PROYECTO DE NORMA MEXICANA

PROY-NMX-I-27001-NYCE-2022

Tecnologías de la información – Técnicas de seguridad – Sistemas de gestión de seguridad de la información – Requisitos

Information technology — Security techniques — Information security management systems — Requirements

Cancelará a la NMX-I-27001-NYCE-2015

SINEC-20221125204637306 **ICS:35.030; 03.100.70**

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 de NYCE, con la participación de las siguientes Instituciones y Empresas:**

   - C8 CONSULTING SERVICES, S.A. DE C.V.
   - CONSULTORES EN INGENIERÍA DE SISTEMAS COMPUTACIONALES Y CALIDAD
   - CREATIVIDAD Y EXPERIENCIA EN TI A.C.
   - INNOVACIONES TELEMATICAS SA DE CV
   - INSTITUTO POLITÉCNICO NACIONAL
   - NATIONAL ELECTRICAL MANUFACTURERS ASSOCIATION
   - NORMALIZACIÓN Y CERTIFICACIÓN NYCE, S.C.
   - ONSILIUM S.A. DE C.V.
   - SEGURIDATA PRIVADA, S.A. DE C.V.
   - SIAAC SOCIEDAD INTERNACIONAL DE ACREDITACIÓN, A.C.
   - TEMANOVA

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.**

   – 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.

- 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".

4. La declaratoria de vigencia de esta Norma Mexicana, se publicó en el Diario Oficial de la Federación el:

Índice del contenido

PROYECTO DE NORMA MEXICANA

PROY-NMX-I-27001-NYCE-2022

Tecnologías de la información – Técnicas de seguridad – Sistemas de gestión de seguridad de la información – Requisitos

(Cancelará a la NMX-I-27001-NYCE-2015)

Information technology — Security techniques — Information security management systems — Requirements

0 Introducción

0.1 General

Esta tercera edición cancela y sustituye a la segunda edición que se indica en el inciso 12.2, que ha sido ha sido enmendada para alinearla con la norma que se indica en el inciso12.5. También incorpora la corrección técnica de la norma que se indica en el inciso 12.6 y el inciso 12.7.

Los principales cambios son los siguientes:

- el texto se ha alineado con la estructura armonizada para las normas de sistemas de gestión.

Este Proyecto de Norma Mexicana se ha preparado para proporcionar los requisitos para establecer, implementar, mantener y mejorar continuamente un Sistema de Gestión de Seguridad de la Información. La adopción de un Sistema de Gestión de Seguridad de la Información es una decisión estratégica para una organización. El establecimiento e implementación de un Sistema de Gestión de Seguridad de la Información de una organización esta influenciado por las necesidades y objetivos de la organización, sus requisitos de seguridad, los procesos organizacionales utilizados y el tamaño y estructura de la organización. Todos estos factores de influencia se espera que cambien con el tiempo.

El Sistema de Gestión de Seguridad de la Información preserva la confidencialidad, integridad y disponibilidad de la información mediante la aplicación de un proceso de gestión de riesgos y da confianza a las partes interesadas de que los riesgos se gestionen adecuadamente.

Es importante que el Sistema de Gestión de Seguridad de la Información sea parte de y este integrado con los procesos de la organización y con la estructura de gestión general y que la seguridad de la información sea considerada en el diseño de procesos, sistemas de información y controles. Se espera que la implementación de un Sistema de Gestión de Seguridad de la Información sea escalado de acuerdo con las necesidades de la organización.

Este Proyecto de Norma Mexicana puede ser utilizado por partes internas y externas para evaluar la capacidad de la organización para cumplir con sus requisitos de seguridad de la información.

El orden en el cual son presentados los requisitos de este Proyecto de Norma Mexicana no refleja su importancia ni implica el orden en el cual deben ser implementados. Los elementos de la lista son enumerados para propósitos de referencia únicamente. La NMX-I-27000-NYCE-2019 describe la información general y el vocabulario de los Sistemas de Gestión de Seguridad de la Información, referenciando a la familia de normas de Sistemas de Gestión de Seguridad de la Información (incluyendo las normas que se indican en los incisos 12.6, 12.7 y la NMX-I-27005-NYCE-2019), con términos y definiciones relacionados.

0.2 Compatibilidad con otras normas de sistemas de gestión

Este Proyecto de Norma Mexicana aplica la estructura de alto nivel, títulos de sub-cláusulas idénticos, textos idénticos, términos comunes y definiciones principales, y por lo tanto mantiene la compatibilidad con otras normas de sistemas de gestión.

Este enfoque común es útil para aquellas organizaciones que optan por operar un sistema de gestión único que cumple con los requisitos de dos o más normas de sistemas de gestión.

1 Objetivo y campo de aplicación

Este Proyecto de Norma Mexicana especifica los requisitos para establecer, implementar, mantener y mejorar continuamente un Sistema de Gestión de Seguridad de la Información en el contexto de la organización. Este Proyecto de Norma Mexicana también incluye requisitos para la valoración y tratamiento de riesgos de seguridad de la información a la medida de las necesidades de la organización. Los requisitos establecidos en este Proyecto de Norma Mexicana son genéricos y se pretende que sean aplicables a todas las organizaciones, sin importar su tipo, tamaño o naturaleza. La exclusión de cualquiera de los requisitos especificados en los capítulos del 4 al 10 no es aceptable cuando una organización pretende la conformidad con este Proyecto de Norma Mexicana.

2 Referencias

Para la correcta aplicación de este Proyecto de Norma Mexicana, se requiere consultar las siguientes normas vigentes o las que la sustituyan.

NMX-I-27000-NYCE-2019	Tecnologías de la información – Técnicas de seguridad – Sistemas de gestión de la seguridad de la información – Fundamentos y vocabulario. (Cancela a la NMX-I-27000-NYCE-2014)
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-SAST-31000-IMNC-2018	Gestión del riesgo – Directrices. (Cancela a la NMX-SAST-31000-IMNC-2016)

3 Términos y definiciones

Para los propósitos de este Proyecto de Norma Mexicana se aplican las definiciones que se indican en la NMX-I-27000-NYCE-2019.

4 Contexto de la organización

4.1 Comprender la organización y su contexto

La organización debe determinar los aspectos externos e internos que son relevantes para su propósito y que afectan a su capacidad para lograr el resultado deseado(s) de su sistema de gestión de seguridad de la información.

Nota: La determinación de estos aspectos se refiere a establecer el contexto externo e interno de la organización considerada en el inciso 5.3 de la NMX-SAST-31000-IMNC-2018.

4.2 Entendimiento de las necesidades y expectativas de las partes interesadas

La organización debe determinar:

a) las partes interesadas que son relevantes al Sistema de Gestión de Seguridad de la Información y;

b) los requisitos relevantes de estas partes interesadas;

Nota: Los requisitos de las partes interesadas pueden incluir los requisitos legales y reglamentarios y las obligaciones contractuales.

c) cuáles de estos requisitos se abordan a través del sistema de gestión de seguridad de información.

4.3 Determinación del alcance del Sistema de Gestión de Seguridad de la Información

La organización debe determinar los límites y la aplicabilidad del Sistema de Gestión de Seguridad de la Información para establecer su alcance.

Al determinar el alcance, la organización debe considerar:

a) los aspectos externos e internos referidos en el inciso 4.1;

b) los requisitos referidos en el inciso 4.2 y;

c) las interfaces y las dependencias entre las actividades realizadas por la organización, y las que se realizan por otras organizaciones.

El alcance debe estar disponible como información documentada.

4.4 Sistema de Gestión de Seguridad de la Información

La organización debe establecer, implementar, mantener y mejorar continuamente un Sistema de Gestión de Seguridad de la Información, incluyendo los procesos necesarios y sus interacciones, de acuerdo con los requisitos de este Proyecto de Norma Mexicana.

5 Liderazgo

5.1 Compromiso y liderazgo

La alta dirección debe demostrar su liderazgo y compromiso con respecto al Sistema de Gestión de Seguridad de la Información a través de:

a) garantizar que la política de seguridad de la información y los objetivos de la seguridad de la información estén establecidos y sean compatibles con la dirección estratégica de la organización;

b) garantizar la integración de los requisitos del Sistema de Gestión de Seguridad de la Información en los procesos de la organización;

c) garantizar que los recursos necesarios para el Sistema de Gestión de Seguridad de la Información estén disponibles;

d) comunicar la importancia de la gestión eficaz de la seguridad de la información y de conformidad con los requisitos del Sistema de Gestión de Seguridad de la Información;

e) garantizar que el Sistema de Gestión de Seguridad de la Información obtenga los resultados previstos;

f) apoyar y dar dirección a las personas para contribuir a la eficacia del Sistema de Gestión de Seguridad de la Información;

g) promover la mejora continua y;

h) apoyar otros roles de gestión relevantes para demostrar su liderazgo y compromiso conforme aplique a sus áreas de responsabilidad.

Nota: La referencia a "negocio" en este Proyecto de Norma Mexicana puede interpretarse en sentido amplio para referirse a aquellas actividades que son fundamentales para los propósitos de la existencia de la organización.

5.2 Política

La alta dirección debe establecer una política de seguridad de la información que:

a) es apropiada al propósito de la organización;

b) incluya objetivos de seguridad de la información (ver inciso 6.2) o proporcione el marco de trabajo para establecer los objetivos de seguridad de la información;

c) incluya el compromiso para satisfacer los requisitos aplicables relacionados con la seguridad de la información y;

d) incluya el compromiso de mejora continua del Sistema de Gestión de Seguridad de la Información;

La política de seguridad de la información debe:

e) estar disponible como información documentada;

f) ser comunicadas dentro de la organización y;

g) estar disponible a las partes interesadas en forma apropiada.

5.3 Roles organizacionales, responsabilidades y autoridades

La alta dirección debe asegurarse que las responsabilidades y autoridades para los roles relevantes a la seguridad de la información se asignen y sean comunicados dentro de la organización.

La alta dirección debe asignar la responsabilidad y autoridad para:

a) garantizar que el Sistema de Gestión de Seguridad de la Información sea conforme a los requisitos de este Proyecto de Norma Mexicana e;

b) informar sobre el desempeño del Sistema de Gestión de Seguridad de la Información a la alta dirección.

Nota: La alta dirección también puede asignar responsabilidades y autoridad para informar sobre el desempeño del Sistema de Gestión de Seguridad de la Información dentro de la organización.

6 Planeación

6.1 Acciones para dirigir los riesgos y las oportunidades

6.1.1 Generalidades

Cuando se planee el Sistema de Gestión de Seguridad de la Información, la organización debe considerar los aspectos referidos en el inciso 4.1 y los requisitos referidos en el inciso 4.2 y determinar los riesgos y oportunidades que necesitan ser dirigidas para:

a) asegurar que el Sistema de Gestión de Seguridad de la información pueda lograr el resultado(s) previsto (s);

b) prevenir, o reducir, los efectos no deseados y;

c) lograr la mejora continua.

La organización debe planear:

d) acciones para dirigir estos riesgos y oportunidades y;

e) como;

1) integrar e implementar las acciones en sus procesos del Sistema de Gestión de Seguridad de la Información y;

2) evaluar la eficacia de estas acciones.

6.1.2 Valoración de riesgos de seguridad de la información

La organización debe definir y aplicar un proceso de valoración de riesgos de seguridad de la información para:

a) establecer y mantener los criterios de riesgos de seguridad de la información que incluya:

1) el criterio de aceptación del riesgo y;

2) los criterios para realizar las valoraciones de riesgos de seguridad de la información;

b) asegurar de que al repetir las valoraciones de riesgos de seguridad de la información produzcan resultados consistentes, válidos y comparables;

c) identificar los riesgos de seguridad de la información:

1) aplicar el proceso de valoración de riesgos de seguridad de la información para identificar riesgos asociados a la pérdida de confidencialidad, integridad y disponibilidad de la información dentro del alcance del Sistema de Gestión de Seguridad de la información; e

2) identificar a los propietarios de los riesgos;

d) analizar los riesgos de seguridad de la información:

1) valorar las consecuencias potenciales que se derivan si los riesgos identificados en el subinciso 1) del inciso c) llegan a materializarse;

2) valorar la probabilidad realista de la ocurrencia de los riesgos identificados en el subinciso 1) del inciso c) y;

3) determinar los niveles de riesgo;

e) evaluar los riesgos de seguridad de la información:

1) comparar los resultados del análisis de riesgo con los criterios de riesgo establecidos en el inciso a); y

2) priorizar los riesgos analizados para el tratamiento de riesgo.

La organización debe conservar información documentada sobre el proceso de valoración de riesgos de Seguridad de la Información.

6.1.3 Tratamiento de riesgos de seguridad de la información

La organización debe definir y aplicar un proceso de tratamiento de riesgos de seguridad de la información para:

a) seleccionar opciones apropiadas de tratamiento de riesgos de seguridad de la información, tomando en cuenta los resultados de la valoración de riesgos;

b) determinar todos los controles que sean necesarios para implementar la(s) opción(es) de tratamiento de riesgos de seguridad de la información elegida(s).

Nota: Las organizaciones pueden diseñar controles según sea necesario, o identificarlos de cualquier fuente.

c) comparar los controles determinados en el inciso 6.1.3 inciso b), con los descritos en el apéndice "A" y verificar que no se hayan omitido controles necesarios;

Notas:

1) El apéndice "A" contiene una lista de posibles controles de seguridad de la información. Los usuarios de este Proyecto de Norma Mexicana son referidos al apéndice "A" para garantizar que no se pasen por alto los controles de seguridad de la información necesarios.

2) Los controles de seguridad de la información listados en el apéndice "A" no son exhaustivos y es posible que sea necesaria información adicional sobre controles de seguridad.

d) producir una declaración de aplicabilidad que contenga;

- los controles necesarios (ver el subinciso 6.1.3 inciso b) e inciso c));
- justificación de las inclusiones,
- si están implementadas o no, y
- la justificación de la exclusión de controles del apéndice "A"

e) formular el plan de tratamiento de riesgos de seguridad de la información; y

f) obtener la aprobación del plan de tratamiento de riesgos de seguridad de la información y aceptación de los riesgos residuales de seguridad de la información por parte de los propietarios de los riesgos.

La organización debe conservar información documentada sobre el proceso de tratamiento de riesgos de seguridad de la información.

Nota: El proceso de valoración y tratamiento de riesgos de seguridad de la información en este Proyecto de Norma Mexicana se alinea con los principios y lineamientos genéricos previstos en la NMX-SAST-31000-IMNC-2018.

6.2 Alcanzando los objetivos y planes de seguridad de la información

La organización debe establecer los objetivos de seguridad de la información en funciones y niveles pertinentes.

Los objetivos de seguridad de la información deben:

a) ser consistentes con la política de seguridad de la información;

b) ser medibles (si es práctico);

c) tener en cuenta los requisitos de seguridad de la información aplicables y los resultados de la valoración del riesgo y del tratamiento del riesgo;

d) ser monitoreados;

e) ser comunicados;

f) estar actualizados según corresponda

g) estar disponibles como información documentada.

La organización debe conservar información documentada sobre los objetivos de seguridad de la información.

Cuando se planee cómo alcanzar sus objetivos de seguridad de la información, la organización debe determinar:

h) qué se va a hacer;

i) qué recursos son requeridos;

j) quién es el responsable;

k) cuando se va a terminar; y

l) como se evalúan los resultados.

6.3 Planificación de cambios

Cuando la organización determine como necesarios cambios en el sistema de gestión de seguridad de la información, estos cambios deben llevarse a cabo de manera planificada.

7 Soporte

7.1 Recursos

La organización debe determinar y proveer los recursos necesarios para el establecimiento, implementación, mantenimiento y mejora continua del Sistema de Gestión de Seguridad de la Información.

7.2 Competencia

La organización debe:

a) determinar la competencia necesaria del personal que hace el trabajo bajo su control que afecte el desempeño de la seguridad de la información;

b) asegurar que estas personas son competentes con base a una educación, capacitación o experiencia apropiada;

c) cuando sea necesario, tomar acciones para adquirir las competencias necesarias, y evaluar la eficacia de las acciones tomadas; y

d) conservar la información documentada apropiada como prueba de competencia.

Nota: Las acciones aplicables pueden incluir, por ejemplo, la provisión de capacitación, tutoría, o reasignación de los empleados actuales, o la contratación de personas competentes.

7.3 Concientización

Las personas que realizan trabajos bajo el control de la organización deben ser conscientes de:

a) la política de seguridad de la información;

b) su contribución a la eficacia del Sistema de Gestión de Seguridad de la Información, incluyendo los beneficios de un mejor desempeño de seguridad de la información; y

c) las implicaciones de no cumplir con los requisitos del Sistema de Gestión de Seguridad de la Información.

7.4 Comunicación

La organización debe determinar la necesidad de comunicaciones internas y externas relacionadas con el Sistema de Gestión de Seguridad de la Información, incluyendo:

a) sobre que comunicar;

b) cuando comunicar;

c) a quién comunicar;

d) cómo comunicar.

7.5 Información documentada

7.5.1 Generalidades

El Sistema de Gestión de Seguridad de la Información de la organización debe incluir:

a) información documentada, requerida por este Proyecto de Norma Mexicana; e

b) información documentada, determinada por la organización como sea necesario para la eficacia del Sistema de Gestión de Seguridad de la Información.

Nota: La extensión de la información documentada para un Sistema de Gestión de Seguridad de la Información puede diferir de una organización a otra debido a:

a) el tamaño de la organización y su tipo de actividades, procesos, productos y servicios;

b) la complejidad de los procesos y sus interacciones; y

c) la competencia de las personas.

7.5.2 Creación y actualización

Al crear y actualizar la información documentada de su apropiada:

a) identificación y descripción (por ejemplo, un título, fecha, autor, o el número de referencia);

b) formato (por ejemplo, el idioma, la versión del software, gráficos) y los medios (por ejemplo, papel, electrónico); y

c) revisión y aprobación de su idoneidad y adecuación.

7.5.3 Control de información documentada

La información documentada requerida por el Sistema de Gestión de Seguridad de la Información y por este Proyecto de Norma Mexicana debe ser controlada para asegurar:

a) que esté disponible y sea adecuada para su uso, donde y cuando sea necesario; y

b) que sea protegida de forma adecuada (por ejemplo, de la pérdida de confidencialidad, uso indebido, o la pérdida de la integridad).

Para el control de la información documentada, la organización debe realizar las siguientes actividades, según corresponda:

c) distribución, acceso, recuperación y uso;

d) almacenamiento y preservación, incluyendo la preservación de la legibilidad;

e) el control de cambios (por ejemplo , control de versiones); y

f) la retención y disposición.

La información documentada de origen externo, que la organización determine que es necesaria para la planeación y operación del Sistema de Gestión de Seguridad de la Información, debe identificarse y controlarse apropiadamente.

Nota: El acceso puede implicar una decisión sobre el permiso de sólo ver la información documentada, o el permiso y la autoridad para ver y cambiar la información documentada, etc.

8 Operación

8.1 Control y planeación operacional

La organización debe planificar, implementar y controlar los procesos necesarios para cumplir con los requisitos e implementar las acciones determinadas en el capítulo 6 a través de:

- establecer criterios para los procesos;

- implementar el control de los procesos de acuerdo con los criterios.

La información documentada debe estar disponible en la medida necesaria para tener confianza en que los procesos se han llevado a cabo según lo planeado.

La organización debe controlar los cambios planificados y revisar las consecuencias de los cambios no deseados, tomando medidas para mitigar cualquier efecto adverso, según sea necesario.

La organización debe garantizar que los procesos, productos o servicios proporcionados externamente que sean relevantes para el sistema de gestión de la seguridad de la información estén controlados.

8.2 Evaluación de riesgos de seguridad de la información

La organización debe llevar a cabo las evaluaciones de riesgos de seguridad de la información a intervalos planificados o cuando se proponen o se producen cambios significativos, teniendo en cuenta los criterios establecidos en el inciso 6.1.2 inciso a).

La organización conserva información documentada de los resultados de las evaluaciones de riesgos de seguridad de la información.

8.3 Tratamiento de riesgos de seguridad de la información

La organización debe implementar el plan de tratamiento de riesgos de seguridad de la información.

La organización debe conservar la información documentada de los resultados del tratamiento de riesgos de seguridad de la información.

9 Evaluación del desempeño

9.1 Monitoreo, medición, análisis y evaluación

La organización debe determinar:

a) que necesita ser monitoreado y medido, incluyendo los procesos y los controles de seguridad de la información;

b) los métodos de monitoreo, medición, análisis y evaluación son necesarios para garantizar los resultados válidos. Los métodos seleccionados deben producir resultados comparables y reproducibles para que se consideren válidos.

c) cuando debe llevarse a cabo el monitoreo y medición;

d) ¿quién debe monitorear y medir?;

e) cuando los resultados del monitoreo y medición deben ser analizados y evaluados; y

f) ¿quién debe analizar y evaluar los resultados?

La información documentada deberá estar disponible como evidencia de los resultados.

La organización debe evaluar el desempeño de la seguridad de la información y la eficacia del Sistema de Gestión de Seguridad de la Información.

9.2 Auditoría interna

9.2.1 General

La organización debe realizar auditorías internas a intervalos planificados para proporcionar información sobre si el Sistema de Gestión de Seguridad de la Información:

a) se ajusta a:

1) los requisitos propios de la organización para su Sistema de Gestión de Seguridad de la Información;

2) los requisitos de este Proyecto de Norma Mexicana;

b) se implementa y mantiene de manera efectivamente.

9.2.2 Programa de auditoría interna

La organización debe planificar, establecer, implementar y mantener uno o varios programas de auditoría, incluyendo la frecuencia, los métodos, las responsabilidades, los requisitos de planificación y la elaboración de informes.

Al establecer los programas de auditoría interna, la organización debe considerar la importancia de los procesos en cuestión y los resultados de auditorías anteriores.

La organización deberá:

a) definir los criterios de auditoría y el alcance de cada auditoría;

b) seleccionar auditores y realizar auditorías que garanticen la objetividad y la imparcialidad del proceso de auditoría;

c) asegurarse de que los resultados de las auditorías se informen a la dirección pertinente.

La información documentada deberá estar disponible como evidencia de la implementación del programa(s) de auditoría y los resultados de la auditoría.

9.3 Revisión por la dirección

9.3.1 General

La alta dirección debe revisar el Sistema de Gestión de Seguridad de la Información de la organización, a intervalos planeados para asegurar su continuad, vigencia, adecuación y eficacia.

9.3.2 Insumos para la revisión por la dirección

La revisión por la dirección debe incluir la consideración de:

a) el estatus de las acciones previas de las revisiones por la dirección;

b) los cambios en temas externos e internos que son relevantes para el Sistema de Gestión de Seguridad de la Información;

c) cambios en las necesidades y expectativas de las partes interesadas que son relevantes para el sistema de gestión de seguridad de la información

d) los resultados retroalimentación sobre el desempeño de la seguridad de la información, incluyendo las tendencias en:

1) no conformidades y acciones correctivas;

2) monitoreo y resultados de medición;

3) resultados de la auditoría; y

4) cumplimiento de los objetivos de seguridad de la información;

e) retroalimentación de las partes interesadas;

f) resultados de la valoración del riesgo y el estatus del plan de tratamiento de riesgo; y

g) las oportunidades para la mejora continua;

9.3.3 Resultados de la revisión por la dirección

Los resultados de la revisión por la dirección deben incluir decisiones relacionadas con las oportunidades de mejora continua y cualquier necesidad de cambios en el sistema de gestión de la seguridad de la información.

Los resultados de las revisiones por la dirección deben estar disponible como información documentada.

10 Mejora

10.1 Mejora continua

La organización debe mejorar continuamente la idoneidad, la adecuación y la eficacia del Sistema de Gestión de Seguridad de la Información.

10.2 No conformidad y acción correctiva

Cuando ocurre una no conformidad, la organización debe:

a) reaccionar a una no conformidad, y según sea el caso:

1) tomar acciones para controlarla y corregirla, y

2) hacer frente a las consecuencias;

b) evaluar la necesidad de acciones para eliminar las causas de la no conformidad, con el fin de que no se repita u ocurra en otro lugar, a través de:

1) revisión de la no conformidad;

2) determinar las causas de la no conformidad; y

3) determinar si existen no conformidades similares o que potencialmente puedan ocurrir;

c) implementar las acciones necesarias;

d) revisar la eficacia de las medidas correctivas tomadas; y

e) realizar cambios al Sistema de Gestión de Seguridad de la Información, si es necesario.

Las acciones correctivas deben ser apropiadas a los efectos de las no conformidades encontradas.

La organización debe conservar información documentada como evidencia de:

f) la naturaleza de las no conformidades y de cualquier acción tomada posteriormente; y

g) los resultados de cualquier acción correctiva.

11 Concordancia con normas internacionales

Esta Norma es idéntica (IDT) con la Norma Internacional:

ISO/IEC 27001:2022 "Information security, cybersecurity and privacy protection — Information security management systems — Requirements".

Apéndice A
(Normativo)

Referencia a controles de seguridad de la información

Los controles de seguridad de la información listados en la Tabla 1, se derivan directamente y están alineados con aquellos listados en la NMX-I-27002-NYCE, de los capítulos 5 al 8 y deben utilizarse en el contexto del inciso 6.1.3.

Tabla 1 - Controles de seguridad de la información

5 Controles organizacionales		
5.1	Políticas para la seguridad de la información	Control Se debe definir, aprobar por la dirección, publicar y comunicar a todos los empleados y partes externas relevantes las políticas de seguridad de la información y temas específicos, así como se deben revisar los cambios significativos en intervalos de tiempo planeados, en caso de que ocurran.
5.2	Roles y responsabilidades para la seguridad de la información	Control Todos los roles y responsabilidades de la seguridad de la información deben definirse y asignarse de acuerdo a las necesidades de la organización.
5.3	Segregación de tareas	Control Las tareas en conflicto y áreas de responsabilidad deben segregarse.
5.4	Responsabilidades de administración	Control La administración debe exigir que todo el personal aplique seguridad de la información de acuerdo a lo establecido en la política de seguridad de la información, políticas de temas específicos y procedimientos de la organización.
5.5	Contacto con autoridades	Control La organización debe establecer y mantener contactos con las autoridades relevantes.
5.6	Contacto con grupos de interés especial	Control La organización debe establecer y Mantener contactos con grupos de interés especial u otros foros de seguridad especializados y asociaciones profesionales.
5.7	Inteligencia de amenazas	Control La información relacionada con amenazas a la seguridad de la información debe ser colectada y analizada para producir inteligencia de amenazas.
5.8	Seguridad de la información en la administración de proyectos	Control La seguridad de la información debe incluirse en la administración de proyectos.
5.9	Inventario de información y otros activos asociados	Control Un inventario de la información y otros activos asociados, incluyendo los dueños, debe ser desarrollado y mantenido.

Tabla 1 – 2 de 9

5.10	Uso aceptable de la información y otros activos asociados	Control Se debe identificar, documentar e implementar reglas para el uso aceptable de la información y de los activos asociados.
5.11	Devolución de activos	Control El personal y otras partes interesadas deben devolver apropiadamente todos los activos de la organización que tengan en su posesión tras el cambio o terminación de su empleo, contrato o acuerdo.
5.12	Clasificación de información	Control La información debe ser clasificada de acuerdo a las necesidades de la organización, tomando como base la confidencialidad, integridad, disponibilidad y requisitos de las partes relevantes interesadas.
5.13	Etiquetado de información	Control Se debe desarrollar e implementar un apropiado conjunto de procedimientos para el etiquetado de la información de acuerdo con el esquema de clasificación de la información adoptado por la organización.
5.14	Transferencia de información	Control Las reglas, procedimientos o acuerdos para la transferencia de información deben existir para todo tipo de instalaciones de transferencia dentro de la organización y entre la organización y otras partes.
5.15	Control de acceso	Control Las reglas para el control físico y lógico del acceso a información y otros activos asociados deben ser establecidas e implementadas con base en el negocio y los requisitos de la seguridad de la información.
5.16	Gestión de la identidad	Control El completo ciclo de vida de las identidades debe ser administrado.
5.17	Información de autenticación	Control La asignación y gestión de información de autenticación debe ser controlada por un proceso de gestión, incluyendo asesoramiento personal de un manejo apropiado de la información de autenticación.
5.18	Derechos de acceso	Control Los derechos de acceso a información y otros activos asociados deben ser provisionados, revisados, modificados y eliminados de acuerdo con la política de temas específicos de la organización y reglas para el control de acceso.
5.19	Seguridad de la información para la relación con proveedores	Control Los procesos y procedimientos deben definirse e implementarse para gestionar los riesgos de seguridad de la información del tipo relación con proveedor.

Tabla 1 – 3 de 9

5.20	Abordar la seguridad dentro los acuerdos con proveedores	Control Todos los requisitos de seguridad de la información relevantes deben establecerse y acordarse con cada proveedor basado en el tipo de relación existente.
5.21	Gestión de la seguridad de la información en la cadena de suministro de las TIC	Control Se deben definir e implementar los procesos y procedimientos para gestionar los riesgos de seguridad de la información asociados con los productos TIC y cadenas de suministros de servicios.
5.22	Gestión de monitoreo, revisión y cambios a los servicios de proveedores	Control La organización debe monitorear, revisar, evaluar y auditar regularmente los cambios en las prácticas de seguridad de la información de la entrega de servicio de proveedores.
5.23	Seguridad de la información para uso de servicios de la nube	Control Los procesos de los servicios para adquisición, uso, auditoría y salida de la nube deben ser establecidos de acuerdo a los requerimientos de seguridad de la información de la organización.
5.24	Gestión, previsión y preparación contra incidentes de seguridad de la información	Control La organización debe prever y prepararse para gestionar incidentes de seguridad de la información definiendo, estableciendo y comunicando los procesos, roles y responsabilidades de la gestión incidentes de seguridad de la información
5.25	Evaluación y decisión sobre eventos de seguridad de la información	Control La organización debe evaluar los eventos de seguridad de la información y decidir si son clasificados como incidentes de seguridad de la información.
5.26	Respuesta a incidentes de seguridad de la información	Control Se debe responder a los incidentes de seguridad de la información de acuerdo con los procedimientos documentados.
5.27	Aprendizaje de incidentes de seguridad de la información	Control El conocimiento obtenido a partir de los incidentes de seguridad de la información debe utilizarse para reforzar y mejorar los controles de seguridad de la información.
5.28	Recopilación de evidencia	Control La organización debe definir y aplicar procedimientos para la identificación, recopilación, adquisición y preservación de la evidencia relacionada con eventos de seguridad de la información.
5.29	Seguridad de la información durante interrupciones	Control La organización debe planear cómo mantener la seguridad de la información a un nivel apropiado durante interrupciones.

Tabla 1 – 4 de 9

5.30	Disponibilidad de las Tecnologías de Información y Comunicación (TIC)	Control Las TIC deben planearse, implementarse, mantenerse y ponerse a prueba con base en los objetivos de continuidad del negocio y los requisitos de continuidad de las instalaciones de procesamiento de la información.
5.31	Requisitos legales, estatutarios, regulatorios y contractuales	Control Los requisitos legales, estatutarios, regulatorios y contractuales relevantes para la seguridad de la información y el enfoque de la organización para conocer estos requisitos deben ser identificados, documentados y mantenerse actualizados.
5.32	Derechos de propiedad intelectual	Control La organización debe implementar procedimientos apropiados para proteger los derechos de propiedad intelectual.
5.33	Protección de registros	Control Los registros deben estar protegidos contra pérdida, destrucción, falsificación, acceso no autorizado y divulgación no autorizada.
5.34	Privacidad y protección de información de identificación personal	Control La organización debe identificar y conocer los requisitos considerando la preservación de la privacidad y protección de información de identificación personal de acuerdo a las leyes y regulaciones y los requisitos contractuales
5.35	Revisión independiente de la seguridad de la información	Control El enfoque de la organización para la gestión de la seguridad de la información y su implementación, incluyendo personas, procesos y tecnologías deben ser revisados independientemente a intervalos planeados o cuando se ocurran cambios significativos.
5.36	Cumplimiento con políticas, reglas y estándares para la seguridad de la información	Control El cumplimiento de la política de seguridad de la información de la organización, políticas de temas específicos, reglas y estándares deben ser regularmente revisados.
5.37	Procedimientos operacionales documentados	Control Los procedimientos operacionales para las instalaciones del procesamiento de la información deben ser documentados y estar disponibles al personal que los necesite.
6	**Controles de personas**	
6.1	Investigación	Control Se deben llevar a cabo verificaciones de antecedentes a todos los candidatos al empleo de acuerdo con las leyes, regulaciones relevantes y la ética, y deben ser proporcionales a los requisitos del negocio, la clasificación de la información a la que se accede y los riesgos percibidos.

Tabla 1 – 5 de 9

6.2	Términos y condiciones del empleo	Control Los acuerdos contractuales con los empleados deben indicar sus responsabilidades y las de la organización para la seguridad de la información.
6.3	Concientización, educación y capacitación en seguridad de la información	Control Todos los empleados de la organización y las partes relevantes interesadas deben recibir concientización, educación y capacitación apropiada y actualizaciones regulares de políticas y procedimientos organizacionales, políticas de temas especiales y procedimientos, cuando sea relevante para sus funciones de trabajo.
6.4	Proceso disciplinario	Control Debe haber y comunicarse un proceso disciplinario formal para tomar acciones contra empleados y otros interesados relevantes que hayan cometido una violación a la política de seguridad de la información.
6.5	Responsabilidades en la terminación o cambio de empleo	Control Las responsabilidades de la seguridad de la información y obligaciones que permanecen válidos después de la terminación o el cambio de empleo deben estar definidos, comunicados a los empleados o contratistas y hacerse cumplir.
6.6	Acuerdos de confidencialidad o no divulgación	Control Se deben identificar, revisar regularmente, documentar y ser firmados por el personal y otras partes relevantes interesadas, los requisitos para los acuerdos de confidencialidad o no divulgación reflejando las necesidades de la organización para la protección de la información.
6.7	Trabajo remoto	Control Se deben implementar medidas de seguridad cuando el personal está trabajando de manera remota para proteger el acceso, proceso o almacenamiento de información fuera de las instalaciones de la organización.
6.8	Reporte de eventos de seguridad de la información	Control La organización debe proporcionar un mecanismo para que el personal reporte eventos de seguridad de la información observados o sospechosos a través de canales apropiados de forma oportuna.
7	**Controles físicos**	
7.1	Perímetros de seguridad física	Control Se deben definir y utilizar perímetros de seguridad para proteger las áreas que contienen información u otros activos asociados.
7.2	Entrada física	Control Se deben proteger las áreas seguras mediante controles de entrada apropiados y puntos de acceso.

Tabla 1 – 6 de 9

7.3	Aseguramiento de oficinas, salas e instalaciones	Control Se debe diseñar y aplicar seguridad física para oficinas, salas e instalaciones.
7.4	Monitoreo de seguridad física	Las instalaciones deben ser continuamente monitoreadas contra accesos físicos no autorizados.
7.5	Protección contra amenazas externas y ambientales	Control Se debe diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes.
7.6	Trabajo en áreas seguras	Control Se deben diseñar y aplicar medidas de seguridad para trabajar en áreas seguras.
7.7	Pantalla y escritorio limpio	Control Se debe definir y asegurar que se cumpla una política de escritorio limpio de papeles y medios de almacenamiento removibles y una política de pantalla limpia para las instalaciones de procesamiento de la información.
7.8	Ubicación y protección de equipo	Control El equipo debe estar situado con seguridad y protegido.
7.9	Seguridad de los equipos y activos fuera de las instalaciones	Control Los activos que se encuentran fuera de las instalaciones deben estar protegidos.
7.10	Medios de almacenamiento	Control Los medios de almacenamiento deben ser gestionados a través de su ciclo de vida durante la adquisición, uso, transporte y disposición de acuerdo con el esquema de clasificación de la organización y manejo requerido.
7.11	Servicios *públicos*	Control El equipo debe estar protegido contra fallas de energía y otras interrupciones causadas por fallas en los servicios públicos.
7.12	Seguridad del cableado	Control El cableado de energía y telecomunicaciones que transporten datos o soporten los servicios de la información deben protegerse de intercepción, interferencia o daño.
7.13	Mantenimiento del equipo	Control El equipo debe mantenerse correctamente para asegurar su continua disponibilidad, integridad y confidencialidad de la información.
7.14	Disposición o reutilización segura del equipo	Control Todos los elementos del equipo que contienen medios de almacenamiento deben ser verificados para garantizar que cualquier dato sensible y software licenciado ha sido eliminado o sobrescrito de manera segura previo a su disposición o reutilización.

Tabla 1 – 7 de 9

8	**Controles tecnológicos**

8.1	*Dispositivos de punto final de usuario*	Control La información almacenada, procesada o disponible en dispositivos hardware de usuarios debe ser protegida.
8.2	Derechos de acceso privilegiado	Control La asignación y uso de los derechos de acceso privilegiado deben restringirse y controlarse.
8.3	Restricción de acceso a la información	Control Se debe restringir el acceso a la información y activos asociados de acuerdo con lo establecido en la política del tema específico de control de acceso.
8.4	Acceso al código fuente del programa	Control El acceso al código fuente por vía escrita o de lectura, herramientas de desarrollo y bibliotecas de software deben ser apropiadamente gestionadas.
8.5	Autenticación segura	Control Las tecnologías y procedimientos de autenticación segura deben ser implementadas con base en las restricciones de acceso a la información y la política del tema específico de control de acceso.
8.6	Gestión de capacidad	Control El uso de recursos debe monitorearse, afinarse para realizar proyecciones de los requisitos futuros de la capacidad.
8.7	Protección contra malware	Control La protección contra malware debe ser implementada y apoyada por la consciencia apropiada del usuario.
8.8	Gestión de vulnerabilidades técnicas	Control Se debe obtener información acerca de las vulnerabilidades técnicas de los sistemas de información que están siendo utilizados de manera oportuna, evaluar la exposición de la organización a tales vulnerabilidades y tomar medidas apropiadas para tratar los riesgos asociados.
8.9	Gestión de la configuración	Control Las configuraciones, incluyendo configuraciones de seguridad, hardware, software, servicios y redes deben ser establecidas, documentadas, implementadas, monitoreadas y revisadas.
8.10	Eliminación de información	Control La información almacenada en los sistemas de información, dispositivos o en cualquier otro medio de almacenamiento debe ser eliminada cuando ya no sea necesaria.
8.11	Enmascaramiento de datos	Control El enmascaramiento de datos debe ser utilizado debe ser usado de acuerdo con la política del tema específico de control de acceso y otras políticas relacionadas y las necesidades del negocio, tomando en consideración la legislación aplicable.

Tabla 1 – 8 de 9

8.12	Prevención de fuga de datos	Control Las medidas de prevención de fuga de datos deben ser aplicadas a los sistemas, redes y cualquier otro dispositivo que procese, almacene o transmita información sensible.
8.13	Respaldos de la información	Control Copias de respaldos de la información, software e imágenes de sistemas deben realizarse y probarse regularmente de acuerdo con la política de respaldos acordada.
8.14	Redundancia de las instalaciones de procesamiento de información	Control Las instalaciones de procesamiento de información se deben implementar con suficiente redundancia para cumplir los requisitos de disponibilidad.
8.15	Inicios de sesión	Control Los inicios de sesión que registren actividades, excepciones faltas u otros eventos relevantes deben ser presentados, almacenados, protegidos y analizados.
8.16	Monitoreo de actividades	Control Las redes, sistemas y aplicaciones deben ser monitoreados de comportamientos maliciosos y se deben tomar las acciones necesarias para evaluar potenciales incidentes de seguridad.
8.17	Sincronización del reloj	Control Los relojes de todos los sistemas de procesamiento de la información dentro de la organización deben estar sincronizados con una sola fuente de tiempo de referencia aprobada.
8.18	Uso de privilegios de los programas de utilidades	Control El uso de programas de utilidades que puedan ser capaces de anular los controles del sistema y de las aplicaciones debe estar restringido y estrechamente controlado.
8.19	Instalación de software en sistemas operacionales	Control Se deben implementar procedimientos y medidas para controlar la instalación de software en sistemas operacionales.
8.20	Seguridad de las redes	Control Las redes deben gestionarse y controlarse para proteger la información en los sistemas y aplicaciones.
8.21	Seguridad en los servicios de red	Control Los mecanismos de seguridad, niveles de servicio y los requisitos de gestión para todos los servicios de la red deben identificarse, implementarse y monitorearse.
8.22	Segregación en redes	Control Los grupos de servicios de información, usuarios y sistemas de información deben estar segregados en las redes de la organización.

Tabla 1 – 9 de 9

8.23	Filtrado web	Control El acceso a sitios web externos debe ser controlado para reducir la exposición a contenido malicioso.
8.24	Uso de criptografía	Control Se deben definir e implementar reglas para el uso efectivo de la criptografía, incluyendo gestión de claves/llaves criptográficas.
8.25	Desarrollo seguro del ciclo de vida	Control Deben establecerse y aplicarse reglas para el desarrollo seguro de software y sistemas.
8.26	Aplicación de requisitos de seguridad	Control Los requisitos relacionados con la seguridad de la información deben ser identificados, especificados y aprobados durante el desarrollo o adquisición de aplicaciones.
8.27	Principios de arquitectura e ingeniería en sistemas seguros	Control Se deben establecer, documentar, mantener y aplicar principios de ingeniería para sistemas seguros a cualquier desarrollo de implementación de sistemas de información.
8.28	Codificación segura	Los principios de codificación segura deben ser aplicados al desarrollo de software.
8.29	Pruebas de seguridad para el desarrollo y aceptación	Control Se deben definir e implementar procesos de pruebas de seguridad durante el desarrollo del ciclo de vida.
8.30	Desarrollo de subcontratación (outsourcing)	Control La organización debe supervisar y monitorear directamente las actividades del desarrollo de la subcontratación (outsourcing).
8.31	Separación de entornos de desarrollo, prueba y producción	Control Se deben separar y mantener la seguridad de los entornos de desarrollo, prueba y producción.
8.32	Gestión del cambio	Control Los cambios a las instalaciones de procesamiento de información y sistemas de información deben estar sujetos a procedimientos de gestión de cambio.
8.33	Información de pruebas	Control La información de las pruebas debe ser apropiadamente seleccionada, protegida y gestionada.
8.34	Protección de sistemas de información durante auditoría	Control Las auditorías y otras actividades de aseguramiento que impliquen evaluación de sistemas operacionales deben ser planeadas y acordadas entre el auditor y el administrador correspondiente.

12 Bibliografía

12.1 ISO/IEC Directives, Part 1, Consolidated ISO Supplement – Procedures specific to ISO, 2012.

12.2 ISO/IEC 27001:2013 "Information Technology — Security Techniques — Information Security Management Systems — Requirements".

12.3 ISO/IEC 27001:2013/COR1:2014 "Information Technology — Security Techniques — Information Security Management Systems — Requirements".

12.4 ISO/IEC 27001:2013/COR 2:2015 "Information Technology — Security Techniques — Information Security Management Systems — Requirements".

12.5 ISO/IEC 27002:2022 "Information security, cybersecurity and privacy protection — Information security controls".

12.6 ISO / IEC 27003:2010 "Information technology -- Security techniques -- Information Security Management System Implementation Guidance".

12.7 ISO /IEC 27004:2009 "Information Technology -- Security Techniques -- Information Security Management – Measurement".