el acceso no autorizado con mecanismos de control (por ejemplo, barras, alarmas, cerraduras). Se recomienda que las puertas y ventanas se cierren con llave cuando no están desatendidas y es conveniente considerar la protección externa para las ventanas, particularmente a nivel del suelo; se sugiere considerar los puntos de ventilación;

c) alarmar, monitorear y probar todas las puertas cortafuegos en un perímetro de seguridad junto con las paredes para establecer el nivel requerido de resistencia de acuerdo con las normas adecuadas. Se recomienda funcionar de manera a prueba de fallas.

Otros datos

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

La protección física se puede lograr mediante la creación de una o más barreras físicas alrededor de las instalaciones de la organización y las instalaciones de procesamiento de información.

Un área segura puede ser una oficina con cerradura o varias habitaciones rodeadas por una barrera de seguridad física interna continua. Pueden ser necesarias barreras y perímetros adicionales para controlar el acceso físico entre áreas con diferentes requisitos de seguridad dentro del perímetro de seguridad. Es conveniente que la organización considere tener medidas de seguridad física que puedan fortalecerse durante situaciones de mayor amenaza.

7.2 Entrada física

Tipo de control	Propiedades de Seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas		Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Seguridad_física#Identidad_y_control_de_acceso		#Protección

Control

Se sugiere que las zonas seguras estén protegidas por controles de entrada y puntos de acceso adecuados.

Propósito

Para garantizar que solo se produzca acceso físico autorizado a la información de la organización y otros activos asociados.

Orientación

General

Los puntos de acceso, como las zonas de entrega y carga y otros puntos en los que puedan entrar personas no autorizadas en las instalaciones, se sugiere controlar y, si es posible, aislarse de las instalaciones de procesamiento de información para evitar el acceso no autorizado.

Se recomienda considerar las siguientes pautas:

a) restringir el acceso a sitios y edificios únicamente al personal autorizado. Es conveniente que el proceso para la gestión de los derechos de acceso a las áreas físicas incluya la provisión, revisión periódica, actualización y revocación de autorizaciones (ver el inciso 5.18);

b) mantener y supervisar de forma segura un cuaderno de bitácora físico o una pista de auditoría electrónica de todos los accesos y proteger todos los registros (ver el inciso 5.33) y la información confidencial de autenticación;

c) establecer e implementar un proceso y mecanismos técnicos para la gestión del acceso a las áreas donde se procesa o almacena la información. Los mecanismos

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

de autenticación incluyen el uso de tarjetas de acceso, biometría o autenticación de dos factores, como una tarjeta de acceso y un PIN secreto. Se sugiere considerar puertas de seguridad dobles para el acceso a áreas sensibles;

d) la creación de un área de recepción supervisada por el personal u otros medios para controlar el acceso físico al sitio o edificio;

e) inspeccionar y examinar las pertenencias personales del personal y de las partes interesadas a la entrada y a la salida;

Nota: La legislación y regulaciones locales pueden existir con respecto a la posibilidad de inspeccionar las pertenencias personales.

f) exigir a todo el personal y a las partes interesadas que lleven algún tipo de identificación visible y que notifiquen inmediatamente al personal de seguridad si se encuentran con visitantes sin escolta y a cualquier persona que no lleve una identificación visible. Se recomienda considerar insignias fácilmente distinguibles para identificar mejor a los empleados, proveedores y visitantes permanentes;

g) conceder al personal del proveedor acceso restringido a áreas seguras o instalaciones de procesamiento de información solo cuando sea necesario. Este acceso se sugiere sea autorizado y monitoreado;

h) prestar especial atención a la seguridad del acceso físico en el caso de edificios que posean activos para múltiples organizaciones;

i) diseñar medidas de seguridad física para que puedan reforzarse cuando aumente la probabilidad de incidentes físicos;

j) asegurar otros puntos de entrada, como salidas de emergencia, del acceso no autorizado;

k) establecer un proceso de gestión de llaves para garantizar la gestión de las llaves físicas o la información de autenticación (por ejemplo, códigos de cerradura, cerraduras combinadas a oficinas, habitaciones e instalaciones, como armarios de llaves) y para garantizar un libro de registro o una auditoría anual de llaves y que se controle el acceso a las claves físicas o a la información de autenticación (ver el inciso 5.17 para obtener más orientación sobre la información de autenticación).

Visitantes

Se recomienda considerar las siguientes pautas:

a) autenticar la identidad de los visitantes por un medio adecuado;

b) registrar la fecha y hora de entrada y salida de los visitantes;

c) solo conceder acceso a los visitantes para fines específicos y autorizados y con instrucciones sobre los requisitos de seguridad de la zona y sobre los procedimientos de emergencia;

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

d) supervisar a todos los visitantes, a menos que se conceda una excepción explícita.

Áreas de entrega y carga y material entrante

Se recomienda considerar las siguientes pautas:

a) restringir el acceso a las zonas de entrega y carga desde fuera del edificio al personal identificado y autorizado;

b) diseñar las áreas de entrega y carga para que las entregas puedan cargarse y descargarse sin que el personal de entrega obtenga acceso no autorizado a otras partes del edificio;

c) asegurar las puertas exteriores de las zonas de entrega y carga cuando se abran las puertas de las zonas restringidas;

d) inspeccionar y examinar las entregas entrantes en busca de explosivos, productos químicos u otros materiales peligrosos antes de que se trasladen de las zonas de entrega y carga;

e) registrar las entregas entrantes de conformidad con los procedimientos de gestión de activos (ver el inciso 5.9 y el inciso 7.10) a la entrada en el emplazamiento;

f) segregar físicamente los envíos entrantes y salientes, siempre que sea posible;

g) inspeccionar las entregas entrantes en busca de pruebas de manipulación en el camino. Si se descubre una manipulación, se sugiere informar inmediatamente al personal de seguridad.

Otros datos

No hay otra información.

7.3 Asegurar oficinas, habitaciones e instalaciones

Tipo de control	Propiedades de Seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad#Disponibilidad	#Proteger	#Seguridad_física#Gestión_de_activos	#Protección

Control

Se recomienda que la seguridad física de las oficinas, salas e instalaciones se diseñe e implemente.

Propósito

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

Para evitar el acceso físico no autorizado, daños e interferencias a la información de la organización y otros activos asociados en oficinas, salas e instalaciones.

Orientación

Se sugiere considerar las siguientes pautas para asegurar oficinas, habitaciones e instalaciones:

a) la ubicación de instalaciones críticas para evitar el acceso del público;

b) en su caso, garantizar que los edificios sean discretos y den una indicación mínima de su finalidad, sin signos evidentes, en el exterior o en el interior del edificio, identificando la presencia de actividades de tratamiento de la información;

c) configurar instalaciones para evitar que la información o las actividades confidenciales sean visibles y audibles desde el exterior. El blindaje electromagnético también se recomienda considerar apropiado;

d) no poner a disposición de cualquier persona no autorizada directorios, guías telefónicas internas y mapas accesibles en línea que identifiquen las ubicaciones de las instalaciones de procesamiento de información confidencial.

Otros datos

No hay otra información.

7.4 Supervisión de la seguridad física

Tipo de control	Propiedades de Seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo#Detectivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger #Detectar	#Seguridad_física	#Protección#Defensa

Control

Es conveniente que las instalaciones sean monitoreadas continuamente para detectar accesos físicos no autorizados.

Propósito

Para detectar y disuadir el acceso físico no autorizado.

Orientación

Se recomienda que las instalaciones físicas sean monitoreadas por sistemas de vigilancia, que pueden incluir guardias, alarmas de intrusos, sistemas de monitoreo de video como circuito cerrado de televisión y software de gestión de información de seguridad física administrado internamente o por un proveedor de servicios de monitoreo.

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

El acceso a los edificios que albergan sistemas críticos se sugiere sean monitoreados continuamente para detectar el acceso no autorizado o el comportamiento sospechoso mediante:

a) la instalación de sistemas de videovigilancia, como circuitos cerrados de televisión, para ver y grabar el acceso a zonas sensibles dentro y fuera de las instalaciones de una organización;

b) instalar, de acuerdo con las normas aplicables pertinentes, y probar periódicamente detectores de contacto, sonido o movimiento para activar una alarma de intruso, como:

   1) instalar detectores de contacto que activen una alarma cuando se haga o rompa un contacto en cualquier lugar donde se pueda hacer o romper un contacto (como ventanas y puertas y debajo de objetos) para ser utilizados como alarma de pánico;

   2) detectores de movimiento basados en tecnología infrarroja que activan una alarma cuando un objeto pasa a través de su campo de visión;

   3) la instalación de sensores sensibles al sonido de la rotura de cristales que puedan utilizarse para activar una alarma para alertar al personal de seguridad;

c) utilizar dichas alarmas para cubrir todas las puertas exteriores y ventanas accesibles.

Se sugiere que las áreas desocupadas se alarmen en todo momento; también es conveniente proporcionar cobertura para otras áreas (por ejemplo, salas de computadoras o comunicaciones).

Es conveniente que el diseño de los sistemas de monitoreo se mantenga confidencial porque la divulgación puede facilitar los robos no detectados.

Se recomienda que los sistemas de vigilancia se protejan del acceso no autorizado a fin de evitar que la información de vigilancia, como las fuentes de vídeo, sea accedida por personas no autorizadas o que los sistemas se deshabiliten de forma remota.

El panel de control del sistema de alarma se sugiere se coloque en una zona alarmada y, para alarmas de seguridad, en un lugar que permita una ruta de salida fácil para la persona que configura la alarma. Se recomienda que el panel de control y los detectores tengan mecanismos a prueba de manipulaciones. Es conveniente que el sistema sea probado regularmente para asegurarse de que funciona según lo previsto, especialmente si sus componentes funcionan con baterías.

Cualquier mecanismo de monitoreo y grabación se recomienda utilizar teniendo en cuenta las leyes y regulaciones locales, incluida la legislación de protección de datos y protección de PII, especialmente con respecto al monitoreo del personal y los períodos de retención de video grabado.

Otros datos

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

No hay otra información.

7.5 Protección contra amenazas físicas y ambientales

Tipo de control	Propiedades de Seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Seguridad_física	#Protección

Control

Es conveniente diseñar y aplicarse la protección contra las amenazas físicas y ambientales, como los desastres naturales y otras amenazas físicas intencionales o no intencionales a la infraestructura.

Propósito

Prevenir o reducir las consecuencias de los eventos originados por amenazas físicas y ambientales.

Orientación

Se recomienda que las evaluaciones de riesgos para identificar las posibles consecuencias de las amenazas físicas y ambientales se realicen antes de comenzar las operaciones críticas en un sitio físico y a intervalos regulares. Se sugiere implementar las salvaguardias necesarias y supervisar los cambios en las amenazas. Es conveniente obtener asesoramiento especializado sobre cómo gestionar los riesgos derivados de amenazas físicas y ambientales como incendios, inundaciones, terremotos, explosiones, disturbios civiles, desechos tóxicos, emisiones ambientales y otras formas de desastres naturales o desastres causados por seres humanos.

Se sugiere que la ubicación y la construcción de los locales físicos tengan en cuenta:

a) la topografía local, como la elevación adecuada, las masas de agua y las fallas tectónicas;

b) amenazas urbanas, como lugares con un alto perfil para atraer disturbios políticos, actividades delictivas o ataques terroristas.

Sobre la base de los resultados de la evaluación de riesgos, se recomienda identificar las amenazas físicas y ambientales pertinentes y considerarse los controles apropiados en los siguientes contextos como ejemplos:

a) incendio: instalación y configuración de sistemas capaces de detectar incendios en una fase temprana para enviar alarmas o activar sistemas de extinción de incendios con el fin de evitar daños por incendio en los medios de almacenamiento y en los sistemas de procesamiento de información relacionados. Es conveniente que la extinción de incendios se realice utilizando la sustancia más adecuada con respecto al medio ambiente circundante (por ejemplo, gas en espacios confinados);

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

b) inundación: instalación de sistemas capaces de detectar inundaciones en una fase temprana bajo los suelos de las zonas que contienen medios de almacenamiento o sistemas de tratamiento de la información. Las bombas de agua o medios equivalentes se sugiere estén fácilmente disponibles en caso de que se produzcan inundaciones;

c) sobretensiones eléctricas: adopción de sistemas capaces de proteger los sistemas de información tanto del servidor como de los clientes contra sobretensiones eléctricas o eventos similares para minimizar las consecuencias de tales eventos;

d) explosivos y armas: realización de inspecciones aleatorias para detectar la presencia de explosivos o armas en el personal, los vehículos o las mercancías que entren en las instalaciones de tratamiento de información sensible.

Otros datos

Las cajas fuertes u otras formas de instalaciones de almacenamiento seguras pueden proteger la información almacenada en ellas contra desastres como un incendio, terremoto, inundación o explosión.

Las organizaciones pueden considerar los conceptos de prevención del delito a través del diseño ambiental al diseñar los controles para asegurar su entorno y reducir las amenazas urbanas. Por ejemplo, en lugar de usar bolardos, estatuas o características de agua pueden servir como una característica y una barrera física.

7.6 Trabajar en áreas seguras

Tipo de control	Propiedades de Seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Seguridad_física	#Protección

Control

Se sugiere diseñar e implementar medidas de seguridad para trabajar en áreas seguras.

Propósito

Para proteger la información y otros activos asociados en áreas seguras de daños e interferencias no autorizadas por parte del personal que trabaja en estas áreas.

Orientación

Es conveniente que las medidas de seguridad para trabajar en zonas seguras se apliquen a todo el personal y abarcar todas las actividades que tengan lugar en la zona segura.

Se recomienda considerar las siguientes pautas:

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

a) hacer que el personal solo tenga conocimiento de la existencia de una zona segura o de las actividades que se realicen en ella sobre la base de la necesidad de conocerla;

b) evitar el trabajo no supervisado en zonas seguras, tanto por razones de seguridad como para reducir las posibilidades de actividades maliciosas;

c) bloquear físicamente e inspeccionar periódicamente las zonas seguras vacantes;

d) no permitir equipos fotográficos, de vídeo, de audio u otros equipos de grabación, como cámaras en los dispositivos de punto final del usuario, a menos que esté autorizado;

e) controlar adecuadamente el transporte y el uso de los dispositivos de punto final del usuario en zonas seguras;

f) publicar los procedimientos de emergencia de una manera fácilmente visible o accesible.

Otros datos

No hay otra información.

7.7 Escritorio limpio y pantalla limpia

Tipo de control	Propiedades de Seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo	#Confidencialidad	#Proteger	#Seguridad_física	#Protección

Control

Se recomienda definir y aplicar adecuadamente normas claras de escritorio para papeles y medios de almacenamiento extraíbles y normas de pantalla claras para las instalaciones de procesamiento de información.

Propósito

Reducir los riesgos de acceso no autorizado, pérdida y daño a la información en escritorios, pantallas y en otros lugares accesibles durante y fuera del horario normal de trabajo.

Orientación

Se sugiere que la organización establezca y comunique una política temática específica sobre un escritorio limpio y una pantalla limpia a todas las partes interesadas pertinentes.

Se sugiere considerar las siguientes pautas:

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

a) guardar encerrando información comercial sensible o crítica (por ejemplo, en papel o en medios de almacenamiento electrónicos) (idealmente en una caja fuerte, gabinete u otra forma de mobiliario de seguridad) cuando no sea necesario, especialmente cuando la oficina está desocupada;

b) proteger los dispositivos de punto final del usuario mediante cerraduras de llave u otros medios de seguridad cuando no estén en uso o estén desatendidos;

c) dejar los dispositivos de punto final del usuario desconectados o protegidos con un mecanismo de bloqueo de pantalla y teclado controlado por un mecanismo de autenticación de usuario cuando no están atendidos. Es conveniente que todos los equipos y sistemas se configuren con una función de tiempo de espera o cierre de sesión automático;

d) hacer que el originador recoja inmediatamente las salidas de impresoras o dispositivos multifunción. El uso de impresoras con una función de autenticación, por lo que los originadores son los únicos que pueden obtener sus impresiones y solo cuando están de pie junto a la impresora;

e) almacenar de forma segura documentos y soportes de almacenamiento extraíbles que contengan información sensible y, cuando ya no sea necesario, desecharlos mediante mecanismos de eliminación seguros;

f) establecer y comunicar normas y directrices para la configuración de ventanas emergentes en las pantallas (por ejemplo, desactivar las nuevas ventanas emergentes de correo electrónico y mensajería, si es posible, durante las presentaciones, el uso compartido de la pantalla o en un área pública);

g) borrar información sensible o crítica en pizarras y otros tipos de pantalla cuando ya no sea necesario.

Se sugiere que la organización cuente con procedimientos al desalojar las instalaciones, incluida la realización de un barrido final antes de partir para garantizar que los activos de la organización no se queden atrás (por ejemplo, documentos caídos detrás de cajones o muebles).

Otros datos

No hay otra información.

7.8 Emplazamiento y protección de equipos

Tipo de control	Propiedades de Seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Seguridad_física#Gestión_de_activos	#Protección

Control

Se sugiere que el equipo este ubicado de forma segura y protegida.

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

Propósito

Reducir los riesgos de las amenazas físicas y ambientales, y del acceso no autorizado y los daños.

Orientación

Se recomienda considerar las siguientes pautas para proteger el equipo:

a) emplazamiento de equipos para minimizar el acceso innecesario a las zonas de trabajo y evitar el acceso no autorizado;

b) posicionar cuidadosamente las instalaciones de procesamiento de información que manejan datos confidenciales para reducir el riesgo de que la información sea vista por personas no autorizadas durante su uso;

c) adoptar controles para minimizar el riesgo de posibles amenazas físicas y medioambientales [por ejemplo, robo, incendio, explosivos, humo, agua (o falla en el suministro de agua), polvo, vibraciones, efectos químicos, interferencias en el suministro eléctrico, interferencias en las comunicaciones, radiación electromagnética y vandalismo];

d) establecer directrices para comer, beber y fumar en las proximidades de las instalaciones de tratamiento de la información;

e) el seguimiento de las condiciones ambientales, como la temperatura y la humedad, en busca de condiciones que puedan afectar negativamente al funcionamiento de las instalaciones de tratamiento de la información;

f) aplicar protección contra rayos a todos los edificios y colocar filtros de protección contra rayos en todas las líneas eléctricas y de comunicaciones entrantes;

g) considerar el uso de métodos de protección especiales, como membranas de teclado, para equipos en entornos industriales;

h) proteger los equipos que procesan información confidencial para minimizar el riesgo de fuga de información debido a la emanación electromagnética;

i) separar físicamente las instalaciones de procesamiento de información administradas por la organización de las no administradas por la organización.

Otros datos

No hay otra información.

7.9 Seguridad de los bienes fuera de las instalaciones

Tipo de control	Propiedades de Seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Seguridad_física#Gestión_de_activos	#Protección

Control

Es conveniente que los activos fuera del sitio estén protegidos.

Propósito

Para evitar la pérdida, daño, robo o compromiso de dispositivos fuera del sitio y la interrupción de las operaciones de la organización.

Orientación

Cualquier dispositivo utilizado fuera de las instalaciones de la organización que almacene o procese información (por ejemplo--, dispositivo móvil), incluidos los dispositivos propiedad de la organización y los dispositivos de propiedad privada y utilizados en nombre de la organización [traiga su propio dispositivo (BYOD)] necesita protección. Se recomienda que el uso de estos dispositivos sea autorizado por la administración.

Se sugiere considerar las siguientes pautas para la protección de los dispositivos que almacenan o procesan información fuera de las instalaciones de la organización:

a) no dejar desatendidos los equipos y los medios de almacenamiento retirados de las instalaciones en lugares públicos y no seguros;

b) observar las instrucciones de los fabricantes para proteger los equipos en todo momento (por ejemplo, protección contra la exposición a campos electromagnéticos fuertes, agua, calor, humedad, polvo);

c) cuando el equipo fuera de las instalaciones se transfiera entre diferentes personas o partes interesadas, manteniendo un registro que defina la cadena de custodia del equipo, incluidos al menos los nombres y organizaciones de los responsables del equipo. La información que no necesita ser transferida con el activo es conveniente se elimine de forma segura antes de la transferencia;

d) cuando sea necesario y práctico, exigir autorización para que el equipo y los medios se retiren de las instalaciones de la organización y llevar un registro de dichas mudanzas a fin de mantener una pista de auditoría (ver el inciso 5.14);

e) la protección contra la visualización de información en un dispositivo (por ejemplo, móvil o portátil) en el transporte público, y los riesgos asociados con la navegación por los hombros;

f) implementar el seguimiento de la ubicación y la capacidad de borrado remoto de dispositivos.

La instalación permanente de equipos fuera de las instalaciones de la organización [como antenas y cajeros automáticos (ATM)] puede estar sujeta a un mayor riesgo de daños, robo o escuchas. Estos riesgos pueden variar considerablemente entre ubicaciones y se sugiere tener en cuenta al determinar las medidas más apropiadas.

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

Se sugiere considerar las siguientes pautas al ubicar este equipo fuera de las instalaciones de la organización:

a) supervisión de la seguridad física (ver el inciso 7.4);

b) la protección contra las amenazas físicas y medioambientales (ver el inciso 7.5);

c) controles de acceso físico y a prueba de manipulaciones;

d) controles lógicos de acceso.

Otros datos

Puede encontrar más información sobre otros aspectos de la protección de los equipos de almacenamiento y procesamiento de información y los dispositivos de punto final del usuario en el inciso 8.1 y el inciso 6.7.

7.10 Medios de almacenamiento

Tipo de control	Propiedades de Seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Seguridad_física#Gestión_de_activos	#Protección

Control

Se recomienda que los medios de almacenamiento se gestionen a lo largo de su ciclo de vida de adquisición, uso, transporte y eliminación de acuerdo con el esquema de clasificación y los requisitos de manipulación de la organización.

Propósito

Para garantizar solo la divulgación, modificación, eliminación o destrucción autorizadas de la información en los medios de almacenamiento.

Orientación

Medios de almacenamiento extraíbles

Se recomienda considerar las siguientes pautas para la administración de medios de almacenamiento extraíbles:

a) establecer una política específica del tema sobre la gestión de los medios de almacenamiento extraíbles y comunicar dicha política específica del tema a cualquier persona que utilice o maneje medios de almacenamiento extraíbles;

b) cuando sea necesario y práctico, exigir autorización para que los medios de almacenamiento se retiren de la organización y mantener un registro de dichas eliminaciones a fin de mantener una pista de auditoría;

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

c) almacenar todos los medios de almacenamiento en un entorno seguro y protegido de acuerdo con su clasificación de la información y protegerlos contra las amenazas medioambientales (como el calor, la humedad, la humedad, el campo electrónico o el envejecimiento), de conformidad con las especificaciones de los fabricantes;

d) si la confidencialidad o la integridad de la información son consideraciones importantes, utilizar técnicas criptográficas para proteger la información en medios de almacenamiento extraíbles;

e) mitigar el riesgo de degradación de los medios de almacenamiento mientras la información almacenada sigue siendo necesaria, transfiriendo la información a nuevos medios de almacenamiento antes de que se vuelva ilegible;

f) almacenar múltiples copias de información valiosa en medios de almacenamiento separados para reducir aún más el riesgo de daños o pérdidas de información casual;

g) considerar el registro de medios de almacenamiento extraíbles para limitar la posibilidad de pérdida de información;

h) solo habilitar puertos de medios de almacenamiento extraíbles [por ejemplo, ranuras para tarjetas digitales seguras (SD) y puertos de bus serie universal (USB)] si existe una razón organizativa para su uso;

i) cuando sea necesario utilizar medios de almacenamiento extraíbles, supervisar la transferencia de información a dichos medios de almacenamiento;

j) la información puede ser vulnerable al acceso no autorizado, al uso indebido o a la corrupción durante el transporte físico, por ejemplo, cuando se envían medios de almacenamiento a través del servicio postal o a través de mensajería.

En este control, los medios incluyen documentos en papel. Al transferir medios de almacenamiento físicos, aplique las medidas de seguridad en el inciso 5.14.

Reutilización o eliminación segura

Se recomienda establecer procedimientos para la reutilización o eliminación seguras de los medios de almacenamiento a fin de reducir al mínimo el riesgo de fuga de información confidencial a personas no autorizadas. Los procedimientos para la reutilización o eliminación seguras de los soportes de almacenamiento que contengan información confidencial se sugiere ser proporcionales a la sensibilidad de dicha información. Se recomienda considerar los siguientes elementos:

a) si es necesario reutilizar dentro de la organización los medios de almacenamiento que contengan información confidencial, eliminar de forma segura los datos o formatear los medios de almacenamiento antes de su reutilización (ver el inciso 8.10);

b) eliminar los medios de almacenamiento que contengan información confidencial de forma segura cuando ya no sean necesarios (por ejemplo, destruyendo, triturando o eliminando de forma segura el contenido);

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

c) disponer de procedimientos para identificar los artículos que pueden requerir una eliminación segura;

d) muchas organizaciones ofrecen servicios de recogida y eliminación de medios de almacenamiento. Se recomienda tener cuidado al seleccionar un proveedor externo adecuado con controles y experiencia adecuados;

e) registrar la eliminación de elementos sensibles con el fin de mantener una pista de auditoría;

f) al acumular medios de almacenamiento para su eliminación, teniendo en cuenta el efecto de agregación, que puede hacer que una gran cantidad de información no sensible se vuelva sensible.

Se recomienda realizar una evaluación del riesgo en los dispositivos dañados que contengan datos confidenciales para determinar si los artículos se destruyen físicamente en lugar de enviarse para su reparación o desecharse (ver el inciso 7.14).

Otros datos

Cuando la información confidencial sobre los medios de almacenamiento no está encriptada, se sugiere considerar la protección física adicional de los medios de almacenamiento.

7.11 Servicios públicos de apoyo

Tipo de control	Propiedades de Seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo #Detectivo	#Integridad #Disponibilidad	#Proteger #Detectar	#Seguridad_física	#Protección

Control

Las instalaciones de procesamiento de información deberían estar protegidas de fallas de energía y otras interrupciones causadas por fallas en los servicios públicos de soporte.

Propósito

Para evitar la pérdida, daño o compromiso de la información y otros activos asociados, o la interrupción de las operaciones de la organización debido a fallas e interrupciones de los servicios públicos de soporte.

Orientación

Las organizaciones dependen de los servicios públicos (por ejemplo, electricidad, telecomunicaciones, suministro de agua, gas, alcantarillado, ventilación y aire acondicionado) para apoyar sus instalaciones de procesamiento de información. Por lo tanto, es conveniente que la organización:

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

a) garantice que los equipos de apoyo a las empresas de servicios públicos estén configurados, operados y mantenidos de conformidad con las especificaciones del fabricante pertinente;

b) garanticen que las empresas de servicios públicos se evalúen periódicamente por su capacidad para satisfacer el crecimiento empresarial y las interacciones con otras empresas de servicios públicos de apoyo;

c) garanticen que los equipos que dan soporte a las empresas de servicios públicos sean inspeccionados y probados periódicamente para garantizar su correcto funcionamiento;

d) si es necesario, activar alarmas para detectar el mal funcionamiento de los servicios públicos;

e) si es necesario, asegúrese de que las empresas de servicios públicos tengan múltiples fuentes con enrutamiento físico diverso;

f) garanticen que los equipos que dan soporte a las empresas de servicios públicos estén en una red separada de las instalaciones de tratamiento de la información si están conectados a una red;

g) garanticen que los equipos que dan soporte a las empresas de servicios públicos estén conectados a Internet solo cuando sea necesario y solo de forma segura.

Se recomienda proporcionar iluminación de emergencia y comunicaciones. Se sugiere que los interruptores y válvulas de emergencia para cortar la energía, el agua, el gas u otros servicios públicos se ubiquen cerca de las salidas de emergencia o las salas de equipos. Es conveniente que los datos de contacto de emergencia se registren y estén disponibles para el personal en caso de una interrupción.

Otros datos

Se puede obtener redundancia adicional para la conectividad de red mediante múltiples rutas de más de un proveedor de servicios públicos.

7.12 Seguridad del cableado

Tipo de control	Propiedades de Seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo	#Confidencialidad #Disponibilidad	#Proteger	#Seguridad_física	#Protección

Control

Los cables que transportan energía, datos o servicios de información de apoyo deberían estar protegidos contra interceptaciones, interferencias o daños.

Propósito

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

Para evitar la pérdida, daño, robo o compromiso de la información y otros activos asociados y la interrupción de las operaciones de la organización relacionadas con el cableado de energía y comunicaciones.

Orientación

Se recomienda considerar las siguientes pautas para la seguridad del cableado:

a) las líneas eléctricas y de telecomunicaciones en las instalaciones de tratamiento de la información subterráneas cuando sea posible, o sujetas a una protección alternativa adecuada, como el protector de cables de suelo y el poste de servicios públicos; si los cables están bajo tierra, protegiéndolos de cortes accidentales (por ejemplo, con conductos blindados o señales de presencia);

b) separar los cables de alimentación de los cables de comunicaciones para evitar interferencias;

c) en el caso de los sistemas sensibles o críticos, otros controles a tener en cuenta incluyen:

   1) instalación de conductos blindados y habitaciones o cajas cerradas y alarmas en los puntos de inspección y terminación;

   2) uso de blindaje electromagnético para proteger los cables;

   3) barridos técnicos periódicos e inspecciones físicas para detectar dispositivos no autorizados conectados a los cables;

   4) acceso controlado a paneles de conexión y salas de cables (por ejemplo, con llaves mecánicas o PIN);

   5) uso de cables de fibra óptica;

d) etiquetar los cables en cada extremo con suficientes detalles de origen y destino para permitir la identificación física y la inspección del cable.

Se sugiere buscar asesoramiento especializado sobre cómo gestionar los riesgos derivados de incidentes de cableado o mal funcionamiento.

Otros datos

A veces, el cableado de energía y telecomunicaciones son recursos compartidos para más de una organización que ocupa locales ubicados conjuntamente.

7.13 Mantenimiento de equipos

Tipo de control	Propiedades de Seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Seguridad_física#Gestión_de_activos	#Protección#Resiliencia

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

Control

Se recomienda que el equipo se mantenga correctamente para garantizar la disponibilidad, integridad y confidencialidad de la información.

Propósito

Evitar la pérdida, daño, robo o compromiso de la información y otros activos asociados y la interrupción de las operaciones de la organización causada por la falta de mantenimiento.

Orientación

Se sugiere considerar las siguientes pautas para el mantenimiento del equipo:

a) mantener el equipo de acuerdo con la frecuencia de servicio y las especificaciones recomendadas por el proveedor;

b) la aplicación y el seguimiento de un programa de mantenimiento por parte de la organización;

c) solo personal de mantenimiento autorizado que realice reparaciones y mantenimiento de equipos;

d) mantener registros de todas las fallas sospechosas o reales, y de todo el mantenimiento preventivo y correctivo;

e) implementar controles apropiados cuando el equipo esté programado para el mantenimiento, teniendo en cuenta si este mantenimiento es realizado por personal en el sitio o externo a la organización; someter al personal de mantenimiento a un acuerdo de confidencialidad adecuado;

f) supervisar al personal de mantenimiento cuando se realiza el mantenimiento in situ;

g) autorizar y controlar el acceso para el mantenimiento remoto;

h) la aplicación de medidas de seguridad para los activos fuera de las instalaciones (ver el inciso 7.9) si el equipo que contiene información se retira de las instalaciones para su mantenimiento;

i) cumplir con todos los requisitos de mantenimiento impuestos por el seguro;

j) antes de volver a poner en funcionamiento el equipo después del mantenimiento, inspeccionarlo para asegurarse de que el equipo no ha sido manipulado y funciona correctamente;

k) aplicar medidas para la eliminación o reutilización segura de los equipos (ver el inciso 7.14) si se recomienda determinar que los equipos se eliminan.

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

Otros datos

El equipo incluye componentes técnicos de instalaciones de procesamiento de información, fuente de alimentación ininterrumpida (UPS) y baterías, generadores de energía, alternadores y convertidores de energía, sistemas físicos de detección de intrusos y alarmas, detectores de humo, extintores de incendios, aire acondicionado y ascensores.

7.14 Eliminación o reutilización segura del equipo

Tipo de control	Propiedades de Seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo	#Confidencialidad	#Proteger	#Seguridad_física#Gestión_de_activos	#Protección

Control

Los equipos que contengan medios de almacenamiento se sugiere verificar para garantizar que los datos confidenciales y el software con licencia se hayan eliminado o sobrescrito de forma segura antes de su eliminación o reutilización.

Propósito

Para evitar fugas de información de los equipos que se eliminan o reutilizan.

Orientación

Se recomienda que el equipo se verifique para garantizar si los medios de almacenamiento están contenidos antes de su eliminación o reutilización.

Los medios de almacenamiento que contengan información confidencial o protegida por derechos de autor es conveniente se destruyan físicamente o se sugiere que la información se destruya, elimine o sobrescriba utilizando técnicas para que la información original no sea recuperable en lugar de utilizar la función de eliminación estándar. Consulte el inciso 7.10 para obtener orientación detallada sobre la eliminación segura de los medios de almacenamiento y el inciso 8.10 para obtener orientación sobre la eliminación de información.

Es conveniente que las etiquetas y marcas que identifiquen a la organización o que indiquen la clasificación, el propietario, el sistema o la red se eliminen antes de la eliminación, incluida la reventa o la donación a organizaciones benéficas.

Se sugiere que la organización considere la eliminación de los controles de seguridad, como los controles de acceso o el equipo de vigilancia al final del contrato de arrendamiento o al mudarse de las instalaciones. Esto depende de factores como:

a) su contrato de arrendamiento para devolver la instalación a su estado original;

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

b) minimizar el riesgo de dejar los sistemas con información confidencial sobre ellos para el próximo inquilino (por ejemplo, listas de acceso de usuarios, archivos de vídeo o imagen);

c) la capacidad de reutilizar los controles en la siguiente instalación.

Otros datos

Se recomienda que los equipos dañados que contienen medios de almacenamiento pueden requerir una evaluación de riesgos para determinar si los artículos se destruyen físicamente en lugar de enviarse para su reparación o desecharse. La información puede verse comprometida a través de la eliminación descuidada o la reutilización del equipo.

Además de la eliminación segura del disco, el cifrado de disco completo reduce el riesgo de divulgación de información confidencial cuando el equipo se elimina o se vuelve a implementar, siempre que:

a) el proceso de cifrado es lo suficientemente fuerte y cubre todo el disco (incluido el espacio de holgura, los archivos de intercambio);

b) las claves criptográficas son lo suficientemente largas como para resistir ataques de fuerza bruta;

c) las claves criptográficas se mantienen confidenciales (por ejemplo, nunca se almacenan en el mismo disco).

Para más información sobre criptografía, ver el inciso 8.24.

Las técnicas para sobrescribir de forma segura los medios de almacenamiento difieren según la tecnología de medios de almacenamiento y el nivel de clasificación de la información en los medios de almacenamiento. Se sugiere que las herramientas de sobreescritura se revisen para asegurarse de que son aplicables a la tecnología de los medios de almacenamiento.

Consulte la norma que se indica en el inciso 10.39 para obtener detalles sobre los métodos para desinfectar los medios de almacenamiento.

8 Controles tecnológicos

8.1 Dispositivos de punto final de usuario

Tipo de control	Propiedades de Seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Gestión_de_activos#Protección_de_la_información	#Protección

Nota: Los dispositivos de punto final de usuario son conocidos en inglés como "endpoint devices".

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

Control

La información almacenada, procesada o accesible a través de los dispositivos de punto final del usuario es conveniente este protegida.

Propósito

Proteger la información contra los riesgos introducidos mediante el uso de dispositivos de punto final de usuario.

Orientación

General

Se recomienda que la organización establezca una directiva específica del tema sobre la configuración y el manejo seguros de los dispositivos de punto final del usuario. Se sugiere que la política específica del tema se comunique a todo el personal pertinente y considerar lo siguiente:

a) el tipo de información y el nivel de clasificación que los dispositivos de punto final del usuario pueden manejar, procesar, almacenar o admitir;

b) registro de dispositivos de punto final de usuario;

c) requisitos de protección física;

d) restricción de la instalación de software (por ejemplo, controlado a distancia por administradores de sistemas);

e) requisitos para el software del dispositivo de punto final del usuario (incluidas las versiones de software) y para la aplicación de actualizaciones (por ejemplo, actualización automática activa);

f) normas para la conexión a servicios de información, redes públicas o cualquier otra red fuera de las instalaciones (por ejemplo, que requieran el uso de cortafuegos personales);

g) controles de acceso;

h) cifrado de dispositivos de almacenamiento;

i) protección contra malware;

j) desactivación, eliminación o bloqueo remotos;

k) copias de seguridad;

l) uso de servicios web y aplicaciones web;

m) análisis del comportamiento del usuario final (ver el inciso 8.16);

n) el uso de dispositivos extraíbles, incluidos los dispositivos de memoria extraíbles, y la posibilidad de deshabilitar los puertos físicos (por ejemplo, puertos USB);

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

o) el uso de capacidades de partición, si son compatibles con el dispositivo de punto final del usuario, que pueden separar de forma segura la información de la organización y otros activos asociados (por ejemplo, software) de otra información y otros activos asociados en el dispositivo.

Se recomienda considerar si cierta información es tan sensible que solo se puede acceder a ella a través de dispositivos de punto final del usuario, pero no almacenarla en dichos dispositivos. En tales casos, se pueden requerir salvaguardas técnicas adicionales en el dispositivo. Por ejemplo, asegurarse de que la descarga de archivos para trabajar sin conexión esté deshabilitada y que el almacenamiento local, como la tarjeta SD, esté deshabilitado.

En la medida de lo posible, las recomendaciones sobre este control son convenientes se apliquen a través de la gestión de la configuración (ver el inciso 8.9) o herramientas automatizadas.

Responsabilidad del usuario

Es conveniente que todos los usuarios sean conscientes de los requisitos y procedimientos de seguridad para proteger los dispositivos de punto final del usuario, así como de sus responsabilidades para implementar dichas medidas de seguridad. Se recomienda aconsejar a los usuarios que:

a) cierren la sesión activa y finalicen los servicios cuando ya no sean necesarios;

b) protejan los dispositivos de punto final del usuario del uso no autorizado con un control físico (por ejemplo bloqueos especiales) y control lógico (por ejemplo, acceso con contraseña) cuando no estén en uso; no dejar desatendidos los dispositivos que transportan información empresarial importante, sensible o crítica;

c) utilicen dispositivos con especial cuidado en lugares públicos, oficinas abiertas, lugares de reunión y otras zonas desprotegidas (por ejemplo, evitar la lectura de información confidencial si las personas pueden leer desde atrás, utilizar filtros de pantalla de privacidad);

d) protejan físicamente los dispositivos de punto final del usuario contra robos (por ejemplo, en automóviles y otras formas de transporte, habitaciones de hotel, centros de conferencias y lugares de reunión).

Se sugiere establecer un procedimiento específico que tenga en cuenta los requisitos legales, legales, reglamentarios, contractuales (incluidos los seguros) y otros requisitos de seguridad de la organización para los casos de robo o pérdida de dispositivos de punto final del usuario.

Uso de dispositivos personales

Cuando la organización permite el uso de dispositivos personales (a veces conocidos como BYOD), además de la orientación dada en este control, se debería considerar lo siguiente:

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

a) la separación del uso personal y empresarial de los dispositivos, incluido el uso de software para respaldar dicha separación y proteger los datos comerciales en un dispositivo privado;

b) proporcionar acceso a la información comercial solo después de que los usuarios hayan reconocido sus deberes (protección física, actualización de software, etc.), renunciando a la propiedad de los datos comerciales, permitiendo la eliminación remota de datos por parte de la organización en caso de robo o pérdida del dispositivo o cuando ya no esté autorizada para usar el servicio. En tales casos, es conveniente considerar la legislación de protección de la PII;

c) políticas y procedimientos específicos sobre temas específicos para prevenir controversias relativas a los derechos de propiedad intelectual desarrollados sobre equipos de propiedad privada;

d) el acceso a equipos de propiedad privada (para verificar la seguridad de la máquina o durante una investigación), que pueden ser impedidos por la legislación;

e) acuerdos de licencia de software que sean tales que las organizaciones puedan ser responsables de la concesión de licencias de software cliente en dispositivos de punto final de usuario propiedad privada del personal o usuarios externos.

Conexiones inalámbricas

Se recomienda que la organización establezca procedimientos para:

a) la configuración de las conexiones inalámbricas en los dispositivos (por ejemplo, la desactivación de protocolos vulnerables);

b) utilizar conexiones inalámbricas o por cable con el ancho de banda adecuado de acuerdo con las políticas específicas del tema pertinente (por ejemplo, porque se necesitan copias de seguridad o actualizaciones de software).

Otros datos

Los controles para proteger la información en los dispositivos de punto final de usuario dependen de si el dispositivo de extremo de usuario se usa solo dentro de las instalaciones seguras y las conexiones de red de la organización, o si está expuesto a un aumento de las amenazas físicas y relacionadas con la red fuera de la organización. Las conexiones inalámbricas para los dispositivos de punto final de usuario son similares a otros tipos de conexiones de red, pero tienen diferencias importantes que deberían tenerse en cuenta al identificar los controles. En particular, la copia de seguridad de la información almacenada en los dispositivos de punto final del usuario a veces puede fallar debido al ancho de banda de red limitado o porque los dispositivos de punto final del usuario no están conectados en los momentos en que se programan las copias de seguridad.

Para algunos puertos USB, como USB-C, no es posible deshabilitar el puerto USB porque se utiliza para otros fines (por ejemplo, entrega de energía y salida de pantalla).

8.2 Derechos de acceso privilegiado

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

Tipo de control	Propiedades de Seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Identidad_y_control_de_acceso	#Protección

Control

La asignación y el uso de los derechos de acceso privilegiado deberían restringirse y gestionarse.

Propósito

Para garantizar que solo los usuarios autorizados, los componentes y servicios de software cuenten con derechos de acceso privilegiados.

Orientación

La asignación de derechos de acceso privilegiado se sugiere controlar mediante un proceso de autorización de conformidad con la política pertinente sobre control de acceso (ver el inciso 5.15). Se recomienda considerar lo siguiente:

a) identificar a los usuarios que necesitan derechos de acceso privilegiados para cada sistema o proceso (por ejemplo, sistemas operativos, sistemas de gestión de bases de datos y aplicaciones);

b) asignar derechos de acceso privilegiado a los usuarios según sea necesario y evento por evento, de conformidad con la política específica sobre control de acceso (ver el inciso 5.15) (es decir, solo a personas con la competencia necesaria para llevar a cabo actividades que requieran acceso privilegiado y sobre la base del requisito mínimo para sus funciones funcionales);

c) mantener un proceso de autorización (es decir, determinar quién puede aprobar los derechos de acceso privilegiado o no conceder derechos de acceso privilegiado hasta que se complete el proceso de autorización) y un registro de todos los privilegios asignados;

d) definir y aplicar los requisitos para la expiración de los derechos de acceso privilegiado;

e) la adopción de medidas para garantizar que los usuarios conozcan sus derechos de acceso privilegiado y cuando se encuentren en modo de acceso privilegiado. Las posibles medidas incluyen el uso de identidades de usuario específicas, configuraciones de interfaz de usuario o incluso equipos específicos;

f) los requisitos de autenticación para los derechos de acceso privilegiado pueden ser superiores a los requisitos para los derechos de acceso normales. La re-autenticación o el aumento de la autenticación pueden ser necesarios antes de trabajar con derechos de acceso privilegiados;

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

g) revisar periódicamente, y después de cualquier cambio organizativo, a los usuarios que trabajan con derechos de acceso privilegiados con el fin de verificar si sus deberes, funciones, responsabilidades y competencias siguen calificándolos para trabajar con derechos de acceso privilegiado (ver el inciso 5.18);

h) establecer reglas específicas para evitar el uso de ID de usuario de administración genéricos (como "root"), en función de las capacidades de configuración de los sistemas. Gestión y protección de la información de autenticación de dichas identidades (ver el inciso 5.17);

i) conceder acceso privilegiado temporal solo durante el período de tiempo necesario para implementar cambios o actividades aprobados (por ejemplo, para actividades de mantenimiento o algunos cambios críticos), en lugar de otorgar permanentemente derechos de acceso privilegiado. Esto a menudo se conoce como procedimiento de rotura de vidrio, y a menudo se automatiza mediante tecnologías de administración de acceso de privilegios;

j) registrar todo el acceso privilegiado a los sistemas con fines de auditoría;

k) no compartir ni vincular identidades con derechos de acceso privilegiado a varias personas, asignando a cada persona una identidad separada que permita asignar derechos de acceso privilegiados específicos. Las identidades se pueden agrupar (por ejemplo, definiendo un grupo de administradores) para simplificar la gestión de los derechos de acceso privilegiado;

l) utilizando únicamente identidades con derechos de acceso privilegiado para realizar tareas administrativas y no para tareas generales cotidianas [es decir, comprobar el correo electrónico, acceder a la web (se sugiere que los usuarios tengan una identidad de red normal separada para estas actividades)].

Otros datos

Los derechos de acceso privilegiado son derechos de acceso proporcionados a una identidad, un rol o un proceso que permite la realización de actividades que los usuarios o procesos típicos no pueden realizar. Los roles de administrador del sistema suelen requerir derechos de acceso privilegiados.

El uso inadecuado de los privilegios de administrador del sistema (cualquier característica o instalación de un sistema de información que permita al usuario anular los controles del sistema o de la aplicación) es un factor importante que contribuye a las fallas o infracciones de los sistemas.

Se puede encontrar más información relacionada con la gestión del acceso y la gestión segura del acceso a la información y los recursos de las tecnologías de la información y las comunicaciones en la norma que se indica en el inciso 10.46.

8.3 Restricción de acceso a la información

Tipo de control	Propiedades de Seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Identidad_y_control_de_acceso	#Protección

Control

El acceso a la información y otros activos asociados se recomienda restringir de conformidad con la política de control de acceso sobre temas específicos establecidos.

Propósito

Para garantizar solo el acceso autorizado y evitar el acceso no autorizado a la información y otros activos asociados.

Orientación

El acceso a la información y otros activos asociados es conveniente restringir de acuerdo con las políticas específicas del tema establecidas. Se recomienda tener en cuenta lo siguiente para respaldar los requisitos de restricción de acceso:

a) no permitir el acceso a información sensible por identidades de usuario desconocidas o de forma anónima. El acceso público o anónimo solo es conveniente concederse a las ubicaciones de almacenamiento que no contengan información confidencial;

b) proporcionar mecanismos de configuración para controlar el acceso a la información en sistemas, aplicaciones y servicios;

c) controlar a qué datos puede acceder un usuario determinado;

d) controlar qué identidades o grupo de identidades tienen a qué acceso, como leer, escribir, eliminar y ejecutar;

e) proporcionar controles de acceso físicos o lógicos para el aislamiento de aplicaciones, datos de aplicaciones o sistemas confidenciales.

Además, las técnicas y procesos de administración de acceso dinámico para proteger la información confidencial que tiene un alto valor para la organización se sugiere considerar cuando la organización:

a) necesita un control granular sobre quién puede acceder a dicha información durante qué período y de qué manera;

b) quiere compartir dicha información con personas ajenas a la organización y mantener el control sobre quién puede acceder a ella;

c) desea gestionar dinámicamente, en tiempo real, el uso y la distribución de dicha información;

d) quiere proteger dicha información contra cambios, copias y distribuciones no autorizadas (incluida la impresión);

e) desea supervisar el uso de la información;

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

f) desea registrar cualquier cambio en dicha información que tenga lugar en caso de que se requiera una investigación futura.

Las técnicas de gestión dinámica del acceso se recomienda proteger la información a lo largo de todo su ciclo de vida (es decir, creación, procesamiento, almacenamiento, transmisión y eliminación), incluyendo:

a) establecer normas sobre la gestión del acceso dinámico sobre la base de casos de uso específicos teniendo en cuenta:

1) conceder permisos de acceso basados en la identidad, el dispositivo, la ubicación o la aplicación;

2) aprovechar el sistema de clasificación para determinar qué información es conveniente proteger con técnicas dinámicas de gestión del acceso;

b) establecer procesos operativos, de seguimiento y de presentación de informes y una infraestructura técnica de apoyo.

Los sistemas dinámicos de gestión del acceso se sugiere proteger la información mediante:

a) requerir autenticación, credenciales apropiadas o un certificado para acceder a la información;

b) restringir el acceso, por ejemplo, a un plazo determinado (por ejemplo, después de una fecha determinada o hasta una fecha determinada);

c) utilizar el cifrado para proteger la información;

d) definir los permisos de impresión de la información;

e) registrar quién accede a la información y cómo se utiliza;

f) generar alertas si se detectaran intentos de uso indebido de la información.

Otros datos

Las técnicas de administración de acceso dinámico y otras tecnologías dinámicas de protección de la información pueden respaldar la protección de la información incluso cuando los datos se comparten más allá de la organización de origen, donde los controles de acceso tradicionales no se pueden aplicar. Se puede aplicar a documentos, correos electrónicos u otros archivos que contengan información para limitar quién puede acceder al contenido y de qué manera. Puede ser a nivel granular y adaptarse a lo largo del ciclo de vida de la información.

Las técnicas de administración de acceso dinámico no reemplazan la administración de acceso clásica [por ejemplo, el uso de listas de control de acceso (ACL)], pero pueden agregar más factores para la condicionalidad, la evaluación en tiempo real, la reducción de datos justo a tiempo y otras mejoras que pueden ser útiles para la información más confidencial. Ofrece una forma de controlar el acceso fuera del entorno de la organización. La respuesta a incidentes puede ser compatible con técnicas de

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

administración de acceso dinámico, ya que los permisos se pueden modificar o revocar en cualquier momento.

En la norma que se indica en el inciso 10.46 se proporciona información adicional sobre un marco para la gestión del acceso.

8.4 Acceso al código fuente

Tipo de control	Propiedades de Seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Identidad_y_control_de_acceso #Seguridad_de_aplicaciones#Configuración_segura	#Protección

Control

Se recomienda que el acceso de lectura y escritura al código fuente, las herramientas de desarrollo y las bibliotecas de software se administren adecuadamente.

Propósito

Para evitar la introducción de funcionalidades no autorizadas, evitar cambios involuntarios o maliciosos y mantener la confidencialidad de la propiedad intelectual valiosa.

Orientación

El acceso al código fuente y a los elementos asociados (como diseños, especificaciones, planes de verificación y planes de validación) y a las herramientas de desarrollo (por ejemplo, compiladores, constructores, herramientas de integración, plataformas de prueba y entornos) debería controlarse estrictamente.

Para el código fuente, esto se puede lograr controlando el almacenamiento central de dicho código, preferiblemente en el sistema de administración del código fuente.

El acceso de lectura y el acceso de escritura al código fuente pueden diferir según el rol del personal. Por ejemplo, el acceso de lectura al código fuente se puede proporcionar ampliamente dentro de la organización, pero el acceso de escritura al código fuente solo está disponible para el personal con privilegios o los propietarios designados. Cuando varios desarrolladores dentro de una organización utilizan componentes de código, se recomienda implementar el acceso de lectura a un repositorio de código centralizado. Además, si se utiliza código de código abierto o componentes de código de terceros dentro de una organización, se puede proporcionar acceso de lectura a dichos repositorios de código externo de manera amplia. Sin embargo, se sugiere que el acceso de escritura aún este restringido.

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

Se recomienda considerar las siguientes directrices para controlar el acceso a las bibliotecas de origen de los programas a fin de reducir la posibilidad de corrupción de los programas informáticos:

a) gestionar el acceso al código fuente del programa y a las bibliotecas fuente del programa de acuerdo con los procedimientos establecidos;

b) conceder acceso de lectura y escritura al código fuente en función de las necesidades del negocio y gestionado para hacer frente a los riesgos de alteración o uso indebido y de acuerdo con los procedimientos establecidos;

c) la actualización del código fuente y los elementos asociados y la concesión de acceso al código fuente de conformidad con los procedimientos de control de cambios (ver el inciso 8.32) y solo la realización después de que se haya recibido la autorización adecuada;

d) no conceder a los desarrolladores acceso directo al repositorio de código fuente, sino a través de herramientas de desarrollo que controlen las actividades y autorizaciones sobre el código fuente;

e) mantener listados de programas en un entorno seguro, donde se sugiere el acceso de lectura y escritura se gestione y asigne adecuadamente;

f) mantener un registro de auditoría de todos los accesos y de todos los cambios en el código fuente.

Si el código fuente del programa está destinado a ser publicado, se recomienda considerar controles adicionales para garantizar su integridad (por ejemplo, firma digital).

Otros datos

Si el acceso al código fuente no se controla adecuadamente, el código fuente puede modificarse o algunos datos en el entorno de desarrollo (por ejemplo, copias de datos de producción, detalles de configuración) pueden ser recuperados por personas no autorizadas.

8.5 Autenticación segura

Tipo de control	Propiedades de Seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Identidad_y_control_de_acceso	#Protección

Control

Las tecnologías y procedimientos de autenticación segura se sugiere implementar en función de las restricciones de acceso a la información y la política específica del tema sobre el control de acceso.

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

Propósito

Para garantizar que un usuario o una entidad se autentique de forma segura, cuando se concede acceso a sistemas, aplicaciones y servicios.

Orientación

Se recomienda elegir una técnica de autenticación adecuada para justificar la identidad reclamada de un usuario, software, mensajes y otras entidades.

La fuerza de la autenticación se sugiere sea adecuada para la clasificación de la información a la que se va a acceder. Cuando se requiera una autenticación reforzada y una verificación de identidad, es conveniente utilizar métodos de autenticación alternativos a las contraseñas, como certificados digitales, tarjetas inteligentes, tokens o medios biométricos.

La información de autenticación se sugiere ir acompañada de factores de autenticación adicionales para acceder a sistemas de información críticos (también conocida como autenticación multifactor). El uso de una combinación de múltiples factores de autenticación, como lo que sabe, lo que tiene y lo que es, reduce las posibilidades de accesos no autorizados. La autenticación multifactor se puede combinar con otras técnicas para requerir factores adicionales en circunstancias específicas, basadas en reglas y patrones predefinidos, como el acceso desde una ubicación inusual, desde un dispositivo inusual o en un momento inusual.

La información de autenticación biométrica es conveniente se invalide si alguna vez se ve comprometida. La autenticación biométrica puede no estar disponible dependiendo de las condiciones de uso (por ejemplo, humedad o envejecimiento). Para prepararse para estos problemas, la autenticación biométrica se sugiere ir acompañada de al menos una técnica de autenticación alternativa.

Se recomienda que el procedimiento para iniciar sesión en un sistema o aplicación se diseñe para minimizar el riesgo de acceso no autorizado. Los procedimientos y tecnologías de inicio de sesión es conveniente se implementen teniendo en cuenta lo siguiente:

a) no mostrar información confidencial del sistema o de la aplicación hasta que el proceso de inicio de sesión se haya completado con éxito para evitar proporcionar a un usuario no autorizado asistencia innecesaria;

b) mostrar un aviso general advirtiendo que el sistema, la aplicación o el servicio solo pueden ser accedidos por usuarios autorizados;

c) no proporcionar mensajes de ayuda durante el procedimiento de inicio de sesión que ayuden a un usuario no autorizado (por ejemplo, si surge una condición de error, el sistema no debería indicar qué parte de los datos es correcta o incorrecta);

d) validar la información de inicio de sesión únicamente al completar todos los datos de cálculo;

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

e) proteger contra los intentos de inicio de sesión por fuerza bruta en nombres de usuario y contraseñas [por ejemplo, utilizar una prueba de Turing pública completamente automatizada para diferenciar a computadoras y seres humanos (CAPTCHA), exigir el restablecimiento de la contraseña después de un número predefinido de intentos fallidos o bloquear al usuario después de un número máximo de errores];

f) registrar intentos fallidos y exitosos;

g) provocar un evento de seguridad si se detectara un posible intento o éxito de incumplimiento de los controles de inicio de sesión (por ejemplo, enviar una alerta al usuario y a los administradores del sistema de la organización cuando se ha alcanzado un cierto número de intentos de contraseña incorrectos);

h) mostrar o enviar la siguiente información en un canal separado al finalizar un inicio de sesión exitoso:

1) fecha y hora del inicio de sesión exitoso anterior;

2) detalles de cualquier intento de inicio de sesión fallido desde el último inicio de sesión exitoso;

i) no mostrar una contraseña en texto sin cifrar cuando se introduce; en algunos casos, puede ser necesario desactivar esta funcionalidad para facilitar el inicio de sesión del usuario (por ejemplo, por razones de accesibilidad o para evitar el bloqueo de usuarios debido a errores repetidos);

j) no transmitir contraseñas en texto sin cifrar a través de una red para evitar ser capturado por un programa "sniffer" de red;

k) terminar las sesiones inactivas después de un período definido de inactividad, especialmente en ubicaciones de alto riesgo, como áreas públicas o externas fuera de la gestión de seguridad de la organización o en dispositivos de punto final del usuario;

l) restringir los tiempos de duración de la conexión para proporcionar seguridad adicional para aplicaciones de alto riesgo y reducir la ventana de oportunidad para el acceso no autorizado.

Otros datos

Se puede encontrar información adicional sobre la garantía de autenticación de entidades en la norma que se indica en el inciso 10.45

8.6 Gestión de la capacidad

Tipo de control	Propiedades de Seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo#Detectivo	#Integridad #Disponibilidad	#Identificar #Proteger#Detectarar	#Contiunidad	#Gobernabilidad_y_Ecosistema #Protección

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

Control

El uso de los recursos se sugiere supervisarse y ajustarse de conformidad con las necesidades de capacidad actuales y previstas.

Propósito

Asegurar la capacidad requerida de las instalaciones de procesamiento de información, recursos humanos, oficinas y otras instalaciones.

Orientación

Se sugiere determinar las necesidades de capacidad de las instalaciones de procesamiento de información, los recursos humanos, las oficinas y otras instalaciones, teniendo en cuenta la importancia crítica para las actividades de los sistemas y procesos de que se trate.

La puesta a punto y la supervisión del sistema deberían aplicarse para garantizar y, cuando sea necesario, mejorar la disponibilidad y la eficiencia de los sistemas.

Se recomienda que la organización realice pruebas de estrés de los sistemas y servicios para confirmar que hay suficiente capacidad del sistema disponible para cumplir con los requisitos de rendimiento máximo.

Se sugiere establecer controles de detección para indicar los problemas a su debido tiempo.

Las proyecciones de las necesidades futuras de capacidad es conveniente tener en cuenta las nuevas necesidades institucionales y del sistema y las tendencias actuales y proyectadas en la capacidad de procesamiento de la información de la organización.

Se sugiere prestar especial atención a cualquier recurso con largos plazos de entrega de adquisición o altos costos. Por lo tanto, se recomienda que los gerentes, propietarios de servicios o productos se supervisen la utilización de los recursos clave del sistema.

Es conveniente que los administradores utilicen la información de capacidad para identificar y evitar posibles limitaciones de recursos y dependencia del personal clave que puede representar una amenaza para la seguridad o los servicios del sistema y planificar las medidas apropiadas.

Proporcionar suficiente capacidad puede lograrse aumentando la capacidad o reduciendo la demanda. Se sugiere considerar lo siguiente para aumentar la capacidad:

a) la contratación de nuevo personal;

b) la obtención de nuevas instalaciones o espacios;

c) la adquisición de sistemas de procesamiento, memoria y almacenamiento más potentes;

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

d) hacer uso de la computación en la nube, que tiene características inherentes que abordan directamente las cuestiones de capacidad. La computación en la nube tiene elasticidad y escalabilidad que permiten una rápida expansión bajo demanda y una reducción de los recursos disponibles para aplicaciones y servicios particulares.

Se recomienda considerar lo siguiente para reducir la demanda de recursos de la organización:

a) eliminación de datos obsoletos (espacio en disco);

b) eliminación de los registros impresos que hayan cumplido su período de retención (liberar espacio de estanterías);

c) desmantelamiento de aplicaciones, sistemas, bases de datos o entornos;

d) optimizar los procesos y cronogramas por lotes;

e) optimizar el código de la aplicación o las consultas de la base de datos;

f) denegar o restringir el ancho de banda de los servicios que consumen recursos si estos no son críticos (por ejemplo, la transmisión de vídeo).

Se sugiere considerar un plan documentado de gestión de la capacidad para los sistemas de misión crítica.

Otros datos

Para obtener más detalles sobre la elasticidad y escalabilidad de la computación en la nube, consulte la norma que se indica en el inciso 10.22.

8.7 Protección contra el malware

Tipo de control	Propiedades de Seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo#Detectivo#Correctivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger #Detectar	#Seguridad_de_sistemas_y_redes#Protección_de_la_información	#Protección#Defensa

Control

Es conveniente que la protección contra el malware se implemente y estar respaldada por la conciencia adecuada del usuario.

Propósito

Para garantizar que la información y otros activos asociados estén protegidos contra el malware.

Orientación

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

Se sugiere que la protección contra el malware se base en el software de detección y reparación de malware, el conocimiento de la seguridad de la información, el acceso adecuado al sistema y los controles de gestión de cambios. El uso de software de detección y reparación de malware por sí solo no suele ser adecuado. Se recomienda considerar la siguiente orientación:

a) aplicar normas y controles que impidan o detectaren el uso de programas informáticos no autorizados [por ejemplo, la inclusión en la lista de aplicaciones permitidas (es decir, el uso de una lista que proporcione aplicaciones permitidas)] (ver el inciso 8.19 y el inciso 8.32);

b) implementar controles que impidan o detectar en el uso de sitios web maliciosos conocidos o sospechosos (por ejemplo, listas de bloqueo);

c) reducir las vulnerabilidades que pueden ser explotadas por malware [por ejemplo, mediante la gestión técnica de vulnerabilidades (ver el inciso 8.8 y el inciso 8.19)];

d) llevar a cabo una validación automatizada periódica del software y el contenido de datos de los sistemas, especialmente para los sistemas que respaldan los procesos empresariales críticos; investigar la presencia de archivos no aprobados o enmiendas no autorizadas;

e) establecer medidas de protección contra los riesgos asociados a la obtención de archivos y programas informáticos, ya sea a partir de redes externas o a través de ellas o en cualquier otro medio;

f) instalar y actualizar regularmente software de detección y reparación de malware para escanear computadoras y medios de almacenamiento electrónico. Realizar exploraciones regulares que incluyen:

   1) escanear cualquier dato recibido a través de redes o a través de cualquier forma de medio de almacenamiento electrónico, en busca de malware antes de su uso;

   2) escanear archivos adjuntos y descargas de correo electrónico y mensajería instantánea en busca de malware antes de su uso. Llevar a cabo este escaneo en diferentes lugares (por ejemplo, en servidores de correo electrónico, computadoras de escritorio) y al ingresar a la red de la organización;

   3) escanear páginas web en busca de malware cuando se accede;

g) determinar la ubicación y configuración de las herramientas de detección y reparación de malware en función de los resultados de la evaluación de riesgos y considerar:

   1) principios de defensa en profundidad donde son más eficaces. Por ejemplo, esto puede conducir a la detección de malware en una puerta de enlace de red (en varios protocolos de aplicación, como correo electrónico, transferencia de archivos y web), así como en dispositivos y servidores de punto final del usuario;

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

2) las técnicas evasivas de los atacantes (por ejemplo, el uso de archivos cifrados) para entregar malware o el uso de protocolos de cifrado para transmitir malware;

h) tener cuidado de protegerse contra la introducción de malware durante los procedimientos de mantenimiento y emergencia, que pueden eludir los controles normales contra el malware;

i) implementar un proceso para autorizar temporal o permanentemente la desactivación de algunas o todas las medidas contra el malware, incluidas las autoridades de aprobación de excepciones, la justificación documentada y la fecha de revisión. Esto puede ser necesario cuando la protección contra el malware causa interrupciones en las operaciones normales;

j) preparar planes adecuados de continuidad de las actividades para recuperarse de ataques de malware, incluidas todas las copias de seguridad de datos y software necesarias (incluidas las copias de seguridad en línea y fuera de línea) y las medidas de recuperación (ver el inciso 8.13);

k) aislar entornos en los que puedan producirse consecuencias catastróficas;

l) definir procedimientos y responsabilidades para hacer frente a la protección contra el malware en los sistemas, incluida la formación en su uso, notificación y recuperación de ataques de malware;

m) proporcionar sensibilización o formación (ver el inciso 6.3) a todos los usuarios sobre cómo identificar y mitigar potencialmente la recepción, el envío o la instalación de correos electrónicos, archivos o programas infectados con malware [la información recopilada en n) y o) puede utilizarse para garantizar que la sensibilización y la formación se mantengan actualizadas];

n) implementar procedimientos para recopilar regularmente información sobre nuevo malware, como suscribirse a listas de correo o revisar sitios web relevantes;

o) verificar que la información relacionada con el malware, como los boletines de advertencia, proviene de fuentes calificadas y de buena reputación (por ejemplo, sitios de Internet confiables o proveedores de software de detección de malware) y es precisa e informativa.

Otros datos

No siempre es posible instalar software que proteja contra el malware en algunos sistemas (por ejemplo, algunos sistemas de control industrial). Algunas formas de malware infectan los sistemas operativos de la computadora y el firmware de la computadora, de modo que los controles comunes de malware no pueden limpiar el sistema y es necesaria una nueva imagen completa del software del sistema operativo y, a veces, del firmware de la computadora para volver a un estado seguro.

8.8 Gestión de vulnerabilidades técnicas

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

Tipo de control	Propiedades de Seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Identificar#Proteger	#Amenazas_y_gestión_de_vulnerabilidades	#Gobernabilidad_y_Ecosistema#Protección #Defensa

Control

Es conveniente obtener información sobre las vulnerabilidades técnicas de los sistemas de información en uso, evaluarse la exposición de la organización a esas vulnerabilidades y adoptarse las medidas apropiadas.

Propósito

Evitar la explotación de vulnerabilidades técnicas.

Orientación

Identificación de vulnerabilidades técnicas

Se recomienda que la organización tenga un inventario preciso de activos (ver el inciso 5.9 al inciso 5.14) como requisito previo para una gestión técnica efectiva de vulnerabilidades; se sugiere que el inventario incluya el proveedor de software, el nombre del software, los números de versión, el estado actual de implementación (por ejemplo, qué software está instalado en qué sistemas) y la(s) persona(s) dentro de la organización responsable del software.

Para identificar vulnerabilidades técnicas, se sugiere que la organización considere:

a) definir y establecer las funciones y responsabilidades asociadas con la gestión técnica de la vulnerabilidad, incluida la supervisión de la vulnerabilidad, la evaluación del riesgo de vulnerabilidad, la actualización, el seguimiento de los activos y las responsabilidades de coordinación necesarias;

b) para los programas informáticos y otras tecnologías (sobre la base de la lista de inventario de activos, ver el inciso 5.9), identificar los recursos de información que se utilizan para identificar las vulnerabilidades técnicas pertinentes y mantener el conocimiento sobre ellas. Actualizar la lista de recursos de información en función de los cambios en el inventario o cuando se encuentren otros recursos nuevos o útiles;

c) exigir a los proveedores de sistemas de información (incluidos sus componentes) que garanticen la notificación, el tratamiento y la divulgación de la vulnerabilidad, incluidos los requisitos de los contratos aplicables (ver el inciso 5.20);

d) utilizar herramientas de análisis de vulnerabilidades adecuadas para las tecnologías utilizadas para identificar vulnerabilidades y verificar si la aplicación de parches de vulnerabilidades fue exitosa;

e) la realización de pruebas de penetración planificadas, documentadas y repetibles o evaluaciones de vulnerabilidad por parte de personas competentes y

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

autorizadas para apoyar la identificación de vulnerabilidades. Ejercer precaución, ya que tales actividades pueden llevar a un compromiso de la seguridad del sistema;

f) el seguimiento del uso de bibliotecas de terceros y código fuente para detectar vulnerabilidades. Es conveniente se incluya en la codificación segura (ver el inciso 8.28).

Se sugiere que la organización desarrolle procedimientos y capacidades para:

a) Detectar la existencia de vulnerabilidades en sus productos y servicios, incluido cualquier componente externo utilizado en estos;

b) recibir informes de vulnerabilidad de fuentes internas o externas.

Se recomienda que la organización proporcione un punto de contacto público como parte de una política específica sobre divulgación de vulnerabilidades para que los investigadores y otras personas puedan informar sobre problemas. Se sugiere que la organización establezca procedimientos de informes de vulnerabilidades, formularios de informes en línea y hacer uso de la inteligencia de amenazas adecuada o foros de intercambio de información. Es conveniente que la organización también considere programas de recompensas por errores donde se ofrecen recompensas como un incentivo para ayudar a las organizaciones a identificar vulnerabilidades con el fin de remediarlas adecuadamente. Se recomienda que la organización también comparta información con organismos industriales competentes u otras partes interesadas.

Evaluación de vulnerabilidades técnicas

Para evaluar las vulnerabilidades técnicas identificadas, se sugiere considerar la siguiente orientación:

a) analizar y verificar los informes para determinar qué actividad de respuesta y corrección es necesaria;

b) una vez identificada una posible vulnerabilidad técnica, identificar los riesgos asociados y las medidas que se recomienda adoptar. Tales acciones pueden implicar la actualización de sistemas vulnerables o la aplicación de otros controles.

Adopción de medidas adecuadas para hacer frente a las vulnerabilidades técnicas

Se sugiere implementar un proceso de administración de actualizaciones de software para garantizar que se instalen los parches aprobados y las actualizaciones de aplicaciones más actualizados para todo el software autorizado. Si los cambios son necesarios, el software original se sugiere se conserve y los cambios se apliquen a una copia designada. Todos los cambios se recomienda probar y documentarse por completo, de modo que puedan volver a aplicarse, si es necesario, a futuras actualizaciones de software. Si es necesario, las modificaciones se sugiere sean probadas y validadas por un organismo de evaluación independiente.

Se recomienda considerar la siguiente orientación para abordar las vulnerabilidades técnicas:

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

a) adoptar medidas adecuadas y oportunas en respuesta a la identificación de posibles vulnerabilidades técnicas; definir un calendario para reaccionar a las notificaciones de vulnerabilidades técnicas potencialmente pertinentes;

b) en función de la urgencia con que deba abordarse una vulnerabilidad técnica, llevar a cabo la acción de acuerdo con los controles relacionados con la gestión del cambio (ver el inciso 8.32) o siguiendo los procedimientos de respuesta a incidentes de seguridad de la información (ver el inciso 5.26);

c) solo utilizando actualizaciones de fuentes legítimas (que pueden ser internas o externas a la organización);

d) probar y evaluar las actualizaciones antes de su instalación para garantizar que sean eficaces y no produzcan efectos secundarios que no puedan tolerarse [es decir, si se dispone de una actualización, evaluar los riesgos asociados con la instalación de la actualización (los riesgos planteados por la vulnerabilidad se sugiere se compare con el riesgo de instalar la actualización)];

e) abordar primero los sistemas de alto riesgo;

f) desarrollar correcciones (normalmente actualizaciones o parches de software);

g) ensayo para confirmar si la remediación o mitigación es eficaz;

h) proporcionar mecanismos para verificar la autenticidad de la remediación;

i) si no hay ninguna actualización disponible o la actualización no se puede instalar, teniendo en cuenta otros controles, tales como:

   1) aplicar cualquier solución sugerida por el proveedor de software u otras fuentes relevantes;

   2) desactivar los servicios o capacidades relacionados con la vulnerabilidad;

   3) adaptar o añadir controles de acceso (por ejemplo, cortafuegos) en las fronteras de la red (ver el inciso 8.20 al inciso 8.22);

   4) proteger sistemas, dispositivos o aplicaciones vulnerables de ataques mediante el despliegue de filtros de tráfico adecuados (a veces llamados parches virtuales);

   5) aumentar el monitoreo para detectar ataques reales;

   6) crear conciencia sobre la vulnerabilidad.

Para el software adquirido, si los proveedores publican regularmente información sobre las actualizaciones de seguridad de su software y proporcionan una facilidad para instalar dichas actualizaciones automáticamente, la organización debería decidir si usar la actualización automática o no.

Otras consideraciones

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

Se recomienda mantener un registro de auditoría para todos los pasos realizados en la gestión de vulnerabilidades técnicas.

El proceso de gestión de la vulnerabilidad técnica se sugiere supervisar y evaluarse periódicamente a fin de garantizar su eficacia y eficiencia.

Es conveniente que un proceso eficaz de gestión de vulnerabilidades técnicas este alineado con las actividades de gestión de incidentes, para comunicar datos sobre vulnerabilidades a la función de respuesta a incidentes y proporcionar procedimientos técnicos que se llevarán a cabo en caso de que ocurra un incidente.

Cuando la organización utiliza un servicio en la nube suministrado por un proveedor de servicios en la nube de terceros, se sugiere que la gestión técnica de la vulnerabilidad de los recursos del proveedor de servicios en la nube este garantizada por el proveedor de servicios en la nube. Las responsabilidades del proveedor de servicios en la nube para la gestión de vulnerabilidades técnicas se recomienda forme parte del acuerdo de servicio en la nube y esto es conveniente incluya procesos para informar de las acciones del proveedor de servicios en la nube relacionadas con las vulnerabilidades técnicas (ver el inciso 5.23). Para algunos servicios en la nube, existen responsabilidades respectivas para el proveedor de servicios en la nube y el cliente del servicio en la nube. Por ejemplo, el cliente del servicio en la nube es responsable de la gestión de vulnerabilidades de sus propios activos utilizados para los servicios en la nube.

Otros datos

La gestión técnica de vulnerabilidades puede considerarse como una subfunción de la gestión del cambio y, como tal, puede aprovechar los procesos y procedimientos de gestión del cambio (ver el inciso 8.32).

Existe la posibilidad de que una actualización no aborde el problema adecuadamente y tenga efectos secundarios negativos. Además, en algunos casos, la desinstalación de una actualización no se puede lograr fácilmente una vez que se ha aplicado la actualización.

Si no es posible realizar pruebas adecuadas de las actualizaciones (por ejemplo, debido a los costos o la falta de recursos), se puede considerar un retraso en la actualización para evaluar los riesgos asociados, en función de la experiencia informada por otros usuarios. El uso de la norma que se indica en el inciso 10.31 puede ser beneficioso.

Cuando se producen parches o actualizaciones de software, la organización puede considerar proporcionar un proceso de actualización automatizado en el que estas actualizaciones se instalen en los sistemas o productos afectados sin la necesidad de intervención del cliente o el usuario. Si se ofrece un proceso de actualización automatizado, puede permitir al cliente o usuario elegir una opción para desactivar la actualización automática o controlar el tiempo de instalación de la actualización.

Cuando el proveedor proporciona un proceso de actualización automatizado y las actualizaciones se pueden instalar en los sistemas o productos afectados sin necesidad de intervención, la organización determina si aplica el proceso automatizado o no. Una razón para no elegir la actualización automatizada es mantener el control sobre cuándo se realiza la actualización. Por ejemplo, un software utilizado para una operación comercial no se puede actualizar hasta que la operación se haya completado.

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

Una debilidad con el escaneo de vulnerabilidades es que es posible que no tenga en cuenta completamente la defensa en profundidad: dos contramedidas que siempre se invocan en secuencia pueden tener vulnerabilidades que están enmascaradas por fortalezas en la otra. La contramedida compuesta no es vulnerable, mientras que un escáner de vulnerabilidades puede informar que ambos componentes son vulnerables. Por lo tanto, la organización debería tener cuidado al revisar y actuar sobre los informes de vulnerabilidad.

Muchas organizaciones suministran software, sistemas, productos y servicios no solo dentro de la organización, sino también a partes interesadas, como clientes, socios u otros usuarios. Estos softwares, sistemas, productos y servicios pueden tener vulnerabilidades de seguridad de la información que afectan la seguridad de los usuarios.

Las organizaciones pueden publicar correcciones y divulgar información sobre vulnerabilidades a los usuarios (generalmente a través de un aviso público) y proporcionar información adecuada para los servicios de base de datos de vulnerabilidades de software.

Para obtener más información relacionada con la gestión de vulnerabilidades técnicas al utilizar la computación en la nube, consulte la serie de normas que se indica en el inciso 10.9 y en la norma que se indica en el inciso 10.29.

La norma que se indica en el inciso 10.47 proporciona información detallada sobre la recepción de informes de vulnerabilidad y la publicación de avisos de vulnerabilidad. La norma que se indica en el inciso 10.49 proporciona información detallada sobre el manejo y la resolución de vulnerabilidades reportadas.

8.9 Gestión de la configuración

Tipo de control	Propiedades de Seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Configuración_ segura	#Protección

Control

Se recomienda que las configuraciones, incluidas las configuraciones de seguridad, de hardware, software, servicios y redes establezcan, documenten, implementen, supervisen y revisen.

Propósito

Para garantizar que el hardware, el software, los servicios y las redes funcionen correctamente con la configuración de seguridad requerida, y que la configuración no se vea alterada por cambios no autorizados o incorrectos.

Orientación

General

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

Se recomienda que la organización defina e implemente procesos y herramientas para hacer cumplir las configuraciones definidas (incluidas las configuraciones de seguridad) para hardware, software, servicios (por ejemplo, servicios en la nube) y redes, para sistemas recién instalados, así como para sistemas operativos a lo largo de su vida útil.

Se sugiere existan funciones, responsabilidades y procedimientos para garantizar un control satisfactorio de todos los cambios de configuración.

Plantillas estándar

Se recomienda que las plantillas estándar para la configuración segura de hardware, software, servicios y redes definan:

a) utilizando orientaciones disponibles públicamente (por ejemplo, plantillas predefinidas de proveedores y de organizaciones de seguridad independientes);

b) considerando el nivel de protección necesario para determinar un nivel suficiente de seguridad;

c) apoyar la política de seguridad de la información de la organización, las políticas específicas del tema, las normas y otros requisitos de seguridad;

d) considerar la viabilidad y aplicabilidad de las configuraciones de seguridad en el contexto de la organización.

Las plantillas se sugiere se revisen periódicamente y actualizarse cuando sea necesario abordar nuevas amenazas o vulnerabilidades, o cuando se introduzcan nuevas versiones de software o hardware.

Se recomienda tener en cuenta lo siguiente para establecer plantillas estándar para la configuración segura de hardware, software, servicios y redes:

a) minimizar el número de identidades con privilegios o derechos de acceso a nivel de administrador;

b) deshabilitar identidades innecesarias, no utilizadas o inseguras;

c) deshabilitar o restringir funciones y servicios innecesarios;

d) restringir el acceso a potentes programas de utilidad y a la configuración de los parámetros del host;

e) sincronización de relojes;

f) cambiar la información de autenticación predeterminada del proveedor, como las contraseñas predeterminadas, inmediatamente después de la instalación y revisar otros parámetros importantes relacionados con la seguridad por defecto;

g) invocar instalaciones de tiempo de espera que cierren automáticamente la sesión de los dispositivos informáticos después de un período predeterminado de inactividad;

h) verificar que se cumplen los requisitos de licencia (ver el inciso 5.32).

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

Administración de configuraciones

Es conveniente que las configuraciones establecidas de hardware, software, servicios y redes se registren y se recomienda mantener un registro de todos los cambios de configuración. Es conveniente que estos registros se almacenen de forma segura. Esto se puede lograr de varias maneras, como bases de datos de configuración o plantillas de configuración.

Se sugiere que los cambios en las configuraciones sigan el proceso de gestión de cambios (ver el inciso 8.32).

Los registros de configuración pueden contener, según corresponda:

a) a)información actualizada del propietario o del punto de contacto del activo;

b) b)fecha del último cambio de configuración;

c) c)versión de la plantilla de configuración;

d) d)relación con las configuraciones de otros activos.

Supervisión de configuraciones

Se sugiere que las configuraciones se supervisen con un conjunto completo de herramientas de administración del sistema (por ejemplo, utilidades de mantenimiento, soporte remoto, herramientas de administración empresarial, software de copia de seguridad y restauración) y es conveniente revisar regularmente para verificar los ajustes de configuración, evaluar las fortalezas de las contraseñas y evaluar las actividades realizadas. Las configuraciones reales se pueden comparar con las plantillas de destino definidas. Se recomienda que cualquier desviación se aborde, ya sea mediante la aplicación automática de la configuración de objetivo definida o mediante el análisis manual de la desviación seguido de acciones correctivas.

Otros datos

La documentación para sistemas a menudo registra detalles sobre la configuración tanto de hardware como de software.

El endurecimiento del sistema es una parte típica de la gestión de la configuración.

La gestión de la configuración se puede integrar con los procesos de gestión de activos y las herramientas asociadas.

La automatización suele ser más efectiva para administrar la configuración de seguridad (por ejemplo, utilizando la infraestructura como código).

Las plantillas de configuración y los destinos pueden ser información confidencial y se recomienda proteger del acceso no autorizado en consecuencia.

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

8.10 Eliminación de información

Tipo de control	Propiedades de Seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo	#Confidencialidad	#Proteger	#Protección_de_la_información#Cumplimiento_y_legal	#Protección

Control

La información almacenada en sistemas de información, dispositivos o en cualquier otro medio de almacenamiento debería eliminarse cuando ya no sea necesaria.

Propósito

Para evitar la exposición innecesaria de información confidencial y para cumplir con los requisitos legales, legales, reglamentarios y contractuales para la eliminación de información.

Orientación

General

La información sensible no es conveniente se conserve durante más tiempo del necesario para reducir el riesgo de divulgación indeseable.

Al eliminar información sobre sistemas, aplicaciones y servicios, se sugiere tener en cuenta lo siguiente:

a) seleccionar un método de eliminación (por ejemplo, sobreescritura electrónica o borrado criptográfico) de conformidad con los requisitos empresariales y teniendo en cuenta las leyes y reglamentos pertinentes;

b) registrar los resultados de la supresión como prueba;

c) cuando se utilicen proveedores de servicios de eliminación de información, obteniendo evidencia de eliminación de información de ellos.

Cuando terceros almacenen la información de la organización en su nombre, se sugiere que la organización considere la inclusión de requisitos sobre la eliminación de información en los acuerdos de terceros para hacerla cumplir durante y después de la terminación de dichos servicios.

Métodos de eliminación

De acuerdo con la política temática específica de la organización sobre la retención de datos y teniendo en cuenta la legislación y los reglamentos pertinentes, se recomienda que la información confidencial se elimine cuando ya no sea necesaria, mediante:

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

a) configurar sistemas para destruir de forma segura la información cuando ya no sea necesario (por ejemplo, después de un período definido sujeto a la política específica del tema sobre retención de datos o por solicitud de acceso del sujeto);

b) eliminar versiones, copias y archivos temporales obsoletos dondequiera que se encuentren;

c) utilizar software de eliminación seguro y aprobado para eliminar permanentemente la información a fin de ayudar a garantizar que la información no se pueda recuperar mediante el uso de herramientas especializadas en recuperación o forenses;

d) utilizar proveedores autorizados y certificados de servicios de eliminación segura;

e) utilizar mecanismos de eliminación adecuados para el tipo de medio de almacenamiento que se elimine (por ejemplo, unidades de disco duro desmagnetización y otros medios de almacenamiento magnéticos).

Cuando se utilizan servicios en la nube, se sugiere que la organización verifique si el método de eliminación proporcionado por el proveedor de servicios en la nube es aceptable y, si es el caso, es conveniente que la organización use o solicite que el proveedor de servicios en la nube elimine la información. Estos procesos de eliminación se recomienda automatizar de acuerdo con las políticas específicas del tema, cuando estén disponibles y sean aplicables. Dependiendo de la sensibilidad de la información eliminada, los registros pueden rastrear o verificar que estos procesos de eliminación hayan ocurrido.

Para evitar la exposición involuntaria de información confidencial cuando el equipo se envía de vuelta a los proveedores, se recomienda que la información confidencial se proteja eliminando los almacenamientos auxiliares (por ejemplo, unidades de disco duro) y la memoria antes de que el equipo abandone las instalaciones de la organización.

Teniendo en cuenta que la eliminación segura de algunos dispositivos (por ejemplo, teléfonos inteligentes) solo se puede lograr mediante la destrucción o el uso de las funciones integradas en estos dispositivos (por ejemplo, "restaurar la configuración de fábrica"), se sugiere que la organización elija el método apropiado de acuerdo con la clasificación de la información manejada por dichos dispositivos.

Las medidas de control descritas en el inciso 7.14 se recomienda aplicar para destruir físicamente el dispositivo de almacenamiento y eliminar simultáneamente la información que contiene.

Un registro oficial de eliminación de información es útil cuando se analiza la causa de un posible evento de fuga de información.

Otros datos

La información sobre la eliminación de datos de usuario en los servicios en la nube se puede encontrar en la norma que se indica en el inciso 10.29.

La información sobre la eliminación de PII se puede encontrar en la norma que se indica en el inciso 10.42.

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

8.11 Enmascaramiento de datos

Tipo de control	Propiedades de Seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo	#Confidencialidad	#Proteger	#Protección_de_la_información	#Protección

Control

El enmascaramiento de datos se sugiere utilizar de acuerdo con la política específica del tema de la organización sobre control de acceso y otras políticas relacionadas con temas específicos, y los requisitos comerciales, teniendo en cuenta la legislación aplicable.

Propósito

Limitar la exposición de datos confidenciales, incluida la PII, y cumplir con los requisitos legales, legales, reglamentarios y contractuales.

Orientación

Cuando la protección de datos confidenciales (por ejemplo, PII) sea una preocupación, es conveniente que la organización considere ocultar dichos datos mediante el uso de técnicas como el enmascaramiento de datos, la seudonimización o la anonimización.

Las técnicas de seudonimización o anonimización pueden ocultar la PII, disfrazar la verdadera identidad de los principales de PII u otra información confidencial, y desconectar el vínculo entre la PII y la identidad del principal de PII o el vínculo entre otra información confidencial.

Cuando se utilizan técnicas de seudonimización o anonimización, se debería verificar que los datos han sido adecuadamente seudonimizados o anonimizados. Se recomienda que la anonimización de datos se considere que todos los elementos de la información confidencial son efectivos. Por ejemplo, si no se considera adecuadamente, una persona puede ser identificada incluso si los datos que pueden identificar directamente a esa persona son anónimos, por la presencia de datos adicionales que permiten identificar a la persona indirectamente.

Las técnicas adicionales para el enmascaramiento de datos incluyen:

a) cifrado (que requiere que los usuarios autorizados tengan una clave);

b) anular o eliminar caracteres (evitando que usuarios no autorizados vean mensajes completos);

c) números y fechas variables;

d) sustitución (cambiar un valor por otro para ocultar datos sensibles);

e) sustituir los valores por su hash.

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

Se sugiere tener en cuenta lo siguiente al implementar técnicas de enmascaramiento de datos:

a) no conceder a todos los usuarios acceso a todos los datos, diseñando así consultas y máscaras para mostrar únicamente los datos mínimos requeridos al usuario;

b) hay casos en los que algunos datos no se sugiere sean visibles para el usuario para algunos registros de un conjunto de datos; en este caso, diseñar e implementar un mecanismo para la ofuscación de datos (por ejemplo, si un paciente no desea que el personal del hospital pueda ver todos sus registros, incluso en caso de emergencia, entonces al personal del hospital se le presentan datos parcialmente ofuscados y los datos solo pueden ser accedidos por personal con roles específicos si contienen información útil para el tratamiento adecuado);

c) cuando los datos están ofuscados, dando al principal de PII la posibilidad de exigir que los usuarios no puedan ver si los datos están ofuscados (ofuscación de la ofuscación; esto se utiliza en los centros de salud, por ejemplo, si el paciente no quiere que el personal vea que se ha ofuscado información confidencial como embarazos o resultados de exámenes de sangre);

d) cualquier requisito legal o reglamentario (por ejemplo, exigir el enmascaramiento de la información de las tarjetas de pago durante el procesamiento o almacenamiento).

Se sugiere tener en cuenta lo siguiente al usar el enmascaramiento de datos, la seudonimización o la anonimización:

a) nivel de fuerza del enmascaramiento, seudonimización o anonimización de los datos en función del uso de los datos tratados;

b) controles de acceso a los datos tratados;

c) acuerdos o restricciones sobre el uso de los datos procesados;

d) prohibir la recopilación de los datos tratados con otra información con el fin de identificar el principal de la PII;

e) realizar un seguimiento de la provisión y recepción de los datos procesados.

Otros datos

La anonimización altera irreversiblemente la PII de tal manera que el principal de PII ya no puede ser identificado directa o indirectamente.

La seudonimización reemplaza la información de identificación con un alias. El conocimiento del algoritmo (a veces denominado "información adicional") utilizado para realizar la seudonimización permite al menos alguna forma de identificación del principal de PII. Por lo tanto, dicha "información adicional" se sugiere mantener separada y protegida.

Si bien la seudonimización es, por lo tanto, más débil que la anonimización, los conjuntos de datos seudonimizados pueden ser más útiles en la investigación estadística.

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

El enmascaramiento de datos es un conjunto de técnicas para ocultar, sustituir u ofuscar elementos de datos confidenciales. El enmascaramiento de datos puede ser estático (cuando los elementos de datos se enmascaran en la base de datos original), dinámico (utilizando automatización y reglas para proteger los datos en tiempo real) o sobre la marcha (con datos enmascarados en la memoria de una aplicación).

Las funciones hash se pueden usar para anonimizar la PII. Para evitar ataques de enumeración, se sugiere siempre combinarse con una función de sal.

La PII en los identificadores de recursos y sus atributos [por ejemplo, nombres de archivo, localizadores uniformes de recursos (URL)] es conveniente evitar o anonimizarse adecuadamente.

Los controles adicionales relacionados con la protección de la PII en las nubes públicas se dan en la NMX-I-27018-NYCE-2021.

Información adicional sobre las técnicas de desidentificación está disponible en la norma que se indica en el inciso 10.15.

8.12 Prevención de fuga de datos

Tipo de control	Propiedades de Seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo #Detectivo	#Confidencialidad	#Proteger #Detectar	#Protección_de_la_información	#Protección#Defensa

Control

Se recomienda que las medidas de prevención de fugas de datos se apliquen a los sistemas, redes y cualquier otro dispositivo que procese, almacene o transmita información confidencial.

Propósito

Detectar y prevenir la divulgación y extracción no autorizada de información por parte de individuos o sistemas.

Orientación

Se sugiere que la organización considere lo siguiente para reducir el riesgo de fuga de datos:

a) identificar y clasificar la información para protegerla contra fugas (por ejemplo, información personal, modelos de precios y diseños de productos);

b) supervisar los canales de fuga de datos (por ejemplo, correo electrónico, transferencias de archivos, dispositivos móviles y dispositivos de almacenamiento portátiles);

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

c) actuar para evitar que se filtre información (por ejemplo, correos electrónicos de cuarentena que contengan información confidencial).

Es conveniente que las herramientas de prevención de fugas de datos se utilicen para:

a) identificar y supervisar la información sensible en riesgo de divulgación no autorizada (por ejemplo, en datos no estructurados en el sistema de un usuario);

b) Detectar la divulgación de información sensible (por ejemplo, cuando la información se carga en servicios en la nube de terceros que no son de confianza o se envía por correo electrónico);

c) bloquear las acciones del usuario o las transmisiones de red que exponen información confidencial (por ejemplo, evitar la copia de entradas de la base de datos en una hoja de cálculo).

Se sugiere que la organización determine si es necesario restringir la capacidad de un usuario para copiar y pegar o cargar datos en servicios, dispositivos y medios de almacenamiento fuera de la organización. Si ese es el caso, se recomienda que la organización implemente tecnología como herramientas de prevención de fugas de datos o la configuración de herramientas existentes que permitan a los usuarios ver y manipular los datos almacenados de forma remota, pero evitar copiar y pegar fuera del control de la organización.

Si se requiere la exportación de datos, se sugiere permitir que el propietario de los datos apruebe la exportación y responsabilice a los usuarios por sus acciones.

La toma de capturas de pantalla o fotografías de la pantalla debería abordarse a través de términos y condiciones de uso, capacitación y auditoría.

Cuando se realice una copia de seguridad de los datos, se recomienda tener cuidado de garantizar que la información confidencial esté protegida mediante medidas como el cifrado, el control de acceso y la protección física de los medios de almacenamiento que contienen la copia de seguridad.

Se recomienda que la prevención de fugas de datos también se considere para proteger contra las acciones de inteligencia de un adversario de la obtención de información confidencial o secreta (geopolítica, humana, financiera, comercial, científica o cualquier otra) que pueda ser de interés para el espionaje o pueda ser crítica para la comunidad. Es conveniente que las acciones de prevención de fugas de datos estén orientadas a confundir las decisiones del adversario, por ejemplo, reemplazando la información auténtica con información falsa, ya sea como una acción independiente o como respuesta a las acciones de inteligencia del adversario. Ejemplos de este tipo de acciones son la ingeniería social inversa o el uso de honeypots para atraer a los atacantes.

Otros datos

Las herramientas de prevención de fugas de datos están diseñadas para identificar datos, monitorear el uso y movimiento de datos y tomar medidas para evitar que los datos se filtren (por ejemplo, alertar a los usuarios sobre su comportamiento de riesgo y bloquear la transferencia de datos a dispositivos de almacenamiento portátiles).

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

La prevención de fugas de datos implica inherentemente el monitoreo de las comunicaciones y las actividades en línea del personal, y por extensión los mensajes de partes externas, lo que plantea preocupaciones legales que se sugiere considerar antes de implementar herramientas de prevención de fugas de datos. Existe una variedad de leyes relacionadas con la privacidad, la protección de datos, el empleo, la interceptación de datos y las telecomunicaciones que son aplicables al monitoreo y procesamiento de datos en el contexto de la prevención de fugas de datos.

La prevención de fugas de datos puede ser compatible con controles de seguridad estándar, como políticas específicas de temas sobre control de acceso y gestión segura de documentos (ver el inciso 5.12 y el inciso 5.15).

8.13 Copia de seguridad de la información

Tipo de control	Propiedades de Seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Correctivo	#Integridad #Disponibilidad	#Recuperación	#Contiunidad	#Protección

Control

Se recomienda que las copias de seguridad de la información, el software y los sistemas se mantengan y prueben periódicamente de conformidad con la política acordada sobre copias de seguridad sobre el tema específico.

Propósito

Para permitir la recuperación de la pérdida de datos o sistemas.

Orientación

Se recomienda establecer una política específica sobre el tema de copia de seguridad para abordar los requisitos de retención de datos y seguridad de la información de la organización.

Se sugiere proporcionar instalaciones de copia de seguridad adecuadas para garantizar que toda la información y el software esenciales se puedan recuperar después de un incidente o falla o pérdida de medios de almacenamiento.

Se recomienda desarrollar e implementar planes sobre cómo la organización realiza copias de seguridad de la información, el software y los sistemas, para abordar la política específica del tema sobre la copia de seguridad.

Al diseñar un plan de copia de seguridad, se sugiere tener en cuenta los siguientes elementos:

a) producir registros precisos y completos de las copias de seguridad y los procedimientos de restauración documentados;

b) reflejar los requisitos empresariales de la organización (por ejemplo, el objetivo del punto de recuperación, ver el inciso 5.30), los requisitos de seguridad de la

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

información en cuestión y la criticidad de la información para el funcionamiento continuo de la organización en la medida (por ejemplo, copia de seguridad completa o diferencial) y frecuencia de las copias de seguridad;

c) almacenar las copias de seguridad en una ubicación remota segura y protegida, a una distancia suficiente para evitar cualquier daño causado por una catástrofe en el emplazamiento principal;

d) proporcionar a la información de reserva un nivel adecuado de protección física y medioambiental (ver el capítulo 7 y el inciso 8.1) coherente con las normas aplicadas en el emplazamiento principal;

e) probar periódicamente los medios de copia de seguridad para garantizar que se pueda confiar en ellos para su uso de emergencia cuando sea necesario. Probar la capacidad de restaurar datos respaldados en un sistema de prueba, no sobrescribiendo los medios de almacenamiento originales en caso de que el proceso de copia de seguridad o restauración falle y cause daños o pérdidas irreparables de datos;

f) proteger las copias de seguridad mediante cifrado de acuerdo con los riesgos identificados (por ejemplo, en situaciones en las que la confidencialidad es importante);

g) tener cuidado de garantizar que se detectare una pérdida inadvertida de datos antes de realizar la copia de seguridad.

Es conveniente que los procedimientos operativos supervisen la ejecución de las copias de seguridad y abordar los errores de las copias de seguridad programadas para garantizar la integridad de las copias de seguridad de acuerdo con la política específica del tema sobre copias de seguridad.

Se recomienda que las medidas de copia de seguridad de los sistemas y servicios individuales se prueben periódicamente para garantizar que cumplen los objetivos de los planes de respuesta a incidentes y continuidad del negocio (ver el inciso 5.30). Se sugiere esto se combine con una prueba de los procedimientos de restauración y verificarse con el tiempo de restauración requerido por el plan de continuidad del negocio. En el caso de sistemas y servicios críticos, las medidas de copia de seguridad deberían abarcar toda la información, las aplicaciones y los datos de los sistemas necesarios para recuperar el sistema completo en caso de desastre.

Cuando la organización utiliza un servicio en la nube, se recomienda tomar copias de seguridad de la información, las aplicaciones y los sistemas de la organización en el entorno de servicios en la nube. Se sugiere que la organización determine si se cumplen los requisitos para la copia de seguridad y de qué manera cuando se utiliza el servicio de copia de seguridad de la información proporcionado como parte del servicio en la nube.

Es conveniente determinar el período de retención de la información comercial esencial, teniendo en cuenta cualquier requisito de conservación de copias de archivo. Se sugiere que la organización considere la eliminación de la información (ver el inciso 8.10) en los medios de almacenamiento utilizados para la copia de seguridad una vez que expire el período de retención de la información y se sugiere tener en cuenta la legislación y los reglamentos.

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

Otros datos

Para obtener más información sobre la seguridad del almacenamiento, incluida la consideración de la retención, consulte la norma que se indica en el inciso 10.39.

8.14 Redundancia de las instalaciones de procesamiento de información

Tipo de control	Propiedades de Seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo	#Disponibilidad	#Proteger	#Continuidad#Gestión_de_activos	#Protección#Resiliencia

Control

Las instalaciones de procesamiento de información se sugiere se implementen con redundancia suficiente para cumplir con los requisitos de disponibilidad.

Propósito

Asegurar el funcionamiento continuo de las instalaciones de procesamiento de información.

Orientación

Es conveniente que la organización determine los requisitos para la disponibilidad de servicios empresariales y sistemas de información. Se recomienda que la organización diseñe e implemente una arquitectura de sistemas con la redundancia adecuada para cumplir con estos requisitos.

La redundancia se puede introducir duplicando las instalaciones de procesamiento de información en parte o en su totalidad (es decir, componentes de repuesto o teniendo dos de todo). Se sugiere que la organización planifique e implemente procedimientos para la activación de los componentes redundantes y las instalaciones de procesamiento. Es conveniente que los procedimientos establezcan si los componentes redundantes y las actividades de procesamiento están siempre activados o, en caso de emergencia, activados automática o manualmente. Es conveniente que los componentes redundantes y las instalaciones de procesamiento de información garanticen el mismo nivel de seguridad que los primarios.

Se sugiere existan mecanismos para alertar a la organización sobre cualquier falla en las instalaciones de procesamiento de información, permitir la ejecución del procedimiento planificado y permitir la disponibilidad continua mientras se reparan o reemplazan las instalaciones de procesamiento de información.

Es conveniente que la organización tenga en cuenta lo siguiente al implementar sistemas redundantes:

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

a) la contratación con dos o más proveedores de redes e instalaciones críticas de tratamiento de la información, como los proveedores de servicios de Internet;

b) utilizar redes redundantes;

c) utilizar dos centros de datos geográficamente separados con sistemas reflejados;

d) utilizar fuentes o fuentes de alimentación físicamente redundantes;

e) utilizar múltiples instancias paralelas de componentes de software, con equilibrio de carga automático entre ellas (entre instancias en el mismo centro de datos o en diferentes centros de datos);

f) tener componentes duplicados en sistemas (por ejemplo, CPU, discos duros, memorias) o en redes (por ejemplo, cortafuegos, enrutadores, conmutadores).

Cuando proceda, preferiblemente en modo de producción, se sugiere probar sistemas de información redundantes para garantizar que la conmutación por error de un componente a otro funciona según lo previsto.

Otros datos

Existe una fuerte relación entre la redundancia y la preparación de las TIC para la continuidad del negocio (ver el inciso 5.30), especialmente si se requieren tiempos de recuperación cortos. Muchas de las medidas de redundancia pueden formar parte de las estrategias y soluciones de continuidad de las TIC.

La aplicación de redundancias puede introducir riesgos para la integridad (por ejemplo, los procesos de copia de datos en componentes duplicados pueden introducir errores) o la confidencialidad (por ejemplo, un control de seguridad deficiente de los componentes duplicados puede llevar a un compromiso) de los sistemas de información e información, se recomienda tener en cuenta al diseñar sistemas de información.

La redundancia en las instalaciones de procesamiento de información generalmente no aborda la falta de disponibilidad de la aplicación debido a fallas dentro de una aplicación.

Con el uso de la computación en la nube pública, es posible tener múltiples versiones en vivo de las instalaciones de procesamiento de información, existentes en múltiples ubicaciones físicas separadas con conmutación por error automática y equilibrio de carga entre ellas.

Algunas de las tecnologías y técnicas para proporcionar redundancia y conmutación por error automática en el contexto de los servicios en la nube se analizan en la norma que se indica en el inciso 10.22.

8.15 Bitácoras

Tipo de control	Propiedades de Seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Detectivo	#Confidencialidad #Integridad	#Detectar	#Gestión_de_eventos_de_seguri	#Protección#Defensa

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

	#Disponibilidad		dad_de_la_información	

Control

Las bitácoras que registran actividades, excepciones, fallas y otros eventos relevantes se sugiere se produzcan, almacenen, protejan y analicen.

Propósito

Para registrar eventos, generar evidencia, garantizar la integridad de la información de registro, prevenir el acceso no autorizado, identificar eventos de seguridad de la información que pueden conducir a un incidente de seguridad de la información y apoyar las investigaciones.

Orientación

General

Se sugiere que la organización determine el propósito para el que se crean las bitácoras, qué datos se recopilan y registran, y cualquier requisito específico de la bitácora para proteger y manejar los datos de registro. Se sugiere se documente en una política de bitácoras de temas específicos.

Se recomienda que las bitácoras de eventos incluyan para cada evento, según corresponda:

a) ID de usuario;

b) actividades del sistema;

c) fechas, horas y detalles de los acontecimientos pertinentes (por ejemplo.log y cierre de sesión);

d) identidad del dispositivo, identificador del sistema y ubicación;

e) direcciones y protocolos de red.

Se sugiere tener en cuenta los siguientes eventos para el registro:

a) intentos de acceso al sistema exitosos y rechazados;

b) intentos exitosos y rechazados de acceso a datos y otros recursos;

c) cambios en la configuración del sistema;

d) uso de privilegios;

e) uso de programas y aplicaciones de utilidad;

f) los archivos a los que se accede y el tipo de acceso, incluida la eliminación de archivos de datos importantes;

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

g) las alarmas generadas por el sistema de control de acceso;

h) activación y desactivación de sistemas de seguridad, como sistemas antivirus y sistemas de detección de intrusos;

i) creación, modificación o supresión de identidades;

j) transacciones ejecutadas por los usuarios en aplicaciones. En algunos casos, las aplicaciones son un servicio o producto proporcionado o ejecutado por un tercero.

Es importante que todos los sistemas tengan fuentes de tiempo sincronizadas (ver el inciso 8.17) ya que esto permite la correlación de registros entre sistemas para el análisis, alerta e investigación de un incidente.

Protección de los registros

Los usuarios, incluidos aquellos con derechos de acceso privilegiados, no se recomienda tener permiso para eliminar o desactivar registros de sus propias actividades. Potencialmente pueden manipular los registros en las instalaciones de procesamiento de información bajo su control directo. Por lo tanto, es necesario proteger y revisar los registros para mantener la responsabilidad de los usuarios privilegiados.

Es conveniente que los controles tengan como objetivo proteger contra cambios no autorizados en la información de registro y problemas operativos con la instalación de registro, que incluyen:

a) alteraciones en los tipos de mensajes que se registran;

b) archivos de registro que se editan o eliminan;

c) falta de registro de eventos o sobreescritura de eventos grabados anteriormente si se excede el medio de almacenamiento que contiene un archivo de registro.

Para la protección de los registros, se sugiere considerar el uso de las siguientes técnicas: hash criptográfico, grabación en un archivo de solo apéndice y solo lectura, grabación en un archivo de transparencia pública.

Es posible que se requiera que algunos registros de auditoría se archiven debido a los requisitos de retención de datos o a los requisitos para recopilar y conservar pruebas (ver el inciso 5.28).

Cuando la organización necesite enviar registros del sistema o de la aplicación a un proveedor para ayudar con la depuración o la solución de problemas de errores, se sugiere que los registros se desidentifican siempre que sea posible mediante técnicas de enmascaramiento de datos (ver el inciso 8.11) para obtener información como nombres de usuario, direcciones de protocolo de Internet (IP), nombres de host o nombre de organización, antes de enviarlos al proveedor.

Los registros de eventos pueden contener datos confidenciales e información de identificación personal. Se sugiere adoptar las medidas adecuadas de protección de la privacidad (ver el inciso 5.34).

Análisis de registros

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

Se sugiere que el análisis de registro cubra el análisis y la interpretación de eventos de seguridad de la información, para ayudar a identificar actividades inusuales o comportamientos anómalos, que pueden representar indicadores de compromiso.

El análisis de los eventos se recomienda se realicen teniendo en cuenta:

a) las competencias necesarias para los expertos que realizan el análisis;

b) determinar el procedimiento de análisis logarítmico;

c) los atributos requeridos de cada evento relacionado con la seguridad;

d) excepciones identificadas mediante el uso de reglas predeterminadas [por ejemplo, información de seguridad y gestión de eventos (SIEM) o reglas de cortafuegos, y sistemas de detección de intrusos (IDS) o firmas de malware];

e) patrones de comportamiento conocidos y tráfico de red estándar en comparación con la actividad y el comportamiento anómalos [análisis de comportamiento de usuarios y entidades (UEBA)];

f) resultados del análisis de tendencias o patrones (por ejemplo, como resultado del uso de análisis de datos, técnicas de big data y herramientas de análisis especializadas);

g) inteligencia de amenazas disponible.

El análisis de registros se sugiere estar respaldado por actividades de monitoreo específicas para ayudar a identificar y analizar el comportamiento anómalo, que incluye:

a) revisar los intentos exitosos y fallidos de acceder a recursos protegidos [por ejemplo, servidores del sistema de nombres de dominio (DNS), portales web y recursos compartidos de archivos];

b) comprobar los registros dns para identificar las conexiones de red salientes a servidores malintencionados, como los asociados con los servidores de comando y control de botnets;

c) examinar los informes de uso de los proveedores de servicios (por ejemplo, facturas o informes de servicios) en busca de actividades inusuales dentro de los sistemas y redes (por ejemplo, mediante la revisión de los patrones de actividad);

d) incluir registros de sucesos de seguimiento físico, como la entrada y la salida, para garantizar una detección y un análisis de incidentes más precisos;

e) correlacionar registros para permitir un análisis eficiente y altamente preciso.

Los incidentes de seguridad de la información sospechosos y reales se sugiere identificarlos (por ejemplo, infección de malware o sondeo de cortafuegos) y estar sujetos a una investigación adicional (por ejemplo, como parte de un proceso de gestión de incidentes de seguridad de la información, ver el inciso 5.25).

Otros datos

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

Los registros del sistema a menudo contienen un gran volumen de información, gran parte de la cual es ajena a la supervisión de la seguridad de la información. Para ayudar a identificar eventos significativos con fines de monitoreo de seguridad de la información, se puede considerar el uso de programas de utilidad adecuados o herramientas de auditoría para realizar interrogatorios de archivos.

El registro de eventos sienta las bases para los sistemas de monitoreo automatizados (ver el inciso 8.16) que son capaces de generar informes consolidados y alertas sobre la seguridad del sistema.

Una herramienta SIEM o un servicio equivalente se puede utilizar para almacenar, correlacionar, normalizar y analizar la información de registro, y para generar alertas. Los SIEM tienden a requerir una configuración cuidadosa para optimizar sus beneficios. Las configuraciones a considerar incluyen la identificación y selección de fuentes de registro apropiadas, el ajuste y la prueba de reglas y el desarrollo de casos de uso.

Los archivos de transparencia pública para el registro de registros se utilizan, por ejemplo, en los sistemas de transparencia de certificados. Dichos archivos pueden proporcionar un mecanismo de detección adicional útil para protegerse contra la manipulación de registros.

En entornos de nube, las responsabilidades de administración de registros se pueden compartir entre el cliente del servicio en la nube y el proveedor de servicios en la nube. Las responsabilidades varían según el tipo de servicio en la nube que se utilice.
Se puede encontrar más orientación en la norma que se indica en el inciso 10.29.

8.16 Actividades de seguimiento

Tipo de control	Propiedades de Seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Detectivo#Correctivo	#Confidencialidad #Integridad #Disponibilidad	#Detectar #Responder	#Gestión_de_eventos_de_seguridad_de_la_información	#Defensa

Control

Las redes, los sistemas y las aplicaciones es conveniente sean monitoreados para detectar comportamientos anómalos y se sugiere tomar las medidas apropiadas para evaluar posibles incidentes de seguridad de la información.

Propósito
Detectar comportamientos anómalos y posibles incidentes de seguridad de la información.

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

Orientación

El alcance y el nivel de supervisión se recomienda determinar de conformidad con los requisitos de seguridad empresarial y de la información y teniendo en cuenta las leyes y reglamentos pertinentes. Los registros de monitoreo se sugiere se mantengan durante períodos de retención definidos.

Se recomienda considerar la inclusión dentro del sistema de monitoreo:

a) tráfico de redes, sistemas y aplicaciones salientes y entrantes;

b) acceso a sistemas, servidores, equipos de red, sistemas de monitorización, aplicaciones críticas, etc.;

c) archivos críticos o de configuración de red y sistema a nivel de administrador;

d) registros de herramientas de seguridad [por ejemplo, antivirus, IDS, sistema de prevención de intrusiones (IPS), filtros web, cortafuegos, prevención de fugas de datos];

e) registros de sucesos relacionados con la actividad del sistema y de la red;

f) comprobar que el código que se está ejecutando está autorizado para ejecutarse en el sistema y que no ha sido manipulado (por ejemplo, mediante la recopilación para añadir código adicional no deseado);

g) el uso de los recursos (por ejemplo, CPU, discos duros, memoria, ancho de banda) y su rendimiento.

Es conveniente que la organización establezca una línea de base de comportamiento normal y monitorear contra esta línea de base para detectar anomalías. Al establecer una línea de base, se recomienda tener en cuenta lo siguiente:

a) revisar la utilización de los sistemas en períodos normales y pico;

b) hora habitual de acceso, ubicación del acceso, frecuencia de acceso para cada usuario o grupo de usuarios.

Es conveniente que el sistema de monitoreo se configure con respecto a la línea de base establecida para identificar comportamientos anómalos, tales como:

a) terminación no planificada de procesos o solicitudes;

b) actividad típicamente asociada con malware o tráfico originado en direcciones IP maliciosas conocidas o dominios de red (por ejemplo, aquellos asociados con servidores de comando y control de botnets);

c) características de ataque conocidas (por ejemplo, denegación de servicio y desbordamientos de búfer);

d) comportamiento inusual del sistema (por ejemplo, registro de pulsaciones de teclas, inyección de procesos y desviaciones en el uso de protocolos estándar);

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

e) cuellos de botella y sobrecargas (por ejemplo, colas de red, niveles de latencia y fluctuación de la red);

f) acceso no autorizado (real o intentado) a sistemas o información;

g) análisis no autorizado de aplicaciones, sistemas y redes empresariales;

h) intentos exitosos y fallidos de acceder a recursos protegidos (por ejemplo, servidores DNS, portales web y sistemas de archivos);

i) comportamiento inusual del usuario y del sistema en relación con el comportamiento esperado.

Se sugiere utilizar el monitoreo continuo a través de una herramienta de monitoreo. Se recomienda que el monitoreo se haga en tiempo real o en intervalos periódicos, sujeto a las necesidades y capacidades de la organización. Se sugiere que las herramientas de monitoreo incluyan la capacidad de manejar grandes cantidades de datos, adaptarse a un panorama de amenazas en constante cambio y permitir la notificación en tiempo real. Las herramientas también se sugiere sean capaces de reconocer firmas y datos específicos o patrones de comportamiento de red o aplicación.

El software de supervisión automatizado se sugiere configurar para generar alertas (por ejemplo, a través de consolas de gestión, mensajes de correo electrónico o sistemas de mensajería instantánea) en función de umbrales predefinidos. Se recomienda que el sistema de alerta se ajuste y capacite en la línea de base de la organización para minimizar los falsos positivos. El personal se sugiere estar dedicado a responder ante las alertas y se recomienda estar debidamente capacitado para interpretar con precisión los posibles incidentes. Es conveniente haber sistemas y procesos redundantes para recibir y responder las notificaciones de alerta.

Los eventos anormales se sugiere se comuniquen a las partes pertinentes para mejorar las siguientes actividades: auditoría, evaluación de la seguridad, análisis y supervisión de vulnerabilidades (ver el inciso 5.25). Es conveniente establecer procedimientos para responder oportunamente a los indicadores positivos del sistema de vigilancia, a fin de reducir al mínimo el efecto de los acontecimientos adversos (ver el inciso 5.26) en la seguridad de la información. También se sugiere establecer procedimientos para identificar y abordar los falsos positivos, incluido el ajuste del software de monitoreo para reducir el número de futuros falsos positivos.

Otros datos

La supervisión de la seguridad se puede mejorar mediante:

a) aprovechar los sistemas de inteligencia sobre amenazas (ver el inciso 5.7);

b) aprovechar las capacidades de aprendizaje automático e inteligencia artificial;

c) utilizar listas de bloqueo o listas de permitidos;

d) llevar a cabo una serie de evaluaciones técnicas de seguridad (por ejemplo, evaluaciones de vulnerabilidad, pruebas de penetración, simulaciones de ciberataques y ejercicios de Ciber respuesta), y utilizar los resultados de estas

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

evaluaciones para ayudar a determinar las líneas de base o el comportamiento aceptable;

e) utilizar sistemas de supervisión del rendimiento para ayudar a establecer y detectar comportamientos anómalos;

f) aprovechar los registros en combinación con los sistemas de seguimiento.

Las actividades de monitoreo a menudo se llevan a cabo utilizando software especializado, como los sistemas de detección de intrusiones. Estos se pueden configurar para una línea de base de actividades normales, aceptables y esperadas del sistema y la red.

El monitoreo de comunicaciones anómalas ayuda en la identificación de botnets (es decir, un conjunto de dispositivos bajo el control malicioso del propietario de la botnet, generalmente utilizado para montar ataques distribuidos de denegación de servicio en otras computadoras de otras organizaciones). Si la computadora está siendo controlada por un dispositivo externo, hay una comunicación entre el dispositivo infectado y el controlador. Por lo tanto, se recomienda que la organización empleé tecnologías para supervisar las comunicaciones anómalas y tomar las medidas necesarias.

8.17 Sincronización del reloj

Tipo de control	Propiedades de Seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Detectivo	#Integridad	#Proteger #Detectar	#Gestión_de_eventos_de_seguridad_de_la_información	#Protección#Defensa

Control

Los relojes de los sistemas de procesamiento de información utilizados por la organización se sugiere sincronizar con las fuentes de tiempo aprobadas.

Propósito

Permitir la correlación y el análisis de eventos relacionados con la seguridad y otros datos registrados, y apoyar las investigaciones sobre incidentes de seguridad de la información.

Orientación

Los requisitos externos e internos para la representación del tiempo, se sugiere que la sincronización confiable y la precisión se documente e implemente. Dichos requisitos pueden provenir de las necesidades legales, estatutarias, reglamentarias, contractuales, de normas y de supervisión interna. Se sugiere definir y considerar un tiempo de referencia estándar para su uso dentro de la organización para todos los sistemas, incluidos los sistemas de gestión de edificios, los sistemas de entrada y salida y otros que pueden utilizarse para ayudar a las investigaciones.

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

Un reloj vinculado a una emisión de radio y hora desde un reloj atómico nacional o un sistema de posicionamiento global (GPS) se recomienda utilizarse como reloj de referencia para los sistemas de registro; una fuente de fecha y hora consistente y confiable para garantizar marcas de tiempo precisas. Se sugiere utilizar protocolos como el protocolo de tiempo de red (NTP) o el protocolo de tiempo de precisión (PTP) para mantener todos los sistemas en red sincronizados con un reloj de referencia.

La organización puede utilizar dos fuentes de tiempo externas al mismo tiempo para mejorar la fiabilidad de los relojes externos y gestionar adecuadamente cualquier variación.

La sincronización del reloj puede ser difícil cuando se usan varios servicios en la nube o cuando se usan servicios en la nube y locales. En este caso, es conveniente monitorear el reloj de cada servicio y registrar la diferencia para mitigar los riesgos derivados de las discrepancias.

Otros datos

La configuración correcta de los relojes de computadora es importante para garantizar la precisión de los registros de eventos, que pueden ser necesarios para investigaciones o como evidencia en casos legales y disciplinarios. Los registros de auditoría inexactos pueden obstaculizar tales investigaciones y dañar la credibilidad de dichas pruebas.

8.18 Uso de programas de utilerías privilegiadas

Tipo de control	Propiedades de Seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Seguridad_de_sistemas_y_redes#Configuración_segura#Seguridad_de_aplicaciones	#Protección

Control

El uso de programas de utilerías que pueden ser capaces de anular los controles del sistema y la aplicación se recomienda restringir y controlarse estrictamente.

Propósito

Para garantizar que el uso de programas de utilería no dañe los controles del sistema y las aplicaciones para la seguridad de la información.

Orientación

Se sugiere considerar las siguientes pautas para el uso de programas de utilidad que pueden ser capaces de anular los controles del sistema y la aplicación:

a) limitación del uso de programas de utilería al número práctico mínimo de usuarios autorizados de confianza (ver el inciso 8.2);

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

b) el uso de procedimientos de identificación, autenticación y autorización para los programas de servicios públicos, incluida la identificación única de la persona que utiliza el programa de servicios públicos;

c) definir y documentar los niveles de autorización para los programas de servicios públicos;

d) autorización para el uso ad hoc de programas de utilería;

e) no poner programas de utilidad a disposición de los usuarios que tengan acceso a las aplicaciones en sistemas en los que se requiera la segregación de funciones;

f) eliminar o deshabilitar todos los programas de utilidad innecesarios;

g) como mínimo, segregación lógica de los programas de utilidad del software de aplicación. Cuando sea práctico, separar las comunicaciones de red para dichos programas del tráfico de aplicaciones;

h) limitación de la disponibilidad de programas de utilidad (por ejemplo, durante la duración de un cambio autorizado);

i) registro de todo uso de programas de utilidad.

Otros datos

La mayoría de los sistemas de información tienen uno o más programas de utilidad que pueden ser capaces de anular los controles del sistema y de las aplicaciones, por ejemplo, diagnósticos, parches, antivirus, desfragmentadores de disco, depuradores, copias de seguridad y herramientas de red.

8.19 Instalación de software en sistemas operativos

Tipo de control	Propiedades de Seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Configuración_segura#Seguridad_de_aplicaciones	#Protección

Control

Se sugiere implementar procedimientos y medidas para administrar de forma segura la instalación de software en los sistemas operativos.

Propósito

Asegurar la integridad de los sistemas operativos y evitar la explotación de vulnerabilidades técnicas.

Orientación

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

Se recomienda considerar las siguientes pautas para administrar de forma segura los cambios y la instalación de software en los sistemas operativos:

a) realizar actualizaciones de software operativo solo por administradores capacitados previa autorización de gestión adecuada (ver el inciso 8.5);

b) garantizar que solo se instale código ejecutable aprobado y ningún código de desarrollo o compiladores en los sistemas operativos;

c) únicamente instalar y actualizar software después de pruebas exhaustivas y exitosas (ver el inciso 8.29 y el inciso 8.31);

d) actualizar todas las bibliotecas de origen de programas correspondientes;

e) utilizar un sistema de control de la configuración para mantener el control de todo el software operativo, así como de la documentación del sistema;

f) definir una estrategia de reversión antes de que se implementen los cambios;

g) mantener un registro de auditoría de todas las actualizaciones del software operativo;

h) archivar versiones antiguas del software, junto con toda la información y parámetros requeridos, procedimientos, detalles de configuración y software de soporte como medida de contingencia, y durante el tiempo que el software sea necesario para leer o procesar datos archivados.

Cualquier decisión de actualizar a una nueva versión se sugiere tener en cuenta los requisitos empresariales para el cambio y la seguridad de la versión (por ejemplo, la introducción de una nueva funcionalidad de seguridad de la información o el número y la gravedad de las vulnerabilidades de seguridad de la información que afectan a la versión actual). Los parches de software deberían aplicarse cuando puedan ayudar a eliminar o reducir las vulnerabilidades de seguridad de la información (ver el inciso 8.8 y el inciso 8.19).

El software informático puede basarse en software y paquetes suministrados externamente (por ejemplo, programas de software que utilizan módulos que están alojados en sitios externos), que se sugiere ser monitoreados y controlados para evitar cambios no autorizados, ya que pueden introducir vulnerabilidades de seguridad de la información.

El software suministrado por el proveedor utilizado en los sistemas operativos se sugiere mantener a un nivel respaldado por el proveedor. Con el tiempo, los proveedores de software dejan de admitir versiones anteriores de software. Se sugiere que la organización considere los riesgos de confiar en software no compatible. El software de código abierto utilizado en los sistemas operativos se sugiere mantener hasta la última versión apropiada del software. Con el tiempo, el código fuente abierto puede dejar de mantenerse, pero todavía está disponible en un repositorio de software de código abierto. Se recomienda que la organización también considere los riesgos de confiar en software de código abierto sin mantenimiento cuando se utiliza en sistemas operativos.

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

Cuando los proveedores participan en la instalación o actualización de software, el acceso físico o lógico solo debería darse cuando sea necesario y con la autorización adecuada. Las actividades del proveedor se sugiere sean monitoreadas (ver el inciso 5.22).

Es conveniente que la organización defina y aplicar reglas estrictas sobre qué tipos de software pueden instalar los usuarios.

El principio de privilegios mínimos se sugiere aplicar a la instalación de programas informáticos en sistemas operativos. Es conveniente que la organización identifique qué tipos de instalaciones de software están permitidas (por ejemplo, actualizaciones y parches de seguridad para el software existente) y qué tipos de instalaciones están prohibidas (por ejemplo, software que es solo para uso personal y software cuyo pedigrí con respecto a ser potencialmente malicioso es desconocido o sospechoso). Estos privilegios se sugiere conceder en función de las funciones de los usuarios afectados.

Otros datos

No hay otra información.

8.20 Seguridad de redes

Tipo de control	Propiedades de Seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo #Detectivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger #Detectar	#Seguridad_de_sistemas_y_redes	#Protección

Control

Las redes y los dispositivos de red es conveniente estén protegidos, gestionados y controlados para proteger la información en sistemas y aplicaciones.

Propósito

Proteger la información en las redes y sus instalaciones de procesamiento de información de apoyo del compromiso a través de la red.

Orientación

Se recomienda aplicar controles para garantizar la seguridad de la información en las redes y proteger los servicios conectados del acceso no autorizado. En particular, se sugiere tener en cuenta los siguientes puntos:

a) el tipo y el nivel de clasificación de la información que la red puede soportar;

b) establecer responsabilidades y procedimientos para la gestión de equipos y dispositivos de red;

c) mantener la documentación actualizada, incluidos los diagramas de red y los archivos de configuración de los dispositivos (por ejemplo, enrutadores, conmutadores);

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

d) separar la responsabilidad operativa de las redes de las operaciones de los sistemas de TIC cuando proceda (ver el inciso 5.3);

e) establecer controles para salvaguardar la confidencialidad y la integridad de los datos que pasan a través de redes públicas, redes de terceros o a través de redes inalámbricas y para proteger los sistemas y aplicaciones conectados (ver el inciso 5.22, el inciso 8.24, el inciso 5.14 y el inciso 6.6). También se pueden requerir controles adicionales para mantener la disponibilidad de los servicios de red y los equipos conectados a la red;

f) el registro y el seguimiento adecuados para permitir el registro y la detección de acciones que puedan afectar a la seguridad de la información o que sean pertinentes para ella (ver el inciso 8.16 y el inciso 8.15);

g) coordinar estrechamente las actividades de gestión de la red tanto para optimizar el servicio a la organización como para garantizar que los controles se apliquen de manera coherente en toda la infraestructura de procesamiento de la información;

h) autenticación de sistemas en la red;

i) restringir y filtrar la conexión de los sistemas a la red (por ejemplo, mediante cortafuegos);

j) Detectar, restringir y autenticar la conexión de equipos y dispositivos a la red;

k) endurecimiento de los dispositivos de red;

l) separar los canales de administración de red de otro tráfico de red;

m) aislar temporalmente las subredes críticas (por ejemplo, con puentes levadizos) si la red está siendo atacada;

n) deshabilitar los protocolos de red vulnerables.

Es conveniente que la organización se asegure de que se aplican los controles de seguridad adecuados al uso de redes virtualizadas. Las redes virtualizadas también cubren redes definidas por software (SDN, SD-WAN). Las redes virtualizadas pueden ser deseables desde el punto de vista de la seguridad, ya que pueden permitir la separación lógica de la comunicación que tiene lugar a través de redes físicas, particularmente para sistemas y aplicaciones que se implementan utilizando computación distribuida.

Otros datos

Puede encontrar información adicional sobre la seguridad de la red en la serie de normas que se indica en el inciso 10.32.

Puede encontrar más información sobre las redes virtualizadas en la norma que se indica en el inciso 10.22.

8.21 Seguridad de los servicios de red

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

Tipo de control	Propiedades de Seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Seguridad_de_sistemas_y_redes	#Protección

Control

Se recomienda identificar, implementar y supervisar los mecanismos de seguridad, los niveles de servicio y los requisitos de servicio de los servicios de red.

Propósito

Garantizar la seguridad en el uso de los servicios de red.

Orientación

Las medidas de seguridad necesarias para servicios particulares, como las características de seguridad, los niveles de servicio y los requisitos de servicio, se sugiere sean identificadas y aplicadas (por proveedores de servicios de red internos o externos). Se sugiere que la organización se asegure de que los proveedores de servicios de red implementen estas medidas.

Es conveniente que la capacidad del proveedor de servicios de red para gestionar los servicios acordados de forma segura se determinen y supervisen periódicamente. Es conveniente que el derecho a la auditoría sea acordado entre la organización y el proveedor. Se sugiere que la organización también considere las certificaciones de terceros proporcionadas por los proveedores de servicios para demostrar que mantienen las medidas de seguridad adecuadas.

Se recomienda formular y aplicar normas sobre el uso de redes y servicios de red que abarquen:

a) las redes y servicios de red a los que se permite acceder;

b) requisitos de autenticación para acceder a diversos servicios de red;

c) procedimientos de autorización para determinar quién puede acceder a qué redes y servicios en red;

d) gestión de la red y controles y procedimientos tecnológicos para proteger el acceso a las conexiones de red y los servicios de red;

e) los medios utilizados para acceder a las redes y servicios de red [por ejemplo, el uso de una red privada virtual (VPN) o una red inalámbrica];

f) hora, ubicación y otros atributos del usuario en el momento del acceso;

g) seguimiento del uso de los servicios de red.

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

Se sugiere tener en cuenta las siguientes características de seguridad de los servicios de red:

a) la tecnología aplicada a la seguridad de los servicios de red, como la autenticación, el cifrado y los controles de conexión de red;

b) los parámetros técnicos necesarios para una conexión segura con los servicios de red de conformidad con las normas de seguridad y conexión de red;

c) el almacenamiento en caché (por ejemplo, en una red de distribución de contenidos) y sus parámetros que permiten a los usuarios elegir el uso del almacenamiento en caché de acuerdo con los requisitos de rendimiento, disponibilidad y confidencialidad;

d) procedimientos para el uso del servicio de red para restringir el acceso a los servicios o aplicaciones de red, cuando sea necesario.

Otros datos

Los servicios de red incluyen la provisión de conexiones, servicios de red privada y soluciones de seguridad de red administradas, como firewalls y sistemas de detección de intrusiones. Estos servicios pueden variar desde un simple ancho de banda no administrado hasta ofertas complejas de valor agregado.

En la norma que se indica en el inciso 10.46 se ofrece más orientación sobre un marco para la gestión del acceso.

8.22 Segregación de redes

Tipo de control	Propiedades de Seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Seguridad_de_sistemas_y_redes	#Protección

Control

Los grupos de servicios de información, usuarios y sistemas de información se recomienda estén segregados en las redes de la organización.

Propósito

Dividir la red en límites de seguridad y controlar el tráfico entre ellos en función de las necesidades del negocio.

Orientación

Se sugiere que la organización considere la gestión de la seguridad de las grandes redes dividiéndolas en dominios de red separados y separándolas de la red pública (es decir, Internet). Los dominios se pueden elegir en función de los niveles de confianza, criticidad

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

y sensibilidad (por ejemplo, dominio de acceso público, dominio de escritorio, dominio de servidor, sistemas de bajo y alto riesgo), a lo largo de unidades organizativas (por ejemplo, recursos humanos, finanzas, marketing) o alguna combinación (por ejemplo, dominio de servidor que se conecta a múltiples unidades organizativas). La segregación se puede hacer utilizando redes físicamente diferentes o utilizando diferentes redes lógicas.

Es conveniente que el perímetro de cada dominio este bien definido. Si se permite el acceso entre dominios de red, se sugiere controlar en el perímetro mediante una puerta de enlace (por ejemplo, firewall, enrutador de filtrado). Los criterios para la segregación de redes en dominios, y el acceso permitido a través de las pasarelas, se recomienda se basen en una evaluación de los requisitos de seguridad de cada dominio. La evaluación es conveniente se ajuste a la política temática específica sobre control de acceso (ver el inciso 5.15), requisitos de acceso, valor y clasificación de la información tratada y tener en cuenta el coste relativo y el impacto en el rendimiento de la incorporación de una tecnología de pasarela adecuada.

Las redes inalámbricas requieren un tratamiento especial debido al perímetro de red mal definido. Se sugiere considerar el ajuste de la cobertura de radio para la segregación de redes inalámbricas. En el caso de los entornos sensibles, se sugiere considerar la posibilidad de tratar todo el acceso inalámbrico como conexiones externas y de separar este acceso de las redes internas hasta que el acceso haya pasado a través de una puerta de enlace de conformidad con los controles de red (ver el inciso 8.20) antes de conceder acceso a los sistemas internos. La red de acceso inalámbrico para invitados se sugiere separarse de las del personal si el personal solo usa dispositivos de punto final de usuario controlado que cumplan con las políticas específicas del tema de la organización. Se recomienda que el WiFi para huéspedes tenga al menos las mismas restricciones que WiFi para el personal, con el fin de desalentar el uso de WiFi para huéspedes por parte del personal.

Otros datos

Las redes a menudo se extienden más allá de los límites de la organización, ya que se forman asociaciones comerciales que requieren la interconexión o el intercambio de instalaciones de procesamiento de información y redes. Tales extensiones pueden aumentar el riesgo de acceso no autorizado a los sistemas de información de la organización que utilizan la red, algunos de los cuales requieren protección de otros usuarios de la red debido a su sensibilidad o criticidad.

8.23 Filtrado web

Tipo de control	Propiedades de Seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Seguridad_de_sistemas_y_redes	#Protección

Control

El acceso a sitios web externos se sugiere gestionar para reducir la exposición a contenido malicioso.

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

Propósito

Para proteger los sistemas de ser comprometidos por malware y para evitar el acceso a recursos web no autorizados.

Orientación

Es conveniente que la organización reduzca los riesgos de que su personal acceda a sitios web que contienen información ilegal o que se sabe que contienen virus o material de phishing. Una técnica para lograr esto funciona mediante el bloqueo de la dirección IP o el dominio de los sitios web en cuestión. Algunos navegadores y tecnologías antimalware hacen esto automáticamente o se pueden configurar para hacerlo.

Se sugiere que la organización identifique los tipos de sitios web a los que el personal se recomienda tener acceso. Es conveniente que la organización considere bloquear el acceso a los siguientes tipos de sitios web:

a) sitios web que tienen una función de carga de información a menos que esté permitido por razones comerciales válidas;

b) sitios web maliciosos conocidos o sospechosos (por ejemplo, aquellos que distribuyen malware o contenido de phishing);

c) servidores de mando y control;

d) sitio web malicioso adquirido a partir de inteligencia de amenazas (ver el inciso 5.7);

e) sitios web que comparten contenido ilegal.

Antes de implementar este control, se sugiere que la organización establezca reglas para el uso seguro y apropiado de los recursos en línea, incluida cualquier restricción a sitios web indeseables o inapropiados y aplicaciones basadas en la web. Se recomienda que las normas se mantengan actualizadas.

Se sugiere impartir capacitación al personal sobre el uso seguro y apropiado de los recursos en línea, incluido el acceso a la web. Es conveniente que la capacitación incluya las reglas de la organización, el punto de contacto para plantear problemas de seguridad y el proceso de excepción cuando se sugiere acceder a recursos web restringidos por razones comerciales legítimas. También se recomienda capacitar al personal para garantizar que no anule ningún aviso del navegador que informe que un sitio web no es seguro, pero permita al usuario continuar.

Otros datos

El filtrado web puede incluir una variedad de técnicas que incluyen firmas, heurística, lista de sitios web o dominios aceptables, lista de sitios web o dominios prohibidos y configuración a medida para ayudar a evitar que el software malicioso y otras actividades maliciosas ataquen la red y los sistemas de la organización.

8.24 Uso de la criptografía

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

Tipo de control	Propiedades de Seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Configuración_ segura	#Protección

Control

Se sugiere definirse e implementarse reglas para el uso efectivo de la criptografía, incluida la administración de claves criptográficas.

Propósito

Garantizar el uso adecuado y efectivo de la criptografía para proteger la confidencialidad, autenticidad o integridad de la información de acuerdo con los requisitos comerciales y de seguridad de la información, y teniendo en cuenta los requisitos legales, estatutarios, reglamentarios y contractuales relacionados con la criptografía.

Orientación

General

Al utilizar la criptografía, se recomienda tener en cuenta lo siguiente:

a) la política específica sobre criptografía definida por la organización, incluidos los principios generales para la protección de la información. Es necesaria una política temática específica sobre el uso de la criptografía para maximizar los beneficios y minimizar los riesgos del uso de técnicas criptográficas y evitar el uso inapropiado o incorrecto;

b) identificar el nivel de protección requerido y la clasificación de la información y, en consecuencia, establecer el tipo, la fuerza y la calidad de los algoritmos criptográficos requeridos;

c) el uso de criptografía para la protección de la información contenida en dispositivos de punto final de usuario móvil o medios de almacenamiento y transmitida a través de redes a dichos dispositivos o medios de almacenamiento;

d) el enfoque de la gestión de claves, incluidos los métodos para abordar la generación y protección de claves criptográficas y la recuperación de información cifrada en caso de claves perdidas, comprometidas o dañadas;

e) funciones y responsabilidades para:

1) la aplicación de las normas para el uso eficaz de la criptografía;

2) la gestión de claves, incluida la generación de claves (ver el inciso 8.24);

f) las normas que se adoptan, así como los algoritmos criptográficos, la fuerza de cifrado, las soluciones criptográficas y las prácticas de uso aprobadas o requeridas para su uso en la organización;

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

g) el impacto del uso de información cifrada en los controles que se basan en la inspección de contenidos (por ejemplo, detección de malware o filtrado de contenidos).

Al aplicar las normas de la organización para el uso eficaz de la criptografía, se sugiere tener en cuenta las reglamentaciones y restricciones nacionales que pueden aplicarse al uso de técnicas criptográficas en diferentes partes del mundo, así como las cuestiones del flujo transfronterizo de información cifrada (ver el inciso 5.31).

El contenido de los acuerdos de nivel de servicio o los contratos con proveedores externos de servicios criptográficos (por ejemplo, con una autoridad de certificación) se sugiere abarcar cuestiones de responsabilidad, fiabilidad de los servicios y plazos de respuesta para la prestación de servicios (ver el inciso 5.22).

Gestión de claves

La administración adecuada de claves requiere procesos seguros para generar, almacenar, archivar, recuperar, distribuir, retirar y destruir claves criptográficas.

Es conveniente que un sistema de gestión clave se base en un conjunto acordado de normas, procedimientos y métodos seguros para:

a) generar claves para diferentes sistemas criptográficos y diferentes aplicaciones;

b) expedir y obtener certificados de clave pública;

c) distribuir claves a las entidades previstas, incluida la forma de activar las claves cuando se reciban;

d) almacenar claves, incluida la forma en que los usuarios autorizados obtienen acceso a las claves;

e) cambiar o actualizar claves, incluidas las reglas sobre cuándo cambiar las claves y cómo se hará;

f) tratar con claves comprometidas;

g) revocar claves, incluida la forma de retirar o desactivar claves [por ejemplo, cuando las claves se han visto comprometidas o cuando un usuario abandona una organización (en cuyo caso las claves también se sugiere archivar)];

h) recuperar claves que se pierden o están dañadas;

i) copia de seguridad o archivado de claves;

j) destruir llaves;

k) registro y auditoría de actividades clave relacionadas con la gestión;

l) establecer fechas de activación y desactivación de las claves para que las claves solo puedan usarse durante el período de tiempo de acuerdo con las reglas de la organización sobre la gestión de claves;

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

m) gestionar las solicitudes legales de acceso a claves criptográficas (por ejemplo, se puede exigir que la información cifrada esté disponible de forma no cifrada como prueba en un caso judicial).

Todas las claves criptográficas se sugiere estén protegidas contra modificaciones y pérdidas. Además, las claves secretas y privadas necesitan protección contra el uso no autorizado, así como la divulgación. El equipo utilizado para generar, almacenar y archivar claves es conveniente este protegido físicamente.

Además de la integridad, para muchos casos de uso, también se sugiere considerar la autenticidad de las claves públicas.

Otros datos

La autenticidad de las claves públicas generalmente se aborda mediante procesos de administración de claves públicas que utilizan autoridades de certificación y certificados de clave pública, pero también es posible abordarla mediante el uso de tecnologías como la aplicación de procesos manuales para claves de números pequeños.

La criptografía se puede utilizar para lograr diferentes objetivos de seguridad de la información, por ejemplo:

a) confidencialidad: utilizar el cifrado de la información para proteger la información sensible o crítica, ya sea almacenada o transmitida;

b) integridad o autenticidad: uso de firmas digitales o códigos de autenticación de mensajes para verificar la autenticidad o integridad de la información sensible o crítica almacenada o transmitida. Uso de algoritmos con el fin de verificar la integridad de los archivos;

c) no repudio: uso de técnicas criptográficas para proporcionar evidencia de la ocurrencia o no ocurrencia de un evento o acción;

d) autenticación: uso de técnicas criptográficas para autenticar a los usuarios y otras entidades del sistema que solicitan acceso o realizan transacciones con usuarios, entidades y recursos del sistema.

La serie de normas que se indica en el inciso 10.3 proporciona más información sobre la gestión de claves.

8.25 Ciclo de vida de desarrollo seguro

Tipo de control	Propiedades de Seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Seguridad_de_aplicaciones#Seguridad_de_sistemas_y_redes	#Protección

Control

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

Se recomienda establecer y aplicarse normas para el desarrollo seguro de programas informáticos y sistemas.

Propósito

Para garantizar que la seguridad de la información se diseñe e implemente dentro del ciclo de vida de desarrollo seguro del software y los sistemas.

Orientación

El desarrollo seguro es un requisito para construir un servicio, arquitectura, software y sistemas seguros. Para lograr esto, se sugiere considerar los siguientes aspectos:

a) separación de los entornos de desarrollo, ensayo y producción (ver el inciso 8.31);

b) orientación sobre la seguridad en el ciclo de vida del desarrollo de software:

1) seguridad en la metodología de desarrollo de programas informáticos (ver el inciso 8.28 y el inciso 8.27);

2) directrices de codificación segura para cada lenguaje de programación utilizado (ver el inciso 8.28);

c) requisitos de seguridad en la fase de especificación y diseño (ver el inciso 5.8);

d) puntos de control de seguridad en los proyectos (ver el inciso 5.8);

e) pruebas de sistemas y seguridad, como pruebas de regresión, análisis de código y pruebas de penetración (ver el inciso 8.29);

f) repositorios seguros para el código fuente y la configuración (ver el inciso 8.4 y el inciso 8.9);

g) seguridad en el control de versiones (ver el inciso 8.32);

h) los conocimientos y la formación necesarios en materia de seguridad de las aplicaciones (ver el inciso 8.28);

i) la capacidad de los desarrolladores para prevenir, encontrar y corregir vulnerabilidades (ver el inciso 8.28);

j) requisitos y alternativas de concesión de licencias para garantizar soluciones rentables evitando al mismo tiempo futuros problemas de concesión de licencias (ver el inciso 5.32).

Si el desarrollo se subcontrata, es conveniente que la organización obtenga la seguridad de que el proveedor cumple con las reglas de la organización para el desarrollo seguro (ver el inciso 8.30).

Otros datos

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

El desarrollo también puede tener lugar dentro de las aplicaciones, como aplicaciones de oficina, scripting, navegadores y bases de datos.

8.26 Requisitos de seguridad de las aplicaciones

Tipo de control	Propiedades de Seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Seguridad_de_aplicaciones#Seguridad_de_sistemas_y_redes	#Protección#Defensa

Control

Se sugiere que los requisitos de seguridad de la información se identifiquen, especifiquen y aprueben al desarrollar o adquirir aplicaciones.

Propósito

Garantizar que todos los requisitos de seguridad de la información se identifiquen y aborden al desarrollar o adquirir aplicaciones.

Orientación

General

Los requisitos de seguridad de las aplicaciones se sugiere identificarse y especificarse. Estos requisitos generalmente se determinan a través de una evaluación de riesgos. Los requisitos es conveniente desarrollarse con el apoyo de especialistas en seguridad de la información.

Los requisitos de seguridad de la aplicación pueden cubrir una amplia gama de temas, dependiendo del propósito de la aplicación.

Los requisitos de seguridad de las aplicaciones se recomienda incluyan, según proceda:

a) nivel de confianza en la identidad de las entidades [por ejemplo, mediante autenticación (ver el inciso 5.17, el inciso 8.2 y el inciso 8.5)];

b) identificar el tipo de información y el nivel de clasificación que es conveniente procesar la solicitud;

c) necesidad de segregación del acceso y del nivel de acceso a los datos y funciones de la aplicación;

d) resiliencia frente a ataques malintencionados o interrupciones involuntarias [por ejemplo, protección contra el desbordamiento del búfer o inyecciones de lenguaje de consulta estructurado (SQL)];

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

e) requisitos legales, legales y reglamentarios en la jurisdicción donde se genera, procesa, completa o almacena la transacción;

f) necesidad de privacidad asociada con todas las partes implicadas;

g) los requisitos de protección de cualquier información confidencial;

h) protección de los datos durante el tratamiento, en tránsito y en reposo;

i) necesidad de cifrar de forma segura las comunicaciones entre todas las partes implicadas;

j) controles de entrada, incluidas las comprobaciones de integridad y la validación de entradas;

k) controles automatizados (por ejemplo, límites de homologación o aprobaciones dobles);

l) controles de salida, considerando también quién puede acceder a las salidas y su autorización;

m) restricciones en torno al contenido de los campos de "texto libre", ya que pueden dar lugar a un almacenamiento incontrolado de datos confidenciales (por ejemplo, datos personales);

n) requisitos derivados del proceso empresarial, como el registro y la supervisión de transacciones, los requisitos de no repudio;

o) requisitos exigidos por otros controles de seguridad (por ejemplo, interfaces para sistemas de registro y supervisión o detección de fugas de datos);

p) manejo de mensajes de error.

Servicios transaccionales

Además, para las aplicaciones que ofrecen servicios transaccionales entre la organización y un socio, se sugiere tener en cuenta lo siguiente al identificar los requisitos de seguridad de la información:

a) el nivel de confianza que cada parte requiere en la identidad reivindicada de la otra;

b) el nivel de confianza requerido en la integridad de la información intercambiada o tratada y los mecanismos para identificar la falta de integridad (por ejemplo, comprobación de redundancia cíclica, hashing, firmas digitales);

c) los procesos de autorización asociados con quién puede aprobar el contenido, emitir o firmar documentos transaccionales clave;

d) confidencialidad, integridad, prueba de envío y recepción de documentos clave y el no repudio (por ejemplo, contratos asociados con procesos de licitación y contrato);

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

e) la confidencialidad e integridad de cualquier transacción (por ejemplo, pedidos, detalles de la dirección de entrega y confirmación de los recibos);

f) requisitos sobre cuánto tiempo se recomienda mantener la confidencialidad de una transacción;

g) seguros y otros requisitos contractuales.

Solicitudes electrónicas de pedidos y pagos

Además, para las solicitudes que involucran pedidos y pagos electrónicos, se sugiere considerar lo siguiente:

a) requisitos para mantener la confidencialidad e integridad de la información de los pedidos;

b) el grado de verificación adecuado para verificar la información de pago facilitada por un cliente;

c) evitar la pérdida o duplicación de la información de las transacciones;

d) almacenar los detalles de la transacción fuera de cualquier entorno de acceso público (por ejemplo, en una plataforma de almacenamiento existente en la intranet de la organización, y no conservada y expuesta en medios de almacenamiento electrónico directamente accesibles desde Internet);

e) cuando se utiliza una autoridad de confianza (por ejemplo, con el fin de emitir y mantener firmas digitales o certificados digitales), la seguridad se integra e integra a lo largo de todo el proceso de gestión de certificados o firmas de extremo a extremo.

Varias de las consideraciones anteriores pueden abordarse mediante la aplicación de la criptografía (ver el inciso 8.24), teniendo en cuenta los requisitos legales (ver el inciso 5.31 al inciso 5.36, especialmente el inciso 5.31 para la legislación sobre criptografía).

Otros datos

Las aplicaciones accesibles a través de redes están sujetas a una serie de amenazas relacionadas con la red, como actividades fraudulentas, disputas contractuales o divulgación de información al público; transmisión incompleta, enrutamiento incorrecto, alteración no autorizada de mensajes, duplicación o reproducción. Por lo tanto, las evaluaciones detalladas de riesgos y la determinación cuidadosa de los controles son indispensables. Los controles requeridos a menudo incluyen métodos criptográficos para la autenticación y la seguridad de la transferencia de datos.

Puede encontrar más información sobre la seguridad de las aplicaciones en la serie de normas que se indica en el inciso 10.33.

8.27 Arquitectura de sistemas seguros y principios de ingeniería

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

Tipo de control	Propiedades de Seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Seguridad_de_aplicaciones#Seguridad_de_sistemas_y_redes	#Protección#Defensa

Control

Se recomienda que los principios para la ingeniería de sistemas seguros establezca, documente, mantenga y aplique a cualquier actividad de desarrollo de sistemas de información.

Propósito

Garantizar que los sistemas de información se diseñen, implementen y operen de forma segura dentro del ciclo de vida del desarrollo.

Orientación

Se sugiere que los principios de ingeniería de seguridad establezcan, documenten y apliquen a las actividades de ingeniería de sistemas de información. La seguridad se sugiere se diseñe en todas las capas de la arquitectura (negocios, datos, aplicaciones y tecnología). La nueva tecnología se recomienda se analice en busca de riesgos de seguridad y el diseño es conveniente se revise en función de los patrones de ataque conocidos.

Los principios de ingeniería segura proporcionan orientación sobre técnicas de autenticación de usuarios, control seguro de sesiones y validación y desinfección de datos.

Es conveniente que los principios de ingeniería de sistemas seguros incluya el análisis de:

a) toda la gama de controles de seguridad necesarios para proteger la información y los sistemas contra las amenazas identificadas;

b) las capacidades de los controles de seguridad para prevenir, detectar o responder ante eventos de seguridad;

c) controles de seguridad específicos requeridos por determinados procesos empresariales (por ejemplo, cifrado de información sensible, comprobación de integridad y firma digital de información);

d) dónde y cómo se sugiere aplicar los controles de seguridad (por ejemplo, integrándose con una arquitectura de seguridad y la infraestructura técnica);

e) cómo los controles de seguridad individuales (manuales y automatizados) trabajan juntos para producir un conjunto integrado de controles.

Es conveniente que los principios de ingeniería de seguridad tengan en cuenta:

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

a) la necesidad de integrarse con una arquitectura de seguridad;

b) infraestructura técnica de seguridad [por ejemplo, infraestructura de clave pública (PKI), gestión de identidad y acceso (IAM), prevención de fugas de datos y gestión dinámica del acceso];

c) capacidad de la organización para desarrollar y apoyar la tecnología elegida;

d) el costo, el tiempo y la complejidad del cumplimiento de los requisitos de seguridad;

e) las buenas prácticas actuales.

La ingeniería de sistemas seguros se sugiere implique:

a) el uso de principios de arquitectura de seguridad, como "seguridad por diseño", "defensa en profundidad", "seguridad por defecto", "denegación por defecto", "falla segura", "desconfianza en la entrada de aplicaciones externas", "seguridad en el despliegue", "asumir incumplimiento", "privilegios mínimos", "usabilidad y capacidad de gestión" y "funcionalidad mínima";

b) una revisión del diseño orientada a la seguridad para ayudar a identificar las vulnerabilidades de seguridad de la información, garantizar que se especifiquen los controles de seguridad y cumplir los requisitos de seguridad;

c) documentación y reconocimiento formal de los controles de seguridad que no cumplen plenamente los requisitos (por ejemplo, debido a requisitos de seguridad primordiales);

d) endurecimiento de sistemas.

Es conveniente que la organización considere los principios de "confianza cero" tales como:

a) asumiendo que los sistemas de información de la organización ya están violados y, por lo tanto, no dependen solo de la seguridad del perímetro de la red;

b) emplear un enfoque de "nunca confiar y siempre verificar" para el acceso a los sistemas de información;

c) garantizar que las solicitudes a los sistemas de información se cifren de extremo a extremo;

d) verificar cada solicitud a un sistema de información como si se originara en una red abierta y externa, incluso si estas solicitudes se originaron internamente en la organización (es decir, no confiar automáticamente en nada dentro o fuera de sus perímetros);

e) utilizando técnicas de "privilegios mínimos" y de control dinámico del acceso (Ver el inciso 5.15, el inciso 5.18 y el inciso 8.2). Esto incluye autenticar y autorizar solicitudes de información o a sistemas basados en información contextual, como información de autenticación (ver el inciso 5.17), identidades de usuario (ver el

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

inciso 5.16), datos sobre el dispositivo de punto final del usuario y clasificación de datos (ver el inciso 5.12);

f) autenticar siempre a los solicitantes y validar siempre las solicitudes de autorización a los sistemas de información en función de la información, incluida la información de autenticación (ver el inciso 5.17) y las identidades de usuario (ver el inciso 5.16), los datos sobre el dispositivo de punto final del usuario y la clasificación de datos (ver el inciso 5.12), por ejemplo, aplicando una autenticación reforzada (por ejemplo, multifactor, ver el inciso 8.5).

Se sugiere que los principios de ingeniería de seguridad establecidos se apliquen, cuando proceda, al desarrollo externalizado de sistemas de información a través de los contratos y otros acuerdos vinculantes entre la organización y el proveedor al que la organización subcontrata. Se recomienda que la organización se asegure de que las prácticas de ingeniería de seguridad de los proveedores se alineen con las necesidades de la organización.

Se recomienda que los principios de ingeniería de seguridad y los procedimientos de ingeniería establecidos se revisen periódicamente para garantizar que contribuyan efectivamente a mejorar los estándares de seguridad dentro del proceso de ingeniería. También se sugiere revisar periódicamente para garantizar que se mantengan actualizados en términos de lucha contra cualquier nueva amenaza potencial y de seguir siendo aplicables a los avances en las tecnologías y soluciones que se están aplicando.

Otros datos

Los principios de ingeniería segura se pueden aplicar al diseño o configuración de una variedad de técnicas, tales como:

- tolerancia a fallas y otras técnicas de resiliencia;
- segregación (por ejemplo, a través de la virtualización o la contenedorización);
- resistencia a la manipulación.

Las técnicas de virtualización segura se pueden utilizar para evitar interferencias entre aplicaciones que se ejecutan en el mismo dispositivo físico. Si un atacante pone en peligro una instancia virtual de una aplicación, solo esa instancia se ve afectada. El ataque no tiene ningún efecto en ninguna otra aplicación o dato.

Las técnicas de resistencia a la manipulación se pueden utilizar para detectar la manipulación de contenedores de información, ya sea física (por ejemplo, una alarma antirrobo) o lógica (por ejemplo, un archivo de datos). Una característica de tales técnicas es que hay un registro del intento de manipular el contenedor. Además, el control puede evitar la extracción exitosa de datos a través de su destrucción (por ejemplo, la memoria del dispositivo se puede eliminar).

8.28 Codificación segura

Tipo de control	Propiedades de Seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Seguridad_de_aplicaciones#Seguridad_de_sistemas_y_redes	#Protección

Control

Los principios de codificación segura se sugiere aplicar al desarrollo de software.

Propósito

Para garantizar que el software se escriba de forma segura, reduciendo así el número de posibles vulnerabilidades de seguridad de la información en el software.

Orientación

General

Es conveniente que la organización establezca procesos en toda la organización para proporcionar un buen gobierno para la codificación segura. Se sugiere establecer y aplicar una línea de base mínima segura. Además, dichos procesos y gobernanza se recomienda ampliar para abarcar los componentes de software de terceros y el software de código abierto.

Es conveniente que la organización monitoreé las amenazas del mundo real y el asesoramiento e información actualizados sobre las vulnerabilidades del software para guiar los principios de codificación segura de la organización a través de la mejora continua y el aprendizaje. Esto puede ayudar a garantizar que se implementen prácticas efectivas de codificación segura para combatir el panorama de amenazas que cambia rápidamente.

Planificación y antes de la codificación

Se sugiere que los principios de codificación segura se utilicen tanto para nuevos desarrollos como en escenarios de reutilización. Estos principios se recomienda se apliquen a las actividades de desarrollo tanto dentro de la organización como para los productos y servicios suministrados por la organización a otros. Es conveniente que la planificación y los requisitos previos antes de la codificación se incluyan:

a) las expectativas específicas de la organización y los principios aprobados para la codificación segura que se utilizan tanto para los desarrollos de código internos como para los subcontratados;

b) prácticas y defectos de codificación comunes e históricos que conducen a vulnerabilidades de seguridad de la información;

c) configurar herramientas de desarrollo, como los entornos de desarrollo integrado (IDE), para ayudar a reforzar la creación de código seguro;

d) siguiendo las orientaciones emitidas por los proveedores de herramientas de desarrollo y entornos de ejecución, según corresponda;

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

e) mantenimiento y uso de herramientas de desarrollo actualizadas (por ejemplo, compiladores);

f) cualificación de los desarrolladores en la escritura de código seguro;

g) diseño y arquitectura seguros, incluida la modelización de amenazas;

h) normas de codificación seguras y, cuando proceda, exigir su uso;

i) uso de entornos controlados para el desarrollo.

Durante la codificación

Las consideraciones durante la codificación deberían incluir:

a) prácticas de codificación seguras específicas de los lenguajes de programación y las técnicas que se utilizan;

b) el uso de técnicas de programación seguras, como la programación en parejas, la refactorización, la revisión por pares, las iteraciones de seguridad y el desarrollo basado en pruebas;

c) el uso de técnicas de programación estructurada;

d) documentar el código y eliminar los defectos de programación, que pueden permitir explotar las vulnerabilidades de seguridad de la información;

e) prohibir el uso de técnicas de diseño inseguras (por ejemplo, el uso de contraseñas codificadas, ejemplos de código no aprobado y servicios web no autenticados).

Se sugiere que las pruebas se realicen durante y después del desarrollo (ver el inciso 8.29).

Los procesos estáticos de pruebas de seguridad de aplicaciones (SAST) pueden identificar vulnerabilidades de seguridad en el software.

Antes de que el software se ponga en funcionamiento, se recomienda evaluar lo siguiente:

a) la superficie de ataque y el principio de privilegios mínimos;

b) realizar un análisis de los errores de programación más comunes y documentar que estos han sido mitigados.

Revisión y mantenimiento

Una vez que el código se ha puesto en funcionamiento:

a) las actualizaciones se sugiere empaquetar e implementarse de forma segura;

b) se recomienda tratar las vulnerabilidades de seguridad de la información notificadas (ver el inciso 8.8);

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

c) se sugiere que los errores y presuntos ataques se registren y los registros es conveniente se revisen periódicamente para realizar ajustes en el código según sea necesario;

d) el código fuente se recomienda proteger contra el acceso no autorizado y la manipulación (por ejemplo, mediante el uso de herramientas de gestión de la configuración, que normalmente proporcionan características como el control de acceso y el control de versiones).

Si utiliza herramientas y bibliotecas externas, se sugiere que la organización considere:

a) garantizar que las bibliotecas externas se gestionen (por ejemplo, manteniendo un inventario de las bibliotecas utilizadas y sus versiones) y se actualicen periódicamente con ciclos de lanzamiento;

b) selección, autorización y reutilización de componentes bien examinados, en particular componentes de autenticación y criptográficos;

c) la licencia, la seguridad y el historial de los componentes externos;

d) garantizar que el software sea mantenible, rastreado y provenga de fuentes probadas y de buena reputación;

e) disponibilidad suficiente a largo plazo de recursos y artefactos de desarrollo.

Cuando sea necesario modificar un paquete de software, deberían tenerse en cuenta los siguientes puntos:

a) el riesgo de que los controles integrados y los procesos de integridad se vean comprometidos;

b) si se sugiere obtener el consentimiento del vendedor;

c) la posibilidad de obtener los cambios requeridos del proveedor como actualizaciones estándar del programa;

d) el impacto si la organización se hace responsable del mantenimiento futuro del software como resultado de cambios;

e) compatibilidad con otro software en uso.

Otros datos

Un principio rector es garantizar que el código relevante para la seguridad se invoque cuando sea necesario y sea resistente a la manipulación. Los programas instalados a partir de código binario compilado también tienen estas propiedades, pero solo para los datos almacenados dentro de la aplicación. Para los lenguajes interpretados, el concepto solo funciona cuando el código se ejecuta en un servidor que de otro modo es inaccesible para los usuarios y procesos que lo utilizan, y que sus datos se mantienen en una base de datos protegida de manera similar. Por ejemplo, el código interpretado se puede ejecutar en un servicio en la nube donde el acceso al código en sí requiere privilegios de administrador. Dicho acceso de administrador se recomienda este protegido por

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

mecanismos de seguridad como los principios de administración justo a tiempo y la autenticación reforzada. Si el propietario de la aplicación puede acceder a los scripts mediante acceso remoto directo al servidor, también lo puede hacer un atacante. Los servidores web se recomienda se configuren para evitar la exploración de directorios en tales casos.

El código de la aplicación se diseña mejor asumiendo que siempre está sujeto a ataques, a través de errores o acciones maliciosas. Además, las aplicaciones críticas se pueden diseñar para ser tolerantes a las fallas internas. Por ejemplo, la salida de un algoritmo complejo se puede verificar para garantizar que se encuentre dentro de los límites seguros antes de que los datos se utilicen en una aplicación, como una aplicación crítica financiera o de seguridad. El código que realiza las comprobaciones de límites es simple y, por lo tanto, mucho más fácil de probar la corrección.

Algunas aplicaciones web son susceptibles a una variedad de vulnerabilidades que se introducen por un diseño y una codificación deficientes, como la inyección de bases de datos y los ataques de secuencias de comandos entre sitios. En estos ataques, las solicitudes pueden ser manipuladas para abusar de la funcionalidad del servidor web.

Puede encontrarse más información sobre la evaluación de la seguridad de las TIC en la serie de normas que se indica en el inciso 10.4.

8.29 Pruebas de seguridad en desarrollo y aceptación

Tipo de control	Propiedades de Seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Identificar	#Seguridad_de_aplicaciones#Aseguramiento_de_seguridad_de_la_información#Seguridad_de_sistemas_y_redes	#Protección

Control

Es conveniente que los procesos de pruebas de seguridad se definan e implementen en el ciclo de vida del desarrollo.

Propósito

Validar si se cumplen los requisitos de seguridad de la información cuando se implementan aplicaciones o código en el entorno de producción.

Orientación

Los nuevos sistemas de información, actualizaciones y nuevas versiones se sugiere se prueben y verifiquen a fondo durante los procesos de desarrollo. Las pruebas de seguridad se sugiere sean una parte integral de las pruebas de sistemas o componentes.

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

Las pruebas de seguridad se recomienda se realicen en función de un conjunto de requisitos, que pueden expresarse como funcionales o no funcionales. Las pruebas de seguridad se sugiere incluyan pruebas de:

a) funciones de seguridad [por ejemplo, autenticación de usuarios (ver el inciso 8.5), restricción de acceso (ver el inciso 8.3) y uso de criptografía (ver el inciso 8.24)];

b) codificación segura (ver el inciso 8.28);

c) configuraciones seguras (ver el inciso 8.9, el inciso 8.20 y el inciso 8.22), incluida la de sistemas operativos, cortafuegos y otros componentes de seguridad.

Es conveniente que los planes de prueba se determinen utilizando un conjunto de criterios. El alcance de las pruebas es conveniente sea proporcional a la importancia, la naturaleza del sistema y el impacto potencial del cambio que se está introduciendo. El plan de prueba se sugiere incluya:

a) calendario detallado de actividades y pruebas;

b) insumos y productos previstos en una serie de condiciones;

c) criterios para evaluar los resultados;

d) decisión sobre nuevas acciones según sea necesario.

La organización puede aprovechar las herramientas automatizadas, como las herramientas de análisis de código o los escáneres de vulnerabilidades, y se sugiere verificar la corrección de los defectos relacionados con la seguridad.

Para los desarrollos internos, tales pruebas se sugiere sean realizadas inicialmente por el equipo de desarrollo. A continuación, es conveniente realizar pruebas de aceptación independientes para garantizar que el sistema funciona según lo esperado y solo como se esperaba (ver el inciso 5.8). Se recomienda considerar lo siguiente:

a) la realización de actividades de revisión del código como elemento pertinente para comprobar si se detectaran fallas de seguridad, incluidas las entradas y condiciones no previstas;

b) realizar análisis de vulnerabilidades para identificar configuraciones inseguras y vulnerabilidades del sistema;

c) realizar pruebas de penetración para identificar código y diseño inseguros.

Para los componentes de desarrollo y compras subcontratadas, se sugiere seguir un proceso de adquisición. Los contratos con el proveedor se recomienda aborden los requisitos de seguridad identificados (ver el inciso 5.20). Es conveniente que los productos y servicios se evalúen según estos criterios antes de la adquisición.

Se recomienda que las pruebas se realicen en un entorno de prueba que coincida lo más posible con el entorno de producción de destino para garantizar que el sistema no introduzca vulnerabilidades en el entorno de la organización y que las pruebas sean fiables (ver el inciso 8.31).

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

Otros datos

Se pueden establecer múltiples entornos de prueba, que se pueden utilizar para diferentes tipos de pruebas (por ejemplo, pruebas funcionales y de rendimiento). Estos diferentes entornos pueden ser virtuales, con configuraciones individuales para simular una variedad de entornos operativos.

Las pruebas y el monitoreo de entornos de prueba, herramientas y tecnologías también se sugiere considerar para garantizar pruebas efectivas. Las mismas consideraciones se aplican a la supervisión de los sistemas de supervisión desplegados en entornos de desarrollo, prueba y producción. Se necesita un juicio, guiado por la sensibilidad de los sistemas y los datos, para determinar cuántas capas de meta-pruebas son útiles.

8.30 Desarrollo externalizado

Tipo de control	Propiedades de Seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo#Detectivo	#Confidencialidad #Integridad #Disponibilidad	#Identificar #Proteger #Detectar	#Seguridad_de_sistemas_y_redes#Seguridad_de_aplicaciones#Seguridad_en_la_relación_con_proveedores	#Gobernabilidad_y_Ecosistema#Protección

Control

Se recomienda que la organización dirija, supervise y revise las actividades relacionadas con el desarrollo de sistemas subcontratados.

Propósito

Para garantizar que las medidas de seguridad de la información requeridas por la organización se implementen en el desarrollo de sistemas subcontratados.

Orientación

Cuando el desarrollo del sistema se subcontrata, se sugiere que la organización comunique, acuerde los requisitos, expectativas, monitoreé y revise continuamente si la entrega del trabajo subcontratado cumple con estas expectativas. Los siguientes puntos se sugiere se consideren en toda la cadena de suministro externa de la organización:

a) los acuerdos de licencia, la propiedad del código y los derechos de propiedad intelectual relacionados con el contenido externalizado (ver el inciso 5.32);

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

b) requisitos contractuales para prácticas seguras de diseño, codificación y ensayo (ver el inciso 8.25 al inciso 8.29);

c) la provisión del modelo de amenazas a considerar por los desarrolladores externos;

d) pruebas de aceptación de la calidad y exactitud de los productos (ver el inciso 8.29);

e) aportación de pruebas de que se establecen niveles mínimos aceptables de capacidades de seguridad y privacidad (por ejemplo, informes de garantía);

f) la aportación de pruebas de que se han aplicado pruebas suficientes para protegerse contra la presencia de contenidos maliciosos (tanto intencionados como no intencionados) en el momento de la entrega;

g) aportación de pruebas de que se han aplicado pruebas suficientes para evitar la presencia de vulnerabilidades conocidas;

h) acuerdos de custodia para el código fuente del software (por ejemplo, si el proveedor cierra el negocio);

i) derecho contractual a auditar los procesos y controles de desarrollo;

j) requisitos de seguridad para el entorno de desarrollo (ver el inciso 8.31);

k) teniendo en cuenta la legislación aplicable (por ejemplo, sobre protección de datos personales).

Otros datos

Puede encontrar más información sobre las relaciones con los proveedores en la serie de normas que se indica en el inciso 10.35.

8.31 Separación de entornos de desarrollo, prueba y producción

Tipo de control	Propiedades de Seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Seguridad_de_aplicaciones#Seguridad_de_sistemas_y_redes	#Protección

Control

Los entornos de desarrollo, pruebas y producción es conveniente estén separados y protegidos.

Propósito

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

Para proteger el entorno de producción y los datos del compromiso de las actividades de desarrollo y prueba.

Orientación

Se sugiere identificar e implementar el nivel de separación entre los entornos de producción, prueba y desarrollo que es necesario para prevenir problemas de producción.

Se recomienda considerar los siguientes elementos:

a) separar adecuadamente los sistemas de desarrollo y producción y operarlos en diferentes dominios (por ejemplo, en entornos virtuales o físicos separados);

b) definir, documentar y aplicar normas y autorización para el despliegue de programas informáticos desde el desarrollo hasta el estado de producción;

c) probar los cambios en los sistemas de producción y las aplicaciones en un entorno de ensayo o ensayo antes de aplicarlos a los sistemas de producción (ver el inciso 8.29);

d) no realizar pruebas en entornos de producción, excepto en circunstancias que hayan sido definidas y aprobadas;

e) compiladores, editores y otras herramientas de desarrollo o programas de utilidad que no sean accesibles desde los sistemas de producción cuando no sean necesarios;

f) la presentación de etiquetas de identificación del entorno adecuadas en los menús para reducir el riesgo de error;

g) no copiar información sensible en los entornos de sistemas de desarrollo y pruebas, a menos que se proporcionen controles equivalentes para los sistemas de desarrollo y ensayo.

En todos los casos, los entornos de desarrollo y prueba se sugiere se protejan teniendo en cuenta:

a) aplicación de parches y actualización de todas las herramientas de desarrollo, integración y prueba (incluidos constructores, integradores, compiladores, sistemas de configuración y bibliotecas);

b) configuración segura de sistemas y programas informáticos;

c) control del acceso a los entornos;

d) el seguimiento de los cambios en el entorno y el código almacenado en el mismo;

e) supervisión segura de los entornos;

f) realizar copias de seguridad de los entornos.

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

Es conveniente que una sola persona no tenga la capacidad de realizar cambios tanto en el desarrollo como en la producción sin una revisión y aprobación previas. Esto puede lograrse, por ejemplo, mediante la segregación de los derechos de acceso o mediante normas que se supervisan. En situaciones excepcionales, se recomienda implementar medidas adicionales como el registro detallado y el monitoreo en tiempo real para detectar y actuar sobre cambios no autorizados.

Otros datos

Sin las medidas y procedimientos adecuados, los desarrolladores y evaluadores que tienen acceso a los sistemas de producción pueden introducir riesgos significativos (por ejemplo, modificación no deseada de archivos o entorno del sistema, fallo del sistema, ejecución de código no autorizado y no probado en sistemas de producción, divulgación de datos confidenciales, integridad de datos y problemas de disponibilidad). Es necesario mantener un entorno conocido y estable en el que realizar pruebas significativas y evitar el acceso inadecuado de los desarrolladores al entorno de producción.

Las medidas y procedimientos incluyen funciones cuidadosamente diseñadas junto con la implementación de requisitos de segregación de funciones y la implementación de procesos de monitoreo adecuados.

El personal de desarrollo y pruebas también representa una amenaza para la confidencialidad de la información de producción. Las actividades de desarrollo y prueba pueden causar cambios no deseados en el software o la información si comparten el mismo entorno informático. Por lo tanto, es deseable separar los entornos de desarrollo, pruebas y producción para reducir el riesgo de cambios accidentales o acceso no autorizado al software de producción y a los datos empresariales (ver el inciso 8.33 para la protección de la información de prueba).

En algunos casos, la distinción entre entornos de desarrollo, prueba y producción puede ser deliberadamente borrosa y las pruebas pueden llevarse a cabo en un entorno de desarrollo o a través de implementaciones controladas a usuarios o servidores en vivo (por ejemplo, una pequeña población de usuarios piloto). En algunos casos, las pruebas de productos pueden ocurrir a través del uso en vivo del producto dentro de la organización. Además, para reducir el tiempo de inactividad de las implementaciones en vivo, se pueden admitir dos entornos de producción idénticos donde solo uno está activo a la vez.

Son necesarios procesos de apoyo para el uso de datos de producción en entornos de desarrollo y prueba (ver el inciso 8.33).

Las organizaciones también pueden tener en cuenta la orientación proporcionada en esta sección para entornos de capacitación al realizar la capacitación del usuario final.

8.32 Gestión del cambio

Tipo de control	Propiedades de Seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Seguridad_de_ aplicaciones#Se	#Protección

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

			guridad_de_sistemas_y_redes	

Control

Los cambios en las instalaciones de procesamiento de información y los sistemas de información se sugiere estén sujetos a procedimientos de gestión de cambios.

Propósito

Para preservar la seguridad de la información al ejecutar cambios.

Orientación

Se recomienda que la introducción de nuevos sistemas y cambios importantes en los sistemas existentes sigan las normas acordadas y un proceso formal de documentación, especificación, pruebas, control de calidad e implementación administrada. Se sugiere exista responsabilidades y procedimientos de gestión para garantizar un control satisfactorio de todos los cambios.

Los procedimientos de control de cambios se recomienda documentar y aplicar para garantizar la confidencialidad, integridad y disponibilidad de la información en las instalaciones de procesamiento de información y los sistemas de información, durante todo el ciclo de vida de desarrollo del sistema, desde las primeras etapas de diseño hasta todos los esfuerzos de mantenimiento posteriores.

Siempre que sea posible, se sugiere integrar los procedimientos de control de cambios para la infraestructura y los programas informáticos de las TIC.

Es conveniente que los procedimientos de control de cambios incluyan:

a) planificar y evaluar el impacto potencial de los cambios teniendo en cuenta todas las dependencias;

b) autorización de cambios;

c) comunicar los cambios a las partes interesadas pertinentes;

d) pruebas y aceptación de pruebas para los cambios (ver el inciso 8.29);

e) la aplicación de cambios, incluidos los planes de despliegue;

f) consideraciones de emergencia y contingencia, incluidos los procedimientos de reserva;

g) mantener registros de los cambios que incluyan todo lo anterior;

h) garantizar que la documentación operativa (ver el inciso 5.37) y los procedimientos de los usuarios se modifiquen según sea necesario para seguir siendo apropiados;

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

i) garantizar que los planes de continuidad de las TIC y los procedimientos de respuesta y recuperación (ver el inciso 5.30) se modifiquen según sea necesario para seguir siendo apropiados.

Otros datos

El control inadecuado de los cambios en las instalaciones de procesamiento de información y los sistemas de información es una causa común de fallas en el sistema o en la seguridad. Los cambios en el entorno de producción, especialmente cuando se transfiere software del entorno de desarrollo al entorno operativo, pueden afectar a la integridad y disponibilidad de las aplicaciones.

Cambiar el software puede afectar el entorno de producción y viceversa.

Las buenas prácticas incluyen la prueba de componentes de TIC en un entorno separado de los entornos de producción y desarrollo (ver el inciso 8.31). Esto proporciona un medio para tener control sobre el nuevo software y permitir una protección adicional de la información operativa que se utiliza con fines de prueba. Se recomienda incluir parches, Service Packs y otras actualizaciones.

El entorno de producción incluye sistemas operativos, bases de datos y plataformas de middleware. El control se sugiere aplicar para los cambios de aplicaciones e infraestructuras.

8.33 Información de la prueba

Tipo de control	Propiedades de Seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad	#Proteger	#Protección_de_la_información	#Protección

Control

Se recomienda que la información de la prueba se seleccione, proteja y gestione adecuadamente.

Propósito

Garantizar la pertinencia de las pruebas y la protección de la información operativa utilizada para las pruebas.

Orientación

La información de las pruebas se sugiere se seleccione para garantizar la fiabilidad de los resultados de los ensayos y la confidencialidad de la información operativa pertinente. La información confidencial (incluida la información de identificación personal) no es conveniente se copie en los entornos de desarrollo y prueba (ver el inciso 8.31).

Se sugiere aplicar las siguientes directrices para proteger las copias de la información operativa, cuando se utilizan con fines de prueba, ya sea que el entorno de prueba se cree internamente o en un servicio en la nube:

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

a) aplicar a los entornos de prueba los mismos procedimientos de control de acceso que los aplicados a los entornos operativos;

b) disponer de una autorización independiente cada vez que se copie la información operativa en un entorno de prueba;

c) registrar la copia y el uso de la información operativa para proporcionar una pista de auditoría;

d) proteger la información sensible mediante la eliminación o el enmascaramiento (ver el inciso 8.11) si se utiliza para las pruebas;

e) eliminar correctamente (ver el inciso 8.10) la información operativa de un entorno de prueba inmediatamente después de que se complete la prueba para evitar el uso no autorizado de la información de prueba.

La información de la prueba se sugiere se almacene de forma segura (para evitar la manipulación, que de otro modo puede dar lugar a resultados no válidos) y solo es conveniente utilizarse con fines de prueba.

Otros datos

Las pruebas de sistema y aceptación pueden requerir volúmenes sustanciales de información de prueba que estén lo más cerca posible de la información operativa.

8.34 Protección de los sistemas de información durante las pruebas de auditoría

Tipo de control	Propiedades de Seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Seguridad_de_sistemas_y_redes#Protección_de_la_información	#Gobernabilidad_y_Ecosistema #Protección

Control
Las pruebas de auditoría y otras actividades de garantía que impliquen la evaluación de los sistemas operativos se sugiere se planifiquen y acuerden entre el probador y la dirección adecuada.

Propósito

Minimizar el impacto de la auditoría y otras actividades de aseguramiento en los sistemas operativos y los procesos comerciales.

Orientación

Se sugiere observar las siguientes pautas:

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

a) acordar las solicitudes de auditoría para el acceso a los sistemas y datos con una gestión adecuada;

b) acordar y controlar el alcance de las pruebas técnicas de auditoría;

c) limitar las pruebas de auditoría al acceso de solo lectura al software y los datos. Si el acceso de solo lectura no está disponible para obtener la información necesaria, ejecutar la prueba por un administrador experimentado que tenga los derechos de acceso necesarios en nombre del auditor;

d) si se concede acceso, establecer y verificar los requisitos de seguridad (por ejemplo, antivirus y parches) de los dispositivos utilizados para acceder a los sistemas (por ejemplo, computadoras portátiles o tabletas) antes de permitir el acceso;

e) permitir únicamente el acceso que no sea de solo lectura para copias aisladas de los archivos del sistema, eliminarlos cuando finalice la auditoría u otorgarles la protección adecuada si existe la obligación de mantener dichos archivos bajo los requisitos de documentación de auditoría;

f) identificar y acordar solicitudes de tratamiento especial o adicional, como la ejecución de herramientas de auditoría;

g) ejecutar pruebas de auditoría que puedan afectar a la disponibilidad del sistema fuera del horario comercial;

h) supervisar y registrar todo el acceso con fines de auditoría y prueba.

Otros datos
Las pruebas de auditoría y otras actividades de aseguramiento también pueden ocurrir en sistemas de desarrollo y prueba, donde tales pruebas pueden afectar, por ejemplo, la integridad del código o conducir a la divulgación de cualquier información confidencial contenida en dichos entornos.

9 Concordancia con normas internacionales

Esta Norma es idéntica (IDT) con la Norma Internacional

ISO/IEC 27002:2022, Information security, cybersecurity and privacy protection – Information security controls third Edition (2022-02).

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

Apéndice A
(Informativo)

Uso de atributos

A.1 General

Este apéndice proporciona una tabla para demostrar el uso de atributos como una forma de crear diferentes vistas de los controles. Los cinco ejemplos de atributos son (ver el inciso 4.2):

a) Tipos de control (#Preventivo, #Detectivo, #Correctivo)

b) Propiedades de seguridad de la información (#Confidencialidad, #Integridad, #Disponibilidad)

c) Conceptos de ciberseguridad (#Identificar, #Proteger, #Detectar, #Responder, #Recuperación)

d) Capacidades operacionales (#Gobernabilidad, #Gestión_de_activos, #Protección_de_la_información, #Seguridad_de_los_recursos_humanos, #Seguridad_física, #Seguridad_de_sistemas_y_redes, #Seguridad_de_aplicaciones, #Configuración_segura, #Identidad_y_control_de_acceso, #Amenazas_y_gestión_de_vulnerabilidades, #Contiunidad, #Seguridad_en_la_relación_con_proveedores, #Cumplimiento_y_legal, #Gestión_de_eventos_de_seguridad_de_la_información, #Aseguramiento_de_seguridad_de_la_información)

e) Dominios de seguridad (#Gobernabilidad_y_Ecosistema, #Protección, #Defensa, #Resiliencia)

La Tabla A.1 contiene una matriz de todos los controles de este Proyecto de Norma Mexicana con sus valores de atributo dados.

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

El filtrado u ordenación de la matriz se puede lograr mediante el uso de una herramienta como una hoja de cálculo simple o una base de datos, que puede incluir más información como texto de control, orientación, orientación específica de la organización o atributos (ver el inciso A.2).

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

Tabla A.1 - Matriz de controles y valores de atributos

Identificador de control de la NMX-I-27002-NYCE-2022	Nombre del control	Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
5.1	Políticas de seguridad de la información	#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Identificar	#Gobernabilidad	#Gobernabilidad_y_Ecosistema #Resiliencia
5.2	Funciones y responsabilidades de seguridad de la información	#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Identificar	#Gobernabilidad	#Gobernabilidad_y_Ecosistema #Protección #Resiliencia
5.3	Separación de funciones	#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Gobernabilidad #Identidad_y_control_de_acceso	#Gobernabilidad_y_Ecosistema
5.4	Responsabilidades de gestión	#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Identificar	#Gobernabilidad	#Gobernabilidad_y_Ecosistema
5.5	Contacto con las autoridades	#Preventivo #Correctivo	#Confidencialidad #Integridad #Disponibilidad	#Identificar #Proteger #Responder #Recuperación	#Gobernabilidad	#Defensa #Resiliencia
5.6	Contacto con grupos de interés especial	#Preventivo #Correctivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger #Responder #Recuperación	#Gobernabilidad	#Defensa
5.7	Inteligencia de amenazas	#Preventivo #Detectivo #Correctivo	#Confidencialidad #Integridad #Disponibilidad	#Identificar #Detectar #Responder	#Amenazas_y_gestión_de_vulnerabilidades	#Defensa #Resiliencia

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

Identificador de control de la NMX-I-27002-NYCE-2022	Nombre del control	Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
5.8	Seguridad de la información en la gestión de proyectos	#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Identificar #Proteger	#Gobernabilidad	#Gobernabilidad_y_Ecosistema #Protección
5.9	Inventario de información y otros activos asociados	#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Identificar	#Gestión_de_activos	#Gobernabilidad_y_Ecosistema #Protección
5.10	Uso aceptable de la información y otros activos asociados	#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Gestión_de_activos #Protección_de_la_información	#Gobernabilidad_y_Ecosistema #Protección
5.11	Devolución de activos	#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Gestión_de_activos	#Protección
5.12	Clasificación de la información	#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Identificar	#Protección_de_la_información	#Protección #Defensa
5.13	Etiquetado de la información	#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Protección_de_la_información	#Defensa #Protección
5.14	Transferencia de información	#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Gestión_de_activos #Protección_de_la_información	#Protección

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

Identificador de control de la NMX-I-27002-NYCE-2022	Nombre del control	Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
5.15	Control de acceso	#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Identidad_y_control_de_acceso	#Protección
5.16	Gestión de identidades	#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Identidad_y_control_de_acceso	#Protección
5.17	Información de autenticación	#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Identidad_y_control_de_acceso	#Protección
5.18	Derechos de acceso	#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Identidad_y_control_de_acceso	#Protección
5.19	Seguridad de la información en las relaciones con los proveedores	#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Identificar	#Seguridad_en_la_relación_con_proveedores	#Gobernabilidad_y_Ecosistema #Protección
5.20	Abordar la seguridad de la información dentro de los acuerdos con proveedores	#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Identificar	#Seguridad_en_la_relación_con_proveedores	#Gobernabilidad_y_Ecosistema #Protección

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

Identificador de control de la NMX-I-27002-NYCE-2022	Nombre del control	Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
5.21	Gestión de la seguridad de la información en la cadena de suministro de las TIC	#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Identificar	#Seguridad_en_la_relación_con_proveedores	#Gobernabilidad_y_Ecosistema #Protección
5.22	Seguimiento, revisión y gestión del cambio de los servicios de los proveedores	#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Identificar	#Seguridad_en_la_relación_con_proveedores #Aseguramiento_de_seguridad_de_la_información	#Gobernabilidad_y_Ecosistema #Protección #Defensa
5.23	Seguridad de la información para el uso de servicios en la nube	#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Seguridad_en_la_relación_con_proveedores	#Gobernabilidad_y_Ecosistema #Protección
5.24	Planificación y preparación de la gestión de incidentes de seguridad de la información	#Correctivo	#Confidencialidad #Integridad #Disponibilidad	#Responder #Recuperación	#Gobernabilidad #Gestión_de_eventos_de_seguridad_de_la_información	#Defensa
5.25	Evaluación y decisión sobre eventos de seguridad de la información	#Detectivo	#Confidencialidad #Integridad #Disponibilidad	#Detectar #Responder	#Gestión_de_eventos_de_seguridad_de_la_información	#Defensa

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

Identificador de control de la NMX-I-27002-NYCE-2022	Nombre del control	Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
5.26	Respuesta a incidentes de seguridad de la información	#Correctivo	#Confidencialidad #Integridad #Disponibilidad	#Responder #Recuperación	#Gestión_de_eventos_de_seguridad_de_la_información	#Defensa
5.27	Aprender de los incidentes de seguridad de la información	#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Identificar #Proteger	#Gestión_de_eventos_de_seguridad_de_la_información	#Defensa
5.28	Recopilación de pruebas	#Correctivo	#Confidencialidad #Integridad #Disponibilidad	#Detectar #Responder	#Gestión_de_eventos_de_seguridad_de_la_información	#Defensa
5.29	Seguridad de la información durante la interrupción	#Preventivo #Correctivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger #Responder	#Contiunidad	#Protección #Resiliencia
5.30	Preparación de las TIC para la continuidad de las actividades	#Correctivo	#Disponibilidad	#Responder	#Contiunidad	#Resiliencia
5.31	Requisitos legales, legales, reglamentarios y contractuales	#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Identificar	#Cumplimiento_y_legal	#Gobernabilidad_y_Ecosistema #Protección
5.32	Derechos de propiedad intelectual	#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Identificar	#Cumplimiento_y_legal	#Gobernabilidad_y_Ecosistema

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

Identificador de control de la NMX-I-27002-NYCE-2022	Nombre del control	Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
5.33	Protección de registros	#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Identificar #Proteger	#Cumplimiento_y_legal #Gestión_de_activos #Protección_de_la_información	#Defensa
5.34	Privacidad y protección de la PII	#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Identificar #Proteger	#Protección_de_la_información #Cumplimiento_y_legal	#Protección
5.35	Revisión independiente de la seguridad de la información	#Preventivo #Correctivo	#Confidencialidad #Integridad #Disponibilidad	#Identificar #Proteger	#Aseguramiento_de_seguridad_de_la_información	#Gobernabilidad_y_Ecosistema
5.36	Cumplimiento de políticas, reglas y estándares de seguridad de la información	#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Identificar #Proteger	#Cumplimiento_y_legal #Aseguramiento_de_seguridad_de_la_información	#Gobernabilidad_y_Ecosistema

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

Identificador de control de la NMX-I-27002-NYCE-2022	Nombre del control	Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
5.37	Procedimientos operativos documentados	#Preventivo #Correctivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger #Recuperación	#Gestión_de_activos #Seguridad_física #Seguridad_de_sistemas_y_redes #Seguridad_de_aplicaciones #Configuración_segura #Identidad_y_control_de_acceso #Amenazas_y_gestión_de_vulnerabilidades #Contiunidad #Gestión_de_eventos_de_seguridad_de_la_información	#Gobernabilidad_y_Ecosistema #Protección #Defensa
6.1	Chequeo	#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Seguridad_de_los_recursos_humanos	#Gobernabilidad_y_Ecosistema
6.2	Términos y condiciones de empleo	#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Seguridad_de_los_recursos_humanos	#Gobernabilidad_y_Ecosistema

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

Identificador de control de la NMX-I-27002-NYCE-2022	Nombre del control	Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
6.3	Sensibilización, educación y formación en materia de seguridad de la información	#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Seguridad_de_los_recursos_humanos	#Gobernabilidad_y_Ecosistema
6.4	Proceso disciplinario	#Preventivo #Correctivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger #Responder	#Seguridad_de_los_recursos_humanos	#Gobernabilidad_y_Ecosistema
6.5	Responsabilidades después de la terminación o cambio de empleo	#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Seguridad_de_los_recursos_humanos #Gestión_de_activos	#Gobernabilidad_y_Ecosistema
6.6	Acuerdos de confidencialidad o no divulgación	#Preventivo	#Confidencialidad	#Proteger	#Seguridad_de_los_recursos_humanos #Protección_de_la_información #Supplier_relationships	#Gobernabilidad_y_Ecosistema

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

Identificador de control de la NMX-I-27002-NYCE-2022	Nombre del control	Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
6.7	Trabajo remoto	#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Gestión_de_activos #Protección_de_la_información #Seguridad_física #Seguridad_de_sistemas_y_redes	#Protección
6.8	Informes de eventos de seguridad de la información	#Detectivo	#Confidencialidad #Integridad #Disponibilidad	#Detectar	#Gestión_de_eventos_de_seguridad_de_la_información	#Defensa
7.1	Perímetros de seguridad física	#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Seguridad_física	#Protección
7.2	Entrada física	#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Seguridad_física #Identidad_y_control_de_acceso	#Protección
7.3	Asegurar oficinas, habitaciones e instalaciones	#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Seguridad_física #Gestión_de_activos	#Protección
7.4	Supervisión de la seguridad física	#Preventivo #Detectivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger #Detectar	#Seguridad_física	#Protección #Defensa

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

Identificador de control de la NMX-I-27002-NYCE-2022	Nombre del control	Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
7.5	Protección contra amenazas físicas y ambientales	#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Seguridad_física	#Protección
7.6	Trabajar en áreas seguras	#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Seguridad_física	#Protección
7.7	Escritorio limpio y pantalla limpia	#Preventivo	#Confidencialidad	#Proteger	#Seguridad_física	#Protección
7.8	Emplazamiento y protección de equipos	#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Seguridad_física #Gestión_de_activos	#Protección
7.9	Seguridad de los bienes fuera de las instalaciones	#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Seguridad_física #Gestión_de_activos	#Protección
7.10	Medios de almacenamiento	#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Seguridad_física #Gestión_de_activos	#Protección
7.11	Servicios públicos de apoyo	#Preventivo #Detectivo	#Integridad #Disponibilidad	#Proteger #Detectar	#Seguridad_física	#Protección
7.12	Seguridad del cableado	#Preventivo	#Confidencialidad #Disponibilidad	#Proteger	#Seguridad_física	#Protección

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

Identificador de control de la NMX-I-27002-NYCE-2022	Nombre del control	Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
7.13	Mantenimiento de equipos	#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Seguridad_física #Gestión_de_activos	#Protección #Resiliencia
7.14	Eliminación o reutilización segura del equipo	#Preventivo	#Confidencialidad	#Proteger	#Seguridad_física #Gestión_de_activos	#Protección
8.1	Dispositivos de punto final de usuario	#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Gestión_de_activos #Protección_de_la_información	#Protección
8.2	Derechos de acceso privilegiado	#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Identidad_y_control_de_acceso	#Protección
8.3	Restricción de acceso a la información	#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Identidad_y_control_de_acceso	#Protección
8.4	Acceso al código fuente	#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Identidad_y_control_de_acceso #Seguridad_de_aplicaciones #Configuración_segura	#Protección
8.5	Autenticación segura	#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Identidad_y_control_de_acceso	#Protección

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

Identificador de control de la NMX-I-27002-NYCE-2022	Nombre del control	Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
8.6	Gestión de la capacidad	#Preventivo #Detectivo	#Integridad #Disponibilidad	#Identificar #Proteger #Detectar	#Contiunidad	#Gobernabilidad_y_Ecosistema #Protección
8.7	Protección contra malware	#Preventivo #Detectivo #Correctivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger #Detectar	#Seguridad_de_sistemas_y_redes #Protección_de_la_información	#Protección #Defensa
8.8	Gestión de vulnerabilidades técnicas	#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Identificar #Proteger	#Amenazas_y_gestión_de_vulnerabilidades	#Gobernabilidad_y_Ecosistema #Protección #Defensa
8.9	Gestión de la configuración	#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Configuración_segura	#Protección
8.10	Eliminación de información	#Preventivo	#Confidencialidad	#Proteger	#Protección_de_la_información #Cumplimiento_y_legal	#Protección
8.11	Enmascaramiento de datos	#Preventivo	#Confidencialidad	#Proteger	#Protección_de_la_información	#Protección
8.12	Prevención de fugas de datos	#Preventivo #Detectivo	#Confidencialidad	#Proteger #Detectar	#Protección_de_la_información	#Protección #Defensa
8.13	Copia de seguridad de la información	#Correctivo	#Integridad #Disponibilidad	#Recuperación	#Contiunidad	#Protección

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

Identificador de control de la NMX-I-27002-NYCE-2022	Nombre del control	Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
8.14	Redundancia de las instalaciones de procesamiento de información	#Preventivo	#Disponibilidad	#Proteger	#Contiunidad #Gestión_de_activos	#Protección #Resiliencia
8.15	Bitácoras	#Detectivo	#Confidencialidad #Integridad #Disponibilidad	#Detectar	#Gestión_de_eventos_de_seguridad_de_la_información	#Protección #Defensa
8.16	Actividades de seguimiento	#Detectivo #Correctivo	#Confidencialidad #Integridad #Disponibilidad	#Detectar #Responder	#Gestión_de_eventos_de_seguridad_de_la_información	#Defensa
8.17	Sincronización de reloj	#Detectivo	#Integridad	#Proteger #Detectar	#Gestión_de_eventos_de_seguridad_de_la_información	#Protección #Defensa
8.18	Uso de programas de utilerías privilegiadas	#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Seguridad_de_sistemas_y_redes #Configuración_segura #Seguridad_de_aplicaciones	#Protección

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

Identificador de control de la NMX-I-27002-NYCE-2022	Nombre del control	Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
8.19	Instalación de software en sistemas operativos	#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Configuración_segura #Seguridad_de_aplicaciones	#Protección
8.20	Seguridad de redes	#Preventivo #Detectivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger #Detectar	#Seguridad_de_sistemas_y_redes	#Protección
8.21	Seguridad de los servicios de red	#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Seguridad_de_sistemas_y_redes	#Protección
8.22	Segregación de redes	#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Seguridad_de_sistemas_y_redes	#Protección
8.23	Filtrado web	#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Seguridad_de_sistemas_y_redes	#Protección
8.24	Uso de la criptografía	#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Configuración_segura	#Protección
8.25	Ciclo de vida de desarrollo seguro	#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Seguridad_de_aplicaciones #Seguridad_de_sistemas_y_redes	#Protección

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

Identificador de control de la NMX-I-27002-NYCE-2022	Nombre del control	Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
8.26	Requisitos de seguridad de las aplicaciones	#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Seguridad_de_aplicaciones #Seguridad_de_sistemas_y_redes	#Protección #Defensa
8.27	Arquitectura de sistemas seguros y principios de ingeniería	#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Seguridad_de_aplicaciones #Seguridad_de_sistemas_y_redes	#Protección
8.28	Codificación segura	#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Seguridad_de_aplicaciones #Seguridad_de_sistemas_y_redes	#Protección
8.29	Pruebas de seguridad en desarrollo y aceptación	#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Identificar	#Seguridad_de_aplicaciones #Aseguramiento_de_seguridad_de_la_información #Seguridad_de_sistemas_y_redes	#Protección

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

Identificador de control de la NMX-I-27002-NYCE-2022	Nombre del control	Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
8.30	Desarrollo externalizado	#Preventivo #Detectivo	#Confidencialidad #Integridad #Disponibilidad	#Identificar #Proteger #Detectar	#Seguridad_de_sistemas_y_redes #Seguridad_de_aplicaciones #Seguridad_en_la_relación_con_proveedores	#Gobernabilidad_y_Ecosistema #Protección
8.31	Separación de entornos de desarrollo, prueba y producción	#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Seguridad_de_aplicaciones #Seguridad_de_sistemas_y_redes	#Protección
8.32	Gestión del cambio	#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Seguridad_de_aplicaciones #Seguridad_de_sistemas_y_redes	#Protección
8.33	Información de la prueba	#Preventivo	#Confidencialidad #Integridad	#Proteger	#Protección_de_la_información	#Protección
8.34	Protección de los sistemas de información durante las pruebas de auditoría	#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger	#Seguridad_de_sistemas_y_redes #Protección_de_la_información	#Gobernabilidad_y_Ecosistema #Protección

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

La Tabla A.2 muestra un ejemplo de cómo crear una vista filtrando por un valor de atributo determinado, en este caso #Correctivo.

Tabla A.2 — Vista de los controles #Correctivo

Identificador de control de la NMX-I-27002-NYCE-2022	Nombre del control	Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
5.5	Contacto con las autoridades	#Preventivo #Correctivo	#Confidencialidad #Integridad #Disponibilidad	#Identificar #Proteger #Responder #Recuperación	#Gobernabilidad	#Defensa #Resiliencia
5.6	Contacto con grupos de interés especial	#Preventivo #Correctivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger #Responder #Recuperación	#Gobernabilidad	#Defensa
5.7	Inteligencia de amenazas	#Preventivo #Detectivo #Correctivo	#Confidencialidad #Integridad #Disponibilidad	#Identificar #Detectar #Responder	#Amenazas_y_gestión_de_vulnerabilidades	#Defensa #Resiliencia
5.24	Planificación y preparación de la gestión de incidentes de seguridad de la información	#Correctivo	#Confidencialidad #Integridad #Disponibilidad	#Responder #Recuperación	#Gobernabilidad #Gestión_de_eventos_de_seguridad_de_la_información	#Defensa
5.26	Respuesta a incidentes de seguridad de la información	#Correctivo	#Confidencialidad #Integridad #Disponibilidad	#Responder #Recuperación	#Gestión_de_eventos_de_seguridad_de_la_información	#Defensa

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

Identificador de control de la NMX-I-27002-NYCE-2022	Nombre del control	Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
5.28	Recopilación de pruebas	#Correctivo	#Confidencialidad #Integridad #Disponibilidad	#Detectar #Responder	#Gestión_de_eventos_de_seguridad_de_la_información	#Defensa
5.29	Seguridad de la información durante la interrupción	#Preventivo #Correctivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger #Responder	#Contiunidad	#Protección #Resiliencia
5.30	Preparación de las TIC para la continuidad de las actividades	#Correctivo	#Disponibilidad	#Responder	#Contiunidad	#Resiliencia
5.35	Revisión independiente de la seguridad de la información	#Preventivo #Correctivo	#Confidencialidad #Integridad #Disponibilidad	#Identificar #Proteger	#Aseguramiento_de_seguridad_de_la_información	#Gobernabilidad_y_Ecosistema

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

Identificador de control de la NMX-I-27002-NYCE-2022	Nombre del control	Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
5.37	Procedimientos operativos documentados	#Preventivo #Correctivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger #Recuperación	#Gestión_de_activos #Seguridad_física #Seguridad_de_sistemas_y_redes #Seguridad_de_aplicaciones #Configuración_segura #Identidad_y_control_de_acceso #Amenazas_y_gestión_de_vulnerabilidades #Contiunidad #Gestión_de_eventos_de_seguridad_de_la_información	#Gobernabilidad_y_Ecosistema #Protección #Defensa
6.4	Proceso disciplinario	#Preventivo #Correctivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger #Responder	#Seguridad_de_los_recursos_humanos	#Gobernabilidad_y_Ecosistema
8.7	Protección contra malware	#Preventivo #Detectivo #Correctivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger #Detectar	#Seguridad_de_sistemas_y_redes #Protección_de_la_información	#Protección #Defensa

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

Identificador de control de la NMX-I-27002-NYCE-2022	Nombre del control	Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
8.13	Copia de seguridad de la información	#Correctivo	#Integridad #Disponibilidad	#Recuperación	#Contiunidad	#Protección
8.16	Actividades de seguimiento	#Detectivo #Correctivo	#Confidencialidad #Integridad #Disponibilidad	#Detectar #Responder	#Gestión_de_eventos_de_seguridad_de_la_información	#Defensa

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

A.2 Punto de vista de la organización

Dado que los atributos se utilizan para crear diferentes vistas de controles, las organizaciones pueden descartar los ejemplos de atributos propuestos en este Proyecto de Norma Mexicana y crear sus propios atributos con diferentes valores para abordar necesidades específicas de la organización. Además, los valores asignados a cada atributo pueden diferir entre organizaciones, ya que las organizaciones pueden tener diferentes puntos de vista sobre el uso o la aplicabilidad del control o de los valores asociados al atributo (cuando los valores son específicos del contexto de la organización). El primer paso es entender por qué un atributo específico de la organización es deseable. Por ejemplo, si una organización ha construido sus planes de tratamiento de riesgos [ver la NMX-I-27001-NYCE-2015, subinciso 6.1.3 inciso e)] basados en eventos, puede desear asociar un atributo de escenario de riesgo a cada control en este Proyecto de Norma Mexicana.

El beneficio de tal atributo es acelerar el proceso de cumplimiento del requisito de la NMX-I-27001-NYCE-2015 relacionado con el tratamiento de riesgos, que consiste en comparar los controles determinados a través del proceso de tratamiento de riesgos (denominados controles "necesarios"), con los de la NMX-I-27001-NYCE-2015, Apéndice A (que se emiten a partir de este Proyecto de Norma Mexicana) para garantizar que no se haya pasado por alto ningún control necesario.

Una vez que se conocen el propósito y los beneficios, el siguiente paso es determinar los valores del atributo. Por ejemplo, se recomienda que la organización identifique 9 eventos:

1) pérdida o robo de dispositivo móvil;

2) pérdida o robo de las instalaciones de la organización;

3) fuerza mayor, vandalismo y terrorismo;

4) falla de software, hardware, energía, Internet y comunicaciones;

5) fraude;

6) piratería;

7) divulgación;

8) incumplimiento de la ley;

9) ingeniería social.

Por lo tanto, el segundo paso se puede lograr asignando identificadores a cada evento (por ejemplo, E1, E2, ..., E9).

El tercer paso consiste en copiar los identificadores de control y los nombres de control de este Proyecto de Norma Mexicana en una hoja de cálculo o base de datos y asociar los valores de atributo con cada control, recordando que cada control puede tener más de un valor de atributo.

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

El paso final es ordenar la hoja de cálculo o consultar la base de datos para extraer la información requerida.

Otros ejemplos de atributos organizacionales (y posibles valores) incluyen:

a) madurez (otros modelos de madurez);

b) estado de aplicación (para hacer, en curso, parcialmente implementado, plenamente implementado);

c) prioridad (1, 2, 3, etc.);

d) áreas organizativas involucradas (seguridad, TIC, recursos humanos, alta dirección, etc.);

e) eventos;

f) activos implicados;

g) construir y ejecutar, para diferenciar los controles utilizados en las diferentes etapas del ciclo de vida del servicio;

h) otros marcos con los que la organización trabaja o desde los que puede estar en transición.

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

Apéndice B
(Informativo)

Correspondencia de este Proyecto de Norma Mexicana NMX-I-27002-NYCE con la NMX-I-27002-NYCE-2015

El propósito de este apéndice es proporcionar compatibilidad con versiones anteriores de la NMX-I-27002-NYCE-2015 para las organizaciones que actualmente están utilizando esa norma y ahora desean hacer la transición a esta versión.

La Tabla B.1 proporciona la correspondencia de los controles especificados en los capítulos 5 al 8 con los de la NMX-I-27002-NYCE-2015.

Tabla B.1 - Correspondencia entre los controles del presente Proyecto de Norma Mexicana y los controles de la NMX-I-27002-NYCE-2015

Identificador de control de la NMX-I-27002-NYCE	Identificador de control de la NMX-I-27002-NYCE-2015	Nombre del control
5.1	05.1.1, 05.1.2	Políticas de seguridad de la información
5.2	06.1.1	Funciones y responsabilidades de seguridad de la información
5.3	06.1.2	Separación de funciones
5.4	07.2.1	Responsabilidades de gestión
5.5	06.1.3	Contacto con las autoridades
5.6	06.1.4	Contacto con grupos de interés especial
5.7	Nuevo	Inteligencia de amenazas
5.8	06.1.5, 14.1.1	Seguridad de la información en la gestión de proyectos
5.9	08.1.1, 08.1.2	Inventario de información y otros activos asociados
5.10	08.1.3, 08.2.3	Uso aceptable de la información y otros activos asociados

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

5.11	08.1.4	Devolución de activos
5.12	08.2.1	Clasificación de la información
5.13	08.2.2	Etiquetado de la información
5.14	13.2.1, 13.2.2, 13.2.3	Transferencia de información
5.15	09.1.1, 09.1.2	Control de acceso
5.16	09.2.1	Gestión de identidades
5.17	09.2.4, 09.3.1, 09.4.3	Información de autenticación
5.18	09.2.2, 09.2.5, 09.2.6	Derechos de acceso
5.19	15.1.1	Seguridad de la información en las relaciones con los proveedores
5.20	15.1.2	Abordar la seguridad de la información dentro de los acuerdos con proveedores
5.21	15.1.3	Gestión de la seguridad de la información en la cadena de suministro de las TIC
5.22	15.2.1, 15.2.2	Seguimiento, revisión y gestión del cambio de los servicios de los proveedores
5.23	Nuevo	Seguridad de la información para el uso de servicios en la nube
5.24	16.1.1	Planificación y preparación de la gestión de incidentes de seguridad de la información
5.25	16.1.4	Evaluación y decisión sobre eventos de seguridad de la información

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

5.26	16.1.5	Respuesta a incidentes de seguridad de la información
5.27	16.1.6	Aprender de los incidentes de seguridad de la información
5.28	16.1.7	Recopilación de pruebas
5.29	17.1.1, 17.1.2, 17.1.3	Seguridad de la información durante la interrupción
5.30	Nuevo	Preparación de las TIC para la continuidad de las actividades
5.31	18.1.1, 18.1.5	Requisitos legales, legales, reglamentarios y contractuales
5.32	18.1.2	Derechos de propiedad intelectual
5.33	18.1.3	Protección de registros
5.34	18.1.4	Privacidad y protección de la PII
5.35	18.2.1	Revisión independiente de la seguridad de la información
5.36	18.2.2, 18.2.3	Cumplimiento de políticas, reglas y estándares de seguridad de la información
5.37	12.1.1	Procedimientos operativos documentados
6.1	07.1.1	Chequeo
6.2	07.1.2	Términos y condiciones de empleo
6.3	07.2.2	Sensibilización, educación y formación en materia de seguridad de la información
6.4	07.2.3	Proceso disciplinario

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

6.5	07.3.1	Responsabilidades después de la terminación o cambio de empleo
6.6	13.2.4	Acuerdos de confidencialidad o no divulgación
6.7	06.2.2	Trabajo remoto
6.8	16.1.2, 16.1.3	Informes de eventos de seguridad de la información
7.1	11.1.1	Perímetros de seguridad física
7.2	11.1.2, 11.1.6	Entrada física
7.3	11.1.3	Asegurar oficinas, habitaciones e instalaciones
7.4	Nuevo	Supervisión de la seguridad física
7.5	11.1.4	Protección contra amenazas físicas y ambientales
7.6	11.1.5	Trabajar en áreas seguras
7.7	11.2.9	Escritorio limpio y pantalla limpia
7.8	11.2.1	Emplazamiento y protección de equipos
7.9	11.2.6	Seguridad de los bienes fuera de las instalaciones
7.10	08.3.1, 08.3.2, 08.3.3, 11.2.5	Medios de almacenamiento
7.11	11.2.2	Servicios públicos de apoyo
7.12	11.2.3	Seguridad del cableado
7.13	11.2.4	Mantenimiento de equipos
7.14	11.2.7	Eliminación o reutilización segura del equipo

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

8.1	06.2.1, 11.2.8	Dispositivos de punto final de usuario
8.2	09.2.3	Derechos de acceso privilegiado
8.3	09.4.1	Restricción de acceso a la información
8.4	09.4.5	Acceso al código fuente
8.5	09.4.2	Autenticación segura
8.6	12.1.3	Gestión de la capacidad
8.7	12.2.1	Protección contra malware
8.8	12.6.1, 18.2.3	Gestión de vulnerabilidades técnicas
8.9	Nuevo	Gestión de la configuración
8.10	Nuevo	Eliminación de información
8.11	Nuevo	Enmascaramiento de datos
8.12	Nuevo	Prevención de fugas de datos
8.13	12.3.1	Copia de seguridad de la información
8.14	17.2.1	Redundancia de las instalaciones de procesamiento de información
8.15	12.4.1, 12.4.2, 12.4.3	Registro
8.16	Nuevo	Actividades de seguimiento
8.17	12.4.4	Sincronización de reloj
8.18	09.4.4	Uso de programas de utilidad privilegiados
8.19	12.5.1, 12.6.2	Instalación de software en sistemas operativos
8.20	13.1.1	Seguridad de redes

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

8.21	13.1.2	Seguridad de los servicios de red
8.22	13.1.3	Segregación de redes
8.23	Nuevo	Filtrado web
8.24	10.1.1, 10.1.2	Uso de la criptografía
8.25	14.2.1	Ciclo de vida de desarrollo seguro
8.26	14.1.2, 14.1.3	Requisitos de seguridad de las aplicaciones
8.27	14.2.5	Arquitectura de sistemas seguros y principios de ingeniería
8.28	Nuevo	Codificación segura
8.29	14.2.8, 14.2.9	Pruebas de seguridad en desarrollo y aceptación
8.30	14.2.7	Desarrollo externalizado
8.31	12.1.4, 14.2.6	Separación de entornos de desarrollo, prueba y producción
8.32	12.1.2, 14.2.2, 14.2.3, 14.2.4	Gestión del cambio
8.33	14.3.1	Información de la prueba
8.34	12.7.1	Protección de los sistemas de información durante las pruebas de auditoría

La Tabla B.2 proporciona la correspondencia de los controles especificados en la NMX-I-27002-NYCE-2015 con los de este Proyecto de Norma Mexicana.

Tabla B.2 — Correspondencia entre los controles de la NMX-I-27002-NYCE-2015 y los controles del presente Proyecto de Norma Mexicana

Identificador de control de la NMX-I-27002-NYCE-2015	Identificador de control de la NMX-I-27002-NYCE-	Nombre de control según la NMX-I-27002-NYCE-2015

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

5		Políticas de seguridad de la información
5.1		Dirección de gestión para la seguridad de la información
5.1.1	5.1	Políticas de seguridad de la información
5.1.2	5.1	Revisión de las políticas de seguridad de la información
6		Organización de la seguridad de la información
6.1		Organización interna
6.1.1	5.2	Funciones y responsabilidades de seguridad de la información
6.1.2	5.3	Separación de funciones
6.1.3	5.5	Contacto con las autoridades
6.1.4	5.6	Contacto con grupos de interés especial
6.1.5	5.8	Seguridad de la información en la gestión de proyectos
6.2		Dispositivos móviles y teletrabajo
6.2.1	8.1	Directiva de dispositivos móviles
6.2.2	6.7	Teletrabajo
7		Seguridad de los recursos humanos
7.1		Antes del empleo
7.1.1	6.1	Chequeo
7.1.2	6.2	Términos y condiciones de empleo

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

7.2		Durante el empleo
7.2.1	5.4	Responsabilidades de gestión
7.2.2	6.3	Sensibilización, educación y formación en materia de seguridad de la información
7.2.3	6.4	Proceso disciplinario
7.3		Terminación y cambio de empleo
7.3.1	6.5	Terminación o cambio de responsabilidades laborales
8		Gestión de activos
8.1		Responsabilidad por los activos
8.1.1	5.9	Inventario de activos
8.1.2	5.9	Propiedad de los activos
8.1.3	5.10	Uso aceptable de los activos
8.1.4	5.11	Devolución de activos
8.2		Clasificación de la información
8.2.1	5.12	Clasificación de la información
8.2.2	5.13	Etiquetado de la información
8.2.3	5.10	Manejo de activos
8.3		Manejo de medios
8.3.1	7.10	Gestión de soportes extraíbles
8.3.2	7.10	Eliminación de medios
8.3.3	7.10	Transferencia de medios físicos

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

9		Control de acceso
9.1		Requisitos empresariales de control de acceso
9.1.1	5.15	Política de control de acceso
9.1.2	5.15	Acceso a redes y servicios de red
9.2		Gestión del acceso de usuarios
9.2.1	5.16	Registro y baja de usuarios
9.2.2	5.18	Aprovisionamiento de acceso de usuario
9.2.3	8.2	Gestión de derechos de acceso privilegiado
9.2.4	5.17	Gestión de la información de autenticación secreta de los usuarios
9.2.5	5.18	Revisión de los derechos de acceso de los usuarios
9.2.6	5.18	Eliminación o ajuste de los derechos de acceso
9.3		Responsabilidades del usuario
9.3.1	5.17	Uso de información secreta de autenticación
9.4		Control de acceso a sistemas y aplicaciones
9.4.1	8.3	Restricción de acceso a la información
9.4.2	8.5	Procedimientos de inicio de sesión seguros
9.4.3	5.17	Sistema de gestión de contraseñas

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

9.4.4	8.18	Uso de programas de utilidad privilegiados
9.4.5	8.4	Control de acceso al código fuente del programa
10		Criptografía
10.1		Controles criptográficos
10.1.1	8.24	Política sobre el uso de controles criptográficos
10.1.2	8.24	Gestión de claves
11		Seguridad física y ambiental
11.1		Áreas seguras
11.1.1	7.1	Perímetro de seguridad física
11.1.2	7.2	Controles físicos de entrada
11.1.3	7.3	Asegurar oficinas, habitaciones e instalaciones
11.1.4	7.5	Protección contra amenazas externas y ambientales
11.1.5	7.6	Trabajar en áreas seguras
11.1.6	7.2	Áreas de entrega y carga
11.2		Equipo
11.2.1	7.8	Emplazamiento y protección de equipos
11.2.2	7.11	Servicios públicos de apoyo
11.2.3	7.12	Seguridad del cableado
11.2.4	7.13	Mantenimiento de equipos
11.2.5	7.10	Eliminación de activos

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

11.2.6	7.9	Seguridad del equipo y los bienes fuera de las instalaciones
11.2.7	7.14	Eliminación o reutilización segura de los equipos
11.2.8	8.1	Equipo de usuario desatendido
11.2.9	7.7	Política de escritorio limpio y pantalla limpia
12		Seguridad de las operaciones
12.1		Procedimientos y responsabilidades operacionales
12.1.1	5.37	Procedimientos operativos documentados
12.1.2	8.32	Gestión del cambio
12.1.3	8.6	Gestión de la capacidad
12.1.4	8.31	Separación de entornos de desarrollo, pruebas y operativos
12.2		Protección contra malware
12.2.1	8.7	Controles contra malware
12.3		Copia de seguridad
12.3.1	8.13	Copia de seguridad de la información
12.4		Registro y monitoreo
12.4.1	8.15	Registro de eventos
12.4.2	8.15	Protección de la información de registro
12.4.3	8.15	Registros de administrador y operador
12.4.4	8.17	Sincronización de reloj

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

12.5		Control de software operativo
12.5.1	8.19	Instalación de software en sistemas operativos
12.6		Gestión técnica de vulnerabilidades
12.6.1	8.8	Gestión de vulnerabilidades técnicas
12.6.2	8.19	Restricciones en la instalación de software
12.7		Consideraciones sobre la auditoría de los sistemas de información
12.7.1	8.34	Controles de auditoría de sistemas de información
13		Seguridad de las comunicaciones
13.1		Instalaciones de gestión de seguridad de red.
13.1.1	8.20	Controles de red
13.1.2	8.21	Seguridad de los servicios de red
13.1.3	8.22	Segregación en redes
13.2		Transferencia de información
13.2.1	5.14	Políticas y procedimientos de transferencia de información
13.2.2	5.14	Acuerdos sobre transferencia de información
13.2.3	5.14	Mensajería electrónica
13.2.4	6.6	Acuerdos de confidencialidad o no divulgación

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

14		Adquisición, desarrollo y mantenimiento de sistemas
14.1		Requisitos de seguridad de los sistemas de información
14.1.1	5.8	Análisis y especificación de requisitos de seguridad de la información
14.1.2	8.26	Protección de los servicios de aplicaciones en redes públicas
14.1.3	8.26	Protección de las transacciones de servicios de aplicaciones
14.2		Seguridad en los procesos de desarrollo y soporte
14.2.1	8.25	Política de desarrollo seguro
14.2.2	8.32	Procedimientos de control de cambios en el sistema
14.2.3	8.32	Revisión técnica de las aplicaciones después de los cambios en la plataforma operativa
14.2.4	8.32	Restricciones en los cambios en los paquetes de software
14.2.5	8.27	Principios de ingeniería de sistemas seguros
14.2.6	8.31	Entorno de desarrollo seguro
14.2.7	8.30	Desarrollo externalizado
14.2.8	8.29	Pruebas de seguridad del sistema
14.2.9	8.29	Pruebas de aceptación del sistema
14.3		Datos de prueba

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

14.3.1	8.33	Protección de los datos de prueba
15		Relaciones con proveedores
15.1		Seguridad de la información en las relaciones con los proveedores
15.1.1	5.19	Política de seguridad de la información para las relaciones con los proveedores
15.1.2	5.20	Abordar la seguridad dentro de los acuerdos con proveedores
15.1.3	5.21	Cadena de suministro de tecnología de la información y la comunicación
15.2		Gestión de la prestación de servicios a proveedores
15.2.1	5.22	Seguimiento y revisión de los servicios de los proveedores
15.2.2	5.22	Gestión de cambios en los servicios de los proveedores
16		Gestión de incidentes de seguridad de la información
16.1		Gestión de incidentes y mejoras de seguridad de la información
16.1.1	5.24	Responsabilidades y procedimientos
16.1.2	6.8	Notificación de eventos de seguridad de la información
16.1.3	6.8	Notificación de debilidades de seguridad de la información

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

16.1.4	5.25	Evaluación y decisión sobre eventos de seguridad de la información
16.1.5	5.26	Respuesta a incidentes de seguridad de la información
16.1.6	5.27	Aprender de los incidentes de seguridad de la información
16.1.7	5.28	Recopilación de pruebas
17		Aspectos de seguridad de la información de la gestión de la continuidad del negocio
17.1		Continuidad de la seguridad de la información
17.1.1	5.29	Planificación de la continuidad de la seguridad de la información
17.1.2	5.29	Implementación de la continuidad de la seguridad de la información
17.1.3	5.29	Verificar, revisar y evaluar la continuidad de la seguridad de la información
17.2		Redundancias
17.2.1	8.14	Disponibilidad de instalaciones de procesamiento de información
18		Conformidad
18.1		Cumplimiento de los requisitos legales y contractuales
18.1.1	5.31	Identificación de la legislación aplicable y los requisitos contractuales

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

18.1.2	5.32	Derechos de propiedad intelectual
18.1.3	5.33	Protección de registros
18.1.4	5.34	Privacidad y protección de la información de identificación personal
18.1.5	5.31	Regulación de los controles criptográficos
18.2		Revisiones de seguridad de la información
18.2.1	5.35	Revisión independiente de la seguridad de la información
18.2.2	5.36	Cumplimiento de políticas y estándares de seguridad
18.2.3	5.36, 8.8	Revisión del cumplimiento técnico

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

10 Bibliografía

10.1 https://www.iso.org/obp

10.2 https://www.electropedia.org/

10.3 ISO/IEC 11770 (all parts), Information security — Key management

10.4 ISO/IEC 15408 (all parts), Information technology — Security techniques — Evaluation criteria for IT security

10.5 ISO 15489 (all parts), Information and documentation — Records management

10.6 ISO 15489-1:2016, Information and documentation — Records management – Part 1: Concepts and principles

10.7 ISO/IEC 17788:2014, Information technology — Cloud computing — Overview and vocabulary

10.8 ISO/IEC 17789:2014, Information technology — Cloud computing — Reference architecture

10.9 ISO/IEC 19086 (all parts), Cloud computing — Service level agreement (SLA) framework

10.10 ISO/IEC 19086-4:2019 Cloud computing — Service level agreement (SLA) framework — Part 4: Components of security and of protection of PII

10.11 ISO/IEC 19770 (all parts), Information technology — IT asset management

10.12 ISO/IEC 19770-1:2017 Information technology — IT asset management — Part 1: IT asset management systems — Requirements

10.13 ISO/IEC 19770-2:2015 Information technology — IT asset management — Part 2: Software identification tag

10.14 ISO/IEC 19941:2017, Information technology — Cloud computing — Interoperability and portability

10.15 ISO/IEC 20889:2018, Privacy enhancing data de-identification terminology and classification of techniques

10.16 ISO 21500, Project, programme and portfolio management — Context and concepts

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

10.17 ISO 21502, Project, programme and portfolio management — Guidance on project management

10.18 ISO/IEC 22123 (all parts), Information technology — Cloud computing

10.19 ISO 22313:2020, Security and resilience — Business continuity management systems — Guidance on the use of ISO 22301

10.20 ISO/TS 22317:2021, Societal security — Business continuity management systems — Guidelines for business impact analysis (BIA)

10.21 ISO 22396, Security and resilience — Community resilience — Guidelines for information exchange between organizations

10.22 ISO/IEC TS 23167:2020, Information technology — Cloud computing — Common technologies and techniques

10.23 ISO/IEC 23751:2022, Information technology — Cloud computing and distributed platforms — Data sharing agreement (DSA) framework

10.24 ISO/IEC 24760 (all parts), IT Security and Privacy — A framework for identity management

10.25 ISO/IEC 27007:2020, Information security, cybersecurity and privacy protection — Guidelines for information security management systems auditing

10.26 ISO/IEC TS 27008:2019, Information technology — Security techniques — Guidelines for the assessment of information security controls

10.27 ISO/IEC 27011, Information technology — Security techniques — Code of practice for Information security controls based on ISO/IEC 27002 for telecommunications organizations

10.28 ISO/IEC TR 27016, Information technology — Security techniques — Information security management — Organizational economics

10.29 ISO/IEC 27017:2015, Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services

10.30 ISO/IEC 27019, Information technology — Security techniques — Information security controls for the energy utility industry

10.31 ISO/IEC 27031:2011, Information technology — Security techniques — Guidelines for information and comunications technology readiness for business continuity

10.32 ISO/IEC 27033 (all parts), Information technology — Security techniques — Network security

10.33 ISO/IEC 27034 (all parts), Information technology — Application security

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

10.34 ISO/IEC 27035 (all parts), Information technology — Security techniques — Information security incident management

10.35 ISO/IEC 27036 (all parts), Information technology — Security techniques — Information security for supplier relationships

10.36 ISO/IEC 27036-2:2022 Cybersecurity — Supplier relationships — Part 2: Requirements

10.37 ISO/IEC 27036-3:2013 Information technology — Security techniques — Information security for supplier relationships — Part 3: Guidelines for information and communication technology supply chain security

10.38 ISO/IEC 27036-4:2016 Information technology — Security techniques — Information security for supplier relationships — Part 4: Guidelines for security of cloud services

10.39 ISO/IEC 27040:2015, Information technology — Security techniques — Storage security

10.40 ISO/IEC 27050 (all parts), Information technology — Electronic Discovery

10.41 ISO/IEC TS 27110, Information technology, cybersecurity and privacy protection — Cybersecurity framework development guidelines

10.42 ISO/IEC 27555:2021, Information security, cybersecurity and privacy protection — Guidelines on personally identifiable information deletion

10.43 ISO/IEC 29100:2011, Information technology — Security techniques — Privacy framework

10.44 ISO/IEC 29115:2013, Information technology — Security techniques — Entity authentication assurance framework

10.45 ISO/IEC 29134:2017, Information technology — Security techniques — Guidelines for privacy impact assessment

10.46 ISO/IEC 29146:2016, Information technology — Security techniques — A framework for access management

10.47 ISO/IEC 29147:2018, Information technology — Security techniques — Vulnerability disclosure

10.48 ISO 30000, Ships and marine technology — Ship recycling management systems — Specifications for management systems for safe and environmentally sound ship recycling facilities

10.49 ISO/IEC 30111:2019, Information technology — Security techniques — Vulnerability handling processes

10.50 IEC 31010, Risk management — Risk assessment techniques

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.

10.51 Information Security Forum (ISF). The ISF Standard of Good Practice for Information Security 2020, August 2018. Available at https:// www .securityforum .org/ tool/ standard -of -good -practice -for -information -security -2020/

10.52 ITIL® Foundation, ITIL 4 edition, AXELOS, February 2019, ISBN: 9780113316076

10.53 National Institute of Standards and Technology (NIST), SP 800-37, Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy, Revision 2. December 2018 [viewed 2020-07-31]. Available at https:// doi .org/ 10 .6028/ NIST .SP .800 -37r2

10.54 Open Web Application Security Project (OWASP). OWASP Top Ten - 2017, The Ten Most Critical Web Application Security Risks, 2017 [viewed 2020-07-31]. Available at https:// owasp .org/ www -project -top -ten/ OWASP _Top _Ten _2017/

10.55 Open Web Application Security Project (OWASP). OWASP Developer Guide, [online] [viewed 2020-10-22]. Available at https:// github .com/ OWASP/ DevGuide

10.56 National Institute of Standards and Technology (NIST), SP 800-63B, Digital Identity Guidelines; Authentication and Lifecycle Management. February 2020 [viewed 2020-07-31]. Available at https:// doi .org/ 10 .6028/ NIST.SP .800 -63b

10.57 OASIS, Structured Threat Information Expression. Available at https:// www.oasis -open .org/ standards #stix2 .0

10.58 OASIS, Trusted Automated Exchange of Indicator Information. Available at https:// www.oasis -open .org/ standards #taxii2 .0

© PROHIBIDA LA COPIA, REPRODUCCIÓN PARCIAL O TOTAL DE ESTE PROYECTO DE NORMA MEXICANA POR CUALQUIER MEDIO, SIN LA AUTORIZACIÓN DE NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C. COPIA CONTROLADA PARA USO DE SALVADOR SANTIAGO ARAUJO DE LA EMPRESA CONSULTORES E INVESTIGADORES EN ADMINISTRACION S.C.