2024

INFORME DE AUDITORÍA

SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACION

CONSULTORES E INVESTIGADORES EN ADMINISTRACIÓN S.C. AEQUITAS ADMINISTRADORA DE ACTIVOS S.R.L. DE C.V.CIA INTEGRACIÓN EN ADMON S.R.L. DE C.V.

Normalización y Certificación NYCE S.C. / NYCE COLOMBIA S.A.S

INFORME DE AUDITORÍA

FORCSG-P12.29.9

DATOS DE LA ORGANIZACIÓN

Solicitud:	202208SGSI256
Razón Social:	**CONSULTORES E INVESTIGADORES EN ADMINISTRACIÓN S.C. AEQUITAS ADMINISTRADORA DE ACTIVOS S.R.L. DE C.V.CIA INTEGRACIÓN EN ADMON S.R.L. DE C.V.**
Domicilio(s) auditado(s):	Sede: Lago Xochimilco No. 283, Ampliación General Vicente Villada, Nezahualcóyotl, C.P. 57760, Edo. De México. Sitio: Insurgentes Sur 686, despacho 902, colonia del valle, delegación Benito Juárez, ciudad de México, código postal 03100. Sitio : Hermenegildo Galeana No. 204, despacho 2, Col. Centro, C.P. 50000, Toluca, Edo. México

DATOS DE LA EVALUACIÓN

Criterios de auditoría:

SGSI

- ISO/IEC 27001:2022
- Documentación propia del Sistema de Gestión
- Especificaciones técnicas o regulaciones aplicables

Tipo de auditoría:	RENOVACIÓN + RESTAURACIÓN + TRANSICIÓN.	**Fechas de auditoría:**	23, 24 y 25 de septiembre del 2024
Código(s) IAF: Sector(es) Económico(s):	IAF: 35		
Alcance(s) de la certificación:	Los servicios de investigación de crédito (referencias comerciales, verificación de propiedad y sociedades en el RPPYC), recuperación de cartera (extrajudicial y judicial), cobranza punta-punta y gestión domiciliaria, soportado por los procesos de sistemas, compras, recursos humanos, contabilidad y tesorería. De acuerdo con la declaración de aplicabilidad (SoA) LIS GSI 007, versión 10, de Septiembre 2024."		
Alcance de la auditoría:	Sede: Lago Xochimilco No. 283, Ampliación General Vicente Villada, Nezahualcóyotl, C.P. 57760, Edo. De México. Sitio : Insurgentes Sur 686, despacho 902, colonia del valle, delegación Benito Juárez, ciudad de México, código postal 03100. Sitio : Hermenegildo Galeana No. 204, despacho 2, Col. Centro, C.P. 50000, Toluca, Edo. México		
Objetivos de la auditoría:	Verificar la conformidad del Sistema de Gestión de la organización con los requisitos y regulaciones aplicables. Evaluar la capacidad y eficacia de la organización para cumplir con los objetivos del SG. Revisar los hallazgos de la auditoría previas.		
Clasificación de hallazgos	**Conforme:** Cumplimiento de un requisito. **Tema de preocupación:** Hallazgo aplicable para auditorías de certificación de etapa 1, que indica la posible ausencia del cumplimiento parcial o total de algún requisito, que la organización auditada debería atender previo a la auditoría de certificación de etapa 2. **Observación:** Inconsistencia en el cumplimiento de un requisito que basado en la experiencia y juicio del auditor no es probable que resulte en una falla del sistema de gestión, incidente aislado o hallazgo encontrado de forma esporádica con un riesgo mínimo de incumplimiento con la norma o estándar de referencia o de impacto a los objetivos del sistema de gestión. Una observación no tiene la categoría de no conformidad; sin embargo, es un hallazgo, el cual debe ser informado al usuario para su revisión con el fin de evitar posibles no conformidades en futuras ocasiones. **No Conforme:** Incumplimiento de un requisito conforme de las normas de referencia, los procedimientos propios de la organización o la regulación aplicable. **No conformidad menor:** No conformidad que no afecta la capacidad del sistema de gestión para lograr los resultados previstos. **No conformidad mayor:** No conformidad que afecta a la capacidad del sistema de gestión para lograr los resultados previstos, en las siguientes circunstancias: - si existe una duda significativa de que se haya implementado un control eficaz de proceso o de que los productos o servicios cumplan los requisitos especificados de la disciplina de referencia- una cantidad de no conformidades menores asociadas al mismo requisito o cuestión podría demostrar una desviación sistemática y por tanto, constituye una no conformidad mayor.		

DATOS DEL PERSONAL ENTREVISTADO

Nombre	Cargo
Salvador Santiago Araujo	Gerente Administrativa
Ana Laura Hernández Montaño	Coordinador de Sistemas
Irais Dafne Mendoza Sánchez	Director General Adjunta
Javier Mendoza Lara	Director General
Socorro Sanchez Mora	Gerente de Operaciones de Investigación de Crédito
Rafael Fernando Mendoza Loza	Coordinador de Sistemas
Berenice Torres Velasco	Gerente de RH
Jesús Eduardo Martínez Padilla	Asistente de Direccion
Claudia Elena Mendoza Lara	Encargada de Contabilidad
Juan Carlos Castelán Santiago	Supervisor del Registro Publico
Luis Gerardo Torres Flores	Supervisor de Banco
Jesús Abraham Ventura Castañeda	Auxiliar de Sistemas

DATOS DEL EQUIPO AUDITOR

Nombre	Rol
Karina ALONSO SANCHEZ	Auditor líder
David Abraham Nieto López	Auditor
N/A	Auditor en entrenamiento

DATOS DE PERSONAL ADICIONAL

Nombre	Rol
N/A	Observador
N/A	Guía
N/A	Testificador
N/A	Traductor e intérprete

INFORME DE HALLAZGOS

Aplicable al Sistema Gestión

No.	Proceso | Servicio | Departamento	Numeral y Requisito de Referencia	Descripción	Clasificación de Hallazgo
1	Contexto de la Organización	4.1 Comprender La Organización Y Su Contexto	Es necesario que la Organización integre en la información del análisis del FODA las consideraciones del cambio climático.	Observación
2	SOPORTE	7.3 Concientización	Durante las entrevista al Personal del Sitio : Insurgentes se detecta la necesidad de Reforzar la Concientización de los Colaboradores en la Sede de Valle-Insurgentes	Observación

Notas

1. La atención de los Temas de Preocupación y las observaciones se revisarán en la siguiente evaluación.
2. La organización cuenta con 45 días naturales posteriores a la entrega de este informe para entregar su plan de acción a cada no conformidad que incluya el análisis de causa y evidencia de cumplimiento de conformidad con su procedimiento de acciones correctivas.

RESUMEN DE LA EVALUACIÓN

Durante la ejecución de la auditoria se revisaron los requisitos del Esquema Aplicable:
A continuación, se muestran los resultados de la evaluación, la nomenclatura utilizada es:

C: Conforme | TP: Tema de Preocupación | OB: Observación | NC: No Conforme

Proceso / Servicio:	Área	Referencias normativas asociadas	Resultado
CONTEXTO DE LA ORGANIZACIÓN	Desarrollo	**4.1 Comprender la organización y su contexto,** 4.2 Entendimiento de las necesidades y expectativas de las partes interesadas, 4.3 Determinación del alcance del sistema de gestión de seguridad de la información, 4.4 Sistema de gestión de la seguridad de información	OB
LIDERAZGO | CONTROLES ORGANIZATIVOS	Desarrollo	5.1 Liderazgo y compromiso, 5.2 Política, 5.3 Roles, responsabilidades y autoridades de la organización, A.5.1 Política de seguridad de la información, 9.3 Revisión por la dirección, 6.2 Alcanzando los objetivos y planes de seguridad de la información, 6.3 Planificación de cambios	C
GESTIÓN DE RIESGOS	Desarrollo	6.1.1 Generalidades, 6.1.2 Valoración de riesgos de seguridad de la información, 6.1.3 Tratamiento de riesgos de seguridad de la información, 8.1 Control y planeación operacional, 8.2 Evaluación de riesgos de seguridad de la información, 8.3 Tratamiento de riesgos de seguridad de la información.	C
SOPORTE	Desarrollo	7.1 Recursos, 7.2 Competencia, **7.3 Concientización**, 7.4 Comunicación	OB
CONTROLES ORGANIZATIVOS | CONTROLES DE PERSONAS	Recursos Humanos	A.6.1 Chequeo, A.6.2 Términos y Condiciones de empleo, A.5.4 Responsabilidades de Gestión, A.6.3 Sensibilización, educación y formación en materia de seguridad de la información, A.6.4 Proceso disciplinario, A.6.5 Responsabilidades después de la terminación o cambio de empleo	C
INFORMACIÓN DOCUMENTADA	SGSI	7.5.1 Generalidades, 7.5.2. Creación y actualización, 7.5.3 Control de la información documentada	C
EVALUACIÓN DEL DESEMPEÑO Y MEJORA	SGSI	9.1 Seguimiento, medición, análisis y evaluación, 9.2 Auditoría interna, 10.2 No conformidad y acción correctiva, 10.1 Mejora continua	C
CONTROLES ORGANIZATIVOS | CONTROLES DE PERSONAS | CONTROLES TECNOLÓGICOS	Desarrollo	A.5.2 Roles y responsabilidades de seguridad de la información, A.5.3 Segregación de funciones, A.5.5 Contacto con las autoridades, A.5.6 Contacto con grupos de interés especial, A.5.8 Seguridad de la información en la gestión de proyectos, A.8.1 Dispositivos de punto final de usuario, A.6.7 Trabajo Remoto	C

CONTROLES ORGANIZATIVOS | CONTROLES FÍSICO | CONTROLES TECNOLÓGICOS	Desarrollo	A.5.9 Inventario de información y otros activos asociados, A.5.10 Uso aceptable de la información y otros activos asociados, A.5.11 Devolución de activos, A.5.12 Clasificación de la información, A.5.13 Etiquetado de la información, A.7.10 Medios de almacenamiento, A.8.10 Eliminación de información	C
CONTROLES ORGANIZATIVOS | CONTROLES TECNOLÓGICOS	Desarrollo	A.5.15 Control de acceso, A.8.12 Prevención de fugas de datos, A.5.16 Gestión de identidades, A.8.2 Derechos de acceso privilegiado, A.5.17 Información de autentificación, A.5.18 Derechos de acceso, A.8.3 Restricción de acceso a la información, A.8.5 Autentificación segura, A.8.18 Uso de programas de utilidad privilegiados, A.8.4 Acceso al código fuente	C
CONTROLES ORGANIZATIVOS | CONTROLES DE PERSONAS | CONTROLES TECNOLÓGICOS	Desarrollo	A.8.20 Seguridad de redes, A.8.21 Seguridad en los servicios de red, A.8.22 Segregación de redes, A.5.14 Transferencia de información, A.6.6 Acuerdos de confidencialidad o no divulgación	C
CONTROLES TECNOLÓGICOS	Desarrollo	A.8.24 Uso de la criptografía	C
CONTROLES FÍSICO	Desarrollo	A.7.1 Perímetros de seguridad física, A.7.2 Entrada Física, A.7.3 Aseguramiento de oficinas, habitaciones e instalaciones., A.7.4 Supervisión de la seguridad física, A.7.5 Protección contra amenazas físicas y ambientales, A.7.6 Trabajar en áreas seguras, A.7.8 Emplazamiento y protección de equipos, A.7.11 Servicios públicos de apoyo, A.7.12 Seguridad del cableado, A.7.13 Mantenimiento de equipos, A.7.9 Seguridad de los bienes fuera de las instalaciones, A.7.14 Eliminación o reutilización segura del equipo, A.7.7 Escritorio limpio y Pantalla limpia	C
CONTROLES ORGANIZATIVOS | CONTROLES TECNOLÓGICOS	Desarrollo	A.5.37 Procedimientos operativos documentados, A.8.32 Gestión del cambio, A.8.9 Gestión de la Configuración, A.8.6 Gestión de la capacidad, A.8.31 Separación de entornos de desarrollo, prueba y producción, A.8.7 Protección contra malware, A.8.13 Copia de seguridad de la información, A.8.15 Registro, A.8.17 Sincronización de reloj, A.8.19 Instalación de software en sistemas operativos, A.8.8 Gestión de vulnerabilidades técnicas, A.8.34 Protección de los sistemas de información durante las pruebas de auditoría, A.8.11 Enmascaramiento de datos	C
CONTROLES TECNOLÓGICOS	Desarrollo	A.8.26 Requisitos de seguridad de las aplicaciones, A.8.25 Ciclo de vida de desarrollo seguro, A.8.27 Arquitectura de sistemas seguros y principios de ingeniería, A.8.28	C

		Codificación segura, A.8.30 Desarrollo externalizado, A.8.29 Pruebas de seguridad en desarrollo y aceptación, A.8.33 Información de la prueba	
CONTROLES ORGANIZATIVOS	Desarrollo	A.5.19 Seguridad de la información en las relaciones con los proveedores, A.5.20 Abordar la seguridad de la información dentro de los acuerdos con proveedores, A.5.21 Gestión de la seguridad de la información en la cadena de suministro de las TIC, A.5.22 Seguimiento, revisión y gestión del cambio de los servicios de los proveedores, A.5.23 Seguridad de la información para el uso de servicio en la nube	C
CONTROLES ORGANIZATIVOS | CONTROLES DE PERSONAS	Desarrollo	A.5.24 Planificación y preparación de la gestión de incidentes de seguridad de la información, A.6.8 Informes de eventos de seguridad de la información, A.5.25 Evaluación y decisión sobre eventos de seguridad de la información, A.5.26 Respuesta a incidentes de seguridad de la información, A.5.27 Aprender de los incidentes de seguridad de la información, A.5.28 Recopilación de pruebas	C
CONTROLES ORGANIZATIVOS | CONTROLES TECNOLÓGICOS	Desarrollo	A.5.7 Inteligencia de amenazas, A.8.23 Filtrado web, A.8.16 Actividades de seguimiento	C
CONTROLES ORGANIZATIVOS | CONTROLES TECNOLÓGICOS	Desarrollo	A.5.29 Seguridad de la información durante la interrupción, A.5.30 Preparación de las TIC para la continuidad de las actividades, A.8.14 Redundancia de las instalaciones de procesamiento de información	C
CONTROLES ORGANIZATIVOS	SGSI	A.5.31 Requisitos legales, reglamentarios y contractuales, A.5.32 Derechos de propiedad intelectual, A.5.33 Protección de registros, A.5.34 Privacidad y protección de la PII, A.5.35 Revisión independiente de la seguridad de la información, A.5.36 Cumplimiento de políticas, reglas y estándares de seguridad de la información	C

DETALLE DE LA EVALUACIÓN

Nota: *Agregar los cuadros que se requieran para la evaluación:*

Proceso / Servicio:	**CONTEXTO DE LA ORGANIZACIÓN**
Departamento, Área o Unidad de Negocio:	Sistemas de Gestión
Personal Relacionado:	Salvador Santiago Araujo- Gerente Administrativa Ana Laura Hernández Montaño-Coordinador de Sistemas. Rafael Fernando Mendoza Loza-Coordinador de Sistemas Irais Dafne Mendoza Sánchez-Director General Adjunta

Elementos normativos relacionados

4.1 Comprensión de la organización y su contexto, 4.2 Comprensión de las necesidades y expectativa de las partes interesadas, 4.3 Determinación del alcance del sistema de gestión, 4.4 Sistema de gestión de seguridad de la información.

Información Documentada revisada

DOC-CALL-001 Contexto de la Organización Versión 11 con fecha del Mayo 2024, LIS -GSI-009 Matriz de partes interesadas del SGSI, versión 03, Mayo 2024, MAN-GSI- 001 Manual de Gestión de Seguridad de la Información, versión 11 Mayo 2024 , MAP-SIS-001 mapa de procesos V5 Agosto 2024

Descripción de la Evaluación

4.1 Comprender la organización y su contexto

Se muestra el documento DOC-CALL-001 Contexto de la Organización Versión 11 con fecha del Mayo 2024
Una consultoría financiera,
Las Cade la Organización en termino de recursos
Los Flujo
Sistema SICOB
Sistemas
propios
Herramienta

Área de administración, RH, contabilidad, IT
También se tiene sistema de gestión de la
calidad.
Se identifica el documento DOC-CALL-001 Contexto de la Organización Versión 11 con fecha del Mayo 2024
Los diversos Fodas se revisan cada año y se lleva un FODA Por área .

Fortalezas
- Certificación ISO/IEC 27001
- Certificación en ISO/IEC 27001:2022
- Recursos para preservar la confidencialidad, Integridad y disponibilidad de la información
- Sensibilización y concientización al personal
- Capacitación constante a nuestro personal
- Contamos con 3 centros de datos espejo
- Servidores propios
- Respaldos y copias de

seguridad

Oportunidades

- Tercerizar algunos servicios para fortalecer la seguridad de la información.
- Mejoras constantes a la seguridad de la información
Prospección de nuevos clientes por la
certificación
mejoras constantes en la seguridad de la
información Disponibilidad de la información
para capacitación

Debilidades
- Se reciben y custodian expectativas en físico para gestiones
- Resistencia al cambio por parte del personal
- Seguimiento el SGSI
- Implementar controles de seguridad para evitar perdida y divulgación de la
información
- Rotación del Personal
- Resistencia al Cambio
-
Amenazas
- Cambios en el marco legar, regulatorio y/o contractual
- Cualquier amenaza externa que altere la confidencialidad, integridad y disponibilidad de la información.
- Debido al crecimiento del uso de la tecnología, aumenta el riesgo por ataques informáticos.
- Inseguridad Publica
- Cambio de Plantilla de las organización de clientes

Observación : Es Necesario Que La Organización Integre En La Información Del Análisis FODA Las Consideraciones Del Cambio Climático En El Programa Institucional Siguiente.

4.2 Entendimiento de las necesidades y expectativas de las partes interesadas
Se identifica el documento LIS -GSI-009 Matriz de partes interesadas del SGSI, versión 03, Mayo 2024, donde se registran lo siguiente:
No. | Partes interesadas | Grupo | contexto | Necesidad. | Expectativas | Cobranza punta-punta | Investigación de código | Recuperación de
carteras | Gestión domiciliaria | Sistemas | Recursos humanos | contabilidad y tesorería | Compras | total procesos | Seguimiento(retroalimentación) | Método de comunicación
Partes interesadas registradas:

- Clientes → Infonavit → Firma acuerdos para la transferencia de información y cadena de custodia → Encuestas de satisfacción
- Clientes ->Citibanamex
- Citibanamex
- Deudores
- Acreditados
- Sujetos de investigación
- Registro Público
- Instituciones de gobierno
- Colaboradores

- Proveedores
- Sociedad en General
- Organismos de certificación
- Socios de la organización
- Colaboradores

Se observa la correcta identificación de necesidades y expectativas por cada una de ellas.
Encuesta de satisfacción de cliente
Gestión de incidentes
Entrega de eliminación de información

Se mantiene la comunicación

4.3 Determinación del alcance del sistema de gestión de seguridad de la información

Se identifica el documento MAN-GSI- 001 Manual de Gestión de Seguridad de la Información, versión 11 Mayo 2024

"Los servicios de investigación de Crédito (referencias comerciales, verificación de propiedad y sociedades en el RPPyC), Recuperación de Cartera (Extrajudicial y Judicial), Cobranza punta-punta y Gestión Domiciliaria, soportado por los procesos de sistemas, compras, recursoshumanos, contabilidad y tesorería. De acuerdo con la declaración de aplicabilidad (SoA) LIS GSI 007, versión 10, de Septiembre 2024."

Excluyen 2 controles y estos se aceptan como excluidos
A.5.23 :No se cuenta con información para su uso de servicios en la Nube la información se resguarda en servidores
A.8.30 :No se maneja o explota desarrollo externo para las actividades operativas y/0 administrativas todo software ajeno a la Organización es manejado por licencias

4.4 Sistema de gestión de la seguridad de información

Se identifica el documento MAN-GSI- 001 Manual de Gestión de Seguridad de la Información, versión 11 Mayo 2024
4.4.Hemos establecido un mapa de procesos , formatos , registros , diagramas , listado y políticas así como objetivos , entre otros para el mantenimiento del Sistema de Gestión.

Se identifica un mapa de procesos MAP-SIS-001 mapa de procesos V5 Agosto 2024 donde se describe la interacción de los procesos ygestión de riesgos administración de la revisión por la dirección, salidas no conformes y satisfacción por el cliente.

- Procedimiento de Vigilancia.
- Procedimiento de Gestión de Incidentes.
- Procedimiento de Desarrollo Seguro.
- Procedimiento de Activos.
- Procedimiento de Proveedores
-

El análisis de estos documentos se realiza de manera anual y se estipula en el proceso de Gestión Documental

Resultado de la Evaluación:	Observación
Auditor:	Karina Alonso Sánchez

Proceso / Servicio:	**LIDERAZGO | CONTROLES ORGANIZATIVOS**

Departamento, Área o Unidad de Negocio:	Sistemas de Gestión
Personal Relacionado:	Salvador Santiago Araujo- Gerente Administrativa Ana Laura Hernández Montaño-Coordinador de Sistemas. Rafael Fernando Mendoza Loza-Coordinador de Sistemas Irais Dafne Mendoza Sánchez-Director General Adjunta

Elementos normativos relacionados

5.1 Liderazgo y compromiso, 5.2 Política, 5.3 Roles, responsabilidades y autoridades de la organización, A.5.1 Política de seguridad de la información, 9.3 Revisión por la dirección, 6.2 Alcanzando los objetivos y planes de seguridad de la información, 6.3 Planificación de cambios

Información Documentada revisada

POL-SGSI-001 Política de Seguridad de la información, versión 1, Enero 2024, FOR-CAL-016 Índice de incidentes críticos que afecten los pilares de la seguridad de lainformación Abril 2023 Versión 02, FOR-DIR-008 Minuta de revisión por la dirección V 04 Diciembre 2023, de MAN.GSI.001 Manual del Sistema de Gestión Versión 11 con fecha de Enero del 2024

Descripción de la Evaluación

5.1 Compromiso y liderazgo

Se realiza entrevista a alta dirección, se menciona que los bancos que son sus clientes les piden que se revise el tema deseguridad de la información como requisito para su relación comercial
Se menciona que los clientes piden protección a los datos personales que manejan
Se menciona que por la parte interna se trabaja con desarrollo de sistemas.
Crecimiento de la organización sobre seguridad de la información
Se menciona que la concientización del personal ha sido un proceso largo, pero se ha hecho hincapié en las incidencias deseguridad
Se busca la mejora continua constante del sistema de gestión

5.2 Política

Se identifica el documento POL-SGSI-001 Política de Seguridad de la información, versión 1, Enero 2024
"Estamos comprometidos en proporcionar servicios desde la Gestión y Administración de Cobranza Punta – Punta, Investigación de Crédito, Recuperación de Cartera y Gestión Domiciliaria, Orientados a cumplir con los requisitos enmateria de seguridad de información a través de la mejora continua de los procesos y activos, apegándonos a la normatividad legal aplicable."

Se identifica dentro de la intranet
Correo de comunicados de septiembre con fecha del 01/09/2024
También se menciona en entrevista que la política se encuentra un impresa y pegada en las instalaciones de la oficina
Se encuentra disponible a partes interesadas en página de internet:
http://www.ciasc.mx/politicas/.

Se muestra boletín mensual sobre la Política de Seguridad de la Información desde la Intranet y se dan a conocer los procesos de auditoria interna para la toda la organización
Boletín Mostrado con fecha del Agosto del 2024

Se muestran correo electrónicos con envíos de temas relevantes sobre el sistema de gestión con fecha del 13 de Septiembre del 2024

5.3 Roles organizacionales, responsabilidades y autoridades

Se identifico el documento FOR-GSI-043 Matriz de asignación de roles y responsabilidades, versión 3, Enero 2024

Matriz RACI

Actividades | Numerales de la norma | Puestos | Actividades | Perfiles de Puesto

Responsable : R

A:Aprobación

C: Consultado

I: Informado

Se muestra como participa el puesto en los diferentes numerales de la norma

Se identifica que se muestra dentro de la intranet

Cuando se realiza la inducción de personal donde se toca el tema del sistema de gestión y se muestran estos puntos.

Se muestra el Organigrama General.

Director General

Director General Adjunto

Imagen

Áreas Operativas

Auxiliares

Gerente de Contabilidades.

Se cuenta con un Rol dedicado a los temas de los seguridad de la información

Coordinador de Sistemas de Gestión :Ana Laura Hernández Montaño

Actividades:

- Gestión Documental
- Concientización y Capacitación
- Seguimiento a Indicadores
- Auditorias Internas

6.2 Alcanzando los objetivos y planes de seguridad de la información

Se muestra el Documento Política de Seguridad de la información versión 1, Enero 2024

Se identifican los siguientes objetivos para este año:

1. Controlar el número de incidentes críticos que afecten la confidencialidad, disponibilidad, integridad de la información.
2. Mantener la mejora continua a través de la concientización permanente, implementación de proyectos o adquisición de nueva tecnología.
3. Reducir el riesgo residual de manera semestral de acuerdo con la apreciación y tratamiento de los riesgos de laorganización.

Estos se miden por Indicadores

Se identifica el documento FOR-CAL-016 Índice de incidentes críticos que afecten los pilares de la seguridad de la información Abril 2023 Versión 02

El análisis se basa en el análisis de riesgos

Difusión interna

- Intranet SG – Sección política y objetivos de seguridad
- Muestran correo electrónico correo de comunicado@cia.com.mx | Fecha: Abril 2024 (se envía de frecuencia mensual)
- Físicamente se coloca en pizarrón que se encuentra en áreas comunes
- Se difunde en capacitaciones onboarding.

9.3 Revisión por la dirección

Se identifica revisión por la dirección que se realizó en junio FOR-DIR-008 Minuta de revisión por la dirección V 04 Diciembre 2023

Se realiza cada 6 meses

Fecha de la reunión día 16 julio del 2024 , se identifican los puntos que se revisaron:

- El estado actual acciones previas de revisiones por la dirección;
- Los cambios en temas externos e internos que sean relevantes para el sistema de gestión de seguridad de la información | SOC
- Desempeño de los Indicadores
- No conformidades y acciones correctivas
- Monitoreo y resultados de medición
- Resultados de la auditoría, y El cumplimiento de los objetivos de seguridad de la información.
- Recuperación de Cartera
- Capacitación
- Adecuación de los Recursos ERP
- Eficacia de las Acciones de mejora
- Procesos Operativos
- Retroalimentación de las partes interesadas;
  Resultados de la valoración del riesgo y el estatus del plan de tratamiento de riesgo, y las oportunidades para lamejora continua.

Se realiza de manera semestre la próxima revisión por la dirección se llevará acabo el Enero l 2025.

Se entrevista al Represéntate de la Alta Direccion: Irais Dafne Mendoza Sánchez : Director General Adjunto.

Se menciona que por el hecho del sector bancario ha sido relevante mostrarles a sus clientes , que se mantiene la confidencialidad de la información, y de esta forma otorgar ese plus y la consideran como carta de presentación.
Se adquirieron licencias para el cuidado de los Antivirus para gestión de nuevos controles de antimalware.
Se menciona que por parte de los Proveedores se revisan y se firman convenios de confidencialidad y se mantiene con los mismo proveedores y de esta forma seguir manteniendo la controles de Seguridad de la Información

6.3 PLANIFICACIÓN DE CAMBIOS

Se muestra el Documento de MAN.GSI.001 Manual del Sistema de Gestión Versión 11 con fecha de Enero del 2024 .
Implementar cualquier acción necesaria
Revisar la eficacia de las acciones correctivas llevados a cabo
Si es necesario hacer cambios al Sistema de Gestión y de Seguridad de la información
Se conserva evidencia de : La naturaleza de las No conformidades y cualquier acciones posterior llevado a cabo y los resultados de cualquier acción correctiva

Se muestra el Documento FOR-CALL-011 Plan de Cambios y Mejoras 02 con fecha de Junio 2024
Se inicia desde el levantamiento del Ticket por medio del sistema que se cuenta internamente

Tipo de Cambio: Cambio Tecnológico
Clasificación: Cambios e Innovación

Descripción del Cambio :Derivado de la creciente demanda y constante numero de clientes en el procesos de investigación de crédito surge la necesidad de desarrollar el sistema ERP a fin de que permita la sustituir por la empresa el proceso de captura como el de negocio Publico
Beneficios:
Impacto Cuantitativo: Reducir los costos y tiempo de mantenimiento de las Aplicaciones

Reducir los errores durante la Operación
Mejorar el Desarrollo

Impacto Cualitativo:
Mejorar la Seguridad de la Operación
Monitoreas la disponibilidad de la información
Unificar la información de las diversas operaciones y no hacer tanta búsquedas

Actividad | Descripción de la Actividad | Responsable

- Planear
- Hacer
- Actuar

Resultado de la Evaluación:	Conforme
Auditor:	Karina Alonso Sánchez

Proceso / Servicio:	**CONTROLES ORGANIZATIVOS | CONTROLES DE PERSONAS | CONTROLES TECNOLÓGICOS.**
Departamento, Área o Unidad de Negocio:	Sistemas de Gestión
Personal Relacionado:	Salvador Santiago Araujo- Gerente Administrativa Ana Laura Hernández Montaño-Coordinador de Sistemas. Rafael Fernando Mendoza Loza-Coordinador de Sistemas Irais Dafne Mendoza Sánchez-Director General Adjunta

Elementos normativos relacionados

A.5.2 Roles y responsabilidades de seguridad de la información, A.5.3 Segregación de funciones, A.5.5 Contacto con las autoridades, A.5.6 Contacto con grupos de interés especial, A.5.8 Seguridad de la información en la gestión de proyectos, A.8.1 Dispositivos de punto final de usuario, A.6.7 Trabajo Remoto

Información Documentada revisada

FOR-GSI-043 Matriz de asignación de roles y responsabilidades, versión 3, Enero 2024 , 2024 FOR-SGSI-025 Matriz de Roles por activos de información critico Versión 4 con fecha del Enero 2024 FOR-SGSI-025, POL-GSI-001 Políticas Generales de Seguridad de la Información versión 7 con fecha del Agosto 2024, Directorio de contactos con autoridades 2024 Versión 02 con fecha del enero del 2024, PRO-GSI-046 Desarrollo Seguro Versión 8 con fecha de Agosto del 2024, Hoja de Vida e Implementación FOR-GSI-002 Versión 2 con fecha de Mayo 2024,

Descripción de la Evaluación

A.5.2 ROLES Y RESPONSABILIDADES DE SEGURIDAD DE LA INFORMACIÓN

Se identifico el documento FOR-GSI-043 Matriz de asignación de roles y responsabilidades, versión 3, Enero 2024
Matriz RACI
Actividades | Numerales de la norma | Puestos | Actividades | Perfiles de Puesto
Responsable : R
A:Aprobación

C: Consultado
I: Informado
Se muestra como participa el puesto en los diferentes numerales de la norma
Se identifica que se muestra dentro de la intranet

Cuando se realiza la inducción de personal donde se toca el tema del sistema de gestión y se muestran estos puntos.
Se muestra el Organigrama General.
Director General
Director General Adjunto
Imagen
Áreas Operativas
Auxiliares
Gerente de Contabilidades.

Se cuenta con un Rol dedicado a los temas de los seguridad de la información
Coordinador de Sistemas de Gestión :Ana Laura Hernández Montaño
Actividades:

- Gestión Documental
- Concientización y Capacitación
- Seguimiento a Indicadores
- Auditorías Internas

A.5.3 SEGREGACIÓN DE FUNCIONES

Se muestra el Documento 2024 FOR-SGSI-025 Matriz de Roles por activos de información critico Versión 4 con fecha del Enero 2024 FOR-SGSI-025

- Bluemessaging
- SICOB
- Sistema de Gestión

Se registra lo siguiente

Tipo de Objeto | Facultades | Sin Permiso

Se muestra A05AX03 Tabla de segregación de tareas versión 1 fecha 03/07/2023

- Tarea Crítica
- Análisis De Conflictos Potenciales
- Mecanismos De Mitigación
- Área De Responsable

Acceso privilegiado al repositorio documental SharePoint | Responsable Infraestructura Tecnológica

- Mitigación : La solicitud se realiza mediante el formulario de Solicitud de Servicios de TI con motivo fundamentado y se analiza por el área de infraestructura tecnológica para ser aprobada o rechazada

Creación de usuario IAM en AWS | Responsable Infraestructura Tecnológica

- Mitigación: La solicitud se realiza mediante el formulario de Solicitud de Servicios de TI con motivo fundamentado y se analiza por el área de infraestructura tecnológica para ser aprobada o rechazada

Asignación de permisos de administrador a usuarios de dominio | Responsable Infraestructura Tecnológica y Dirección de Desarrollo

- Mitigación: a solicitud se realiza mediante el formulario de Solicitud de Servicios de Ti con motivo fundamentado y se analiza por el área de infraestructura tecnológica y dirección de desarrollo para ser aprobada o rechazada

Solicitud de información entre áreas | Responsable Área

- Mitigación: La Solicitud se realiza discretamente con el responsable del área

No se ha tenido necesidad de realizar ajustes

A.5.5 CONTACTO CON LAS AUTORIDADES | A.5.6 CONTACTO CON GRUPOS DE INTERÉS ESPECIAL

Se muestra FOR-GSI-049 Directorio de contactos con autoridades 2024 Versión 02 con fecha del enero del 2024

Sucursal |

- Policía: 911
- Bomberos : 55 57434343
- Protección Civil: 55434343
- Ambulancia: 57 434344

Se muestra el lista de Grupo de Especial Interés

- Asociación de Cobranza y Servicios Jurídicos
- Amedirth: Asociación Mexicana en Direccion de Recursos Humanos A.C
- Conocer : Conocimientos , Competitiva y Crecimiento

Se muestra grupo de WhatsApp APCONALEP

Grupo de WhatsApp : EXPERTOS CONOCER

Roberto Mirada Consejo Directivos del la APCOB

Correo con fecha del 16/08/2024
Asunto : CONVECOB 2024

Como sabe se acerca nuestra próxima CONVECOB 2024, que se llevara a cabo en el hotel Bel Air los días 25, 26 y 27 de septiembre del presente año, motivo por el que me pongo en contacto con usted para revisar su participación en el evento y realizar el registro correspondiente y asegurar su adquisición.

A.5.8 SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE PROYECTOS.

Se muestra el Documento PRO-GSI-046 Desarrollo Seguro Versión 8 con fecha de Agosto del 2024

Derivado a la naturaleza de los servicios que proporcionamos en la Organización, debemos contar con un área dedicada al desarrollo de aplicaciones y/o software, el área de Sistemas debe de establecer un marco organizacional para el desarrollo de software, en el cual se establezca una metodología para todo el ciclo de vida del desarrollo.
Sistemas
Todos los proyectos de creación de software creados o desarrollado por el personal es propiedad de la organización.
Sistemas
La organización cuenta con un ambiente de ejecución aislado, donde cada aplicativo, información y herramienta se encuentran en diferentes servidores con el fin de mitigar.

Todas las aplicaciones cuenten con un módulo de seguridad, mediante el cual solo sé administre y gestione el ABC (altas, bajas y cambios) de usuarios, asegurando la trazabilidad de las sesiones de cada usuario. Este módulo debe contar con herramientas para la generación de reportes del control de acceso y gestión de usuarios.
El módulo de seguridad deberá alimentarse desde la base de datos de recursos humanos y mantenerse actualizada.

El personal de desarrollo deberá:
1 Establecer un marco organizacional para el desarrollo de software, en el cual se establezca una metodología para todo el ciclo de vida del desarrollo.
2 Documentar todas las etapas del proceso de desarrollo de software en el formato de Hoja de vida e implementación FOR GSI 002.
3.Adoptar las metodologías organizacionales para el desarrollo de proyectos y cumplir con los lineamientos definidos por la organización.
4.Asegurar su participación continua durante el proyecto de desarrollo.
5.Proveer ambientes controlados para el desarrollo de software organizacional como son:

- Entorno de desarrollo.
  Entorno de Testing
  Entorno de UAT.
  Entorno de producción.

Todos los datos de prueba deberán contar con un mecanismo de enmascaramiento de la información reservada y/o confidencial. Una vez utilizados los datos de prueba, el desarrollador deberá borrados antes de su pase a producción

Se muestra la Hoja de Vida e Implementación FOR-GSI-002 Versión 2 con fecha de Mayo 2024

Fecha de Solicitu:26 de Agosto del 2024

Área Solicitante: Investigadores de Crédito

Etapas

1. Análisis de Requisitos
2. Diseño y Arquitectura
3. Programación
4. Pruebas
5. Documentación

Fecha de Termino: 12/10 /2024

Se muestra la Bitácora de Pruebas LIS-GSI-012 Versión 1 con fecha del Enero 2022 firmada y con registros de

Fecha | Prueba a Realizar | Persona que realiza | Dictamen | Firma de Aprobación | Observaciones

Se muestra el Documento de Plan FOR-CALL-011 Cambios y Mejoras

A.8.1 DISPOSITIVOS DE PUNTO FINAL DE USUARIO

Se muestra el Documento de POL-SGSI-001 Políticas Generales de Seguridad de la información Version01 con fecha del Agosto 2024

empresa adopta una política y medidas de seguridad adecuadas para la protección contra los riesgos en la utilización de equipos de cómputo (escritorio y laptop), celulares, impresoras, etc.
Se lleva un registro de todos los equipos de cómputo, monitores, no-breaks, impresoras, celulares, y demás activos tecnológicos, estos son registrados en el documento Inventario y clasificación de activos LIS GSI 023, en el cual se indica número de empleado, nombre completo, puesto y área del usuario responsable de dicho equipo, así como el número de serie, marca, modelo y características técnicas del equipo.

En caso de que el puesto del colaborador requiera traslado constante entre las oficinas y/o sucursales de la empresa, el jefe inmediato o gerente de área, podrá realizar una solicitud de equipo de cómputo, laptop y/o celular empresarial al área de sistemas esto con el fin de que dicho colaborador pueda desempeñar sus funciones sin ningún contratiempo.
La solicitud deberá ser enviada al área de sistemas por medio de CIA-Desk y/o correo electrónico, y esta solicitud será autorizada por la gerencia administrativa y/o dirección general.

El área de Sistemas es responsable del mantenimiento preventivo el cual se debe de realizar de manera semestral de acuerdo al Programa anual de mantenimiento preventivo LIS GSI 010 y concluido dicho mantenimiento, el usuario responsable del equipo y/o jefe de área debe firmar el formato de Conformidad de mantenimiento y correctivo FOR SIS 001 esto con el fin de avalar que recibió de manera adecuada el mantenimiento preventivo.

Los usuarios deben reportar cualquier mal funcionamiento que presente los equipos de cómputo, monitores, no-breaks, impresoras, celulares, y demás activos tecnológicos al área de Sistemas a través de los siguientes canales de comunicación:
1. Portal de soporte (CIA-DESK).
Liga del portal https://ciadesk.ciasc.mx:8080/HELPDESK.
Enviar correo electrónico a soporte@ciasc.mx.
1 Llamada telefónica al conmutador 55-1999-8640 extensiones 169, 170 y 188.
2 Llamada telefónica al equipo celular del departamento de sistemas 55-5023-0222.

Es responsabilidad del usuario que firma la Carta responsiva FOR GSI 031 para preservar la integridad física del dispositivo móvil como su uso en zonas públicas, salas de reunión, áreas desprotegidas fuera de las instalaciones de la empresa, así como atender los controles administrativos que se le indiquen para salvaguardar la confidencialidad e integridad de este.

Se muestra el Formato de Carta Responsiva FOR- GSI-31 Agosto 2024 Versión 10

Datos del colaborador

Equipos Asignados: | Activo | Marca | Modelo

- Numero de Empleado
- Fecha de Acceso
- Fecha de Retiro
- Asignación de Usuario

Firma de recepción de equipos y accesorios

- Usuario
- Personal de Sistemas

Firma de Entrega de Equipos y Accesorios

Se muestra Carta Responsiva los 3 Sitios

Sucursal : Nezahualcóyotl

Departamento: Recursos Humanos

Numero de Empleado: 9732

Fecha de Entrega : 09/09/2024

Nombre: Torres Velasco Berenice

Equipo: Celular Huawei Y6 2019

Sucursal : Valle Insurgente
Departamento: Cobranza Punta- Punta
Numero de Empleado: 7968
Fecha de Entrega : 21/05/2024
Nombre: Antonio Gabriel Muñoz Jurado
Equipo: Computadora HP 260 G3 DM
MONITOR ACER

Sucursal : Toluca
Departamento: Cobranza Punta- Punta
Numero de Empleado: 9013
Fecha de Entrega : 05/02/2024
Nombre: Ricardo Sánchez Matías
Equipo: Computadora HP 280 G5 SFF
MONITOR DELL E1916HV

A.6.7 TRABAJO REMOTO

Se muestra el Documento POL-GSI-001 Políticas Generales de Seguridad de la Información versión 7 con fecha del Agosto 2024

El teletrabajo en la empresa se realiza de la siguiente manera:
• Personal que por la naturaleza de su puesto está autorizado para realizar teletrabajo desde equipos de cómputo portátiles corporativos, declarando únicamente los siguientes:

- Director General.
  Director General Adjunto.
  Gerente Administrativo.
  Gerente de Recursos Humanos.
  Gerente de Investigación de Crédito.
  Gerente de Cobranza Punta - Punta.

> Personal del área de Sistemas, no tiene autorizado realizar teletrabajo, sin embargo, si puede conectarse vía remota a los equipos de cómputo de la empresa (excepto a los equipos de que involucran la operación del cliente CitiBanamex) para soporte técnico y mantenimiento y este siempre será en el equipo de cómputo
ubicado en su oficina correspondiente del coordinador y/o auxiliar de sistemas.
◦ Personal Operativo, no se permite y queda estrictamente prohibido la realización de teletrabajo.
◦ Personal Operativo Banamex no se permite y queda estrictamente prohibido la realización de teletrabajo.

La empresa cuenta con una infraestructura de red por medio de directorio activo, la cual administra GPO a cada grupo y usuario del dominio; por este motivo las computadoras de la empresa que tengan autorización para realizar teletrabajo se deberán conectar por medio de VPN, ya que de lo contrario no podrán acceder a la red del directorio
activo y por tal motivo tampoco al servidor de archivos.

Resultado de la Evaluación:	Conforme
Auditor:	Karina Alonso Sánchez

Proceso / Servicio:	**EVALUACIÓN DEL DESEMPEÑO Y MEJORA**
Departamento, Área o Unidad de Negocio:	Sistemas de Gestión
Personal Relacionado:	Salvador Santiago Araujo- Gerente Administrativa Ana Laura Hernández Montaño-Coordinador de Sistemas. Rafael Fernando Mendoza Loza-Coordinador de Sistemas Irais Dafne Mendoza Sánchez-Director General Adjunta

Elementos normativos relacionados

9.1 Seguimiento, medición, análisis y evaluación, 9.2 Auditoría interna, 10.2 No conformidad y acción correctiva, 10.1 Mejora continua

Información Documentada revisada

FOR-CAL-003 Incidentes críticos 2024 V02, Resultado de Capítulos FR-SGI-048 Versión 3 con fecha Agosto 2024, FOR CA 014 Calendario de auditorías, versión 01, Enero 2024, FOR-REH-001 Formato descripción de puesto, versión 3, Enero 2024, FOR-GSI -048 Plan de acción Agosto 2024 v03, FOR-CALL-011 Plan de Cambios y Mejoras 02 con fecha de Junio 2024, FOR-CALL-011 Plan de Cambios y Mejoras 02 con fecha de Junio 2024, Resultado de Controles FR-SGI-048 Versión 3 con fecha Agosto 2024.

Descripción de la Evaluación

9.1 Monitoreo, medición, análisis y evaluación

Se identifica el documento FOR-CAL-003 Incidentes críticos 2024 V02

Objetivo: índice de incidentes críticos reportados por el usuario

Fuente de información CIA- DESK

Meta: No tener ninguna incidencia que ponga en riesgo la confidencialidad disponibilidad e integridad de la información

Frecuencia de medición: Mensual

Responsables: Coordinador de sistemas TI

9.2 AUDITORÍA INTERNA

Se muestra el Documento de Resultado de Capítulos FR-SGI-048 Versión 3 con fecha Agosto 2024

Se muestra Lista de Verificación Capítulos del 4 a 10

NC :

NC : 5.2 : |3 SITIOS Durante el muestreo aleatorio realizado al personal, se identificó que conocen a que se refieren las políticas de seguridad de la información (escritorio limpio, recoger impresiones de la impresora, uso de dispositivos móviles, etc.), sin embargo, no ubican la política general de seguridad de la información y/o contexto de la organización

Plan de Acción: Campaña de Comunicación interna enfocada a la ubicación y comprensión de la Política
Inducir información de la Política y Objetivos |

Se realizan Juntas Generales para revisar avances de los Planes de Acción.

NC :
6.1 SEDE Insurgentes: Para el tratamiento de riesgos, la auxiliar de sistemas de insurgentes indica que desconoce el proceso a seguir ya que este tratamiento solo se realiza en la oficina de Nezahualcóyotl y a ella solo le indican las acciones a realizar en su sucursal.

Plan de Acción: Realizar una sesión con todo el equipo para poder concientizar en temas de Riesgos
Estado: Cerrado: 30 de Agosto del 2024

7.5 : Durante el ejercicio de auditoria se revisó la parte de control de información documentada y de identifica que en el procedimiento
"Respaldos y eliminación de información" PRO GSI 032 se indica que se hacen respaldos diarios de la información, sin embargo, no indica que horarios deben realizarse, también se identificó que se manejan dos formatos "Excepciones" FOR GSI 047 para un lapso de tres meses y "Carta responsiva de excepciones" FOR GSI 051, la cual se indicó que es permanente, sin embargo, no se menciona en el punto 7.2 del procedimiento de "control de accesos" PRO GSI 016 que este documento sea permanente; por otra parte se identifica que en recursos humanos están utilizando los formatos FOR GSI 058; Manejo de Información Citibanamex y FOR GSI 059 Carta Compromiso de Accesos, sin embargo estos no se encuentra en su versión vigente. Aplica para Nezahualcóyotl, Insurgentes y Toluca.

Plan de Acción: Se analizo con los 5 Porques!! Revisar y actualiza el contenido de los documentos , se suben la documentación actualizada en la intranet
Estado : Cerrado 30 de Agosto del 2024

Se muestra el Documento de Resultado de Controles FR-SGI-048 Versión 3 con fecha Agosto 2024

Observación : 8.1.1 : En la sucursal de Nezahualcóyotl, en la carpeta donde se resguardan los formatos "Programa Anual de Mantenimiento Preventivo" LIS GSI 010 hay formatos del año 2022, haciendo un muestreo, se identificaron tres formatos que no cuentan con las firmas completas de los usuario

Plan de Acción : Se realiza una sesión con todo el equipo de sistemas para concientizar a todo el equipo en temas de riesgos y se refuerce en los 3 sitios

NC: 9.2.3 En la sucursal de Toluca se identifico que existe personas (Abogado auxiliar administrativo) con acceso libre a internet por ejemplo Netflix , YouTube , Facebook

Plan de Acción :El gerente de TI administrativo y el coordinador TI Realizaron un monitoreo general a los equipos de cómputo de Nezahualcóyotl insurgente y Toluca con el fin de identificar todos los equipos que pudiera tener configuraciones distintas
Estado : Cerrado 30 de Agosto del 2024

NC:9.2.6 : En la sucursal de Insurgentes, en el muestreo aleatorio realizado al formato "Excepciones por puesto " FOR SIS 009 se revisaron 3 máquinas; 1 de gerente y 2 abogados, en las Áreas de los abogados se encontró que tiene acceso a WhatsApp web, pero no se cuenta con el formato de excepciones.

Plan de Acción : El gerente de TI administrativo y el coordinador TI Realizaron un monitoreo general a los equipos de cómputo de Nezahualcóyotl insurgente y Toluca con el fin de identificar todos los equipos que pudiera tener configuraciones distintas
Estado : Cerrado 30 de Agosto del 2024

NC:A.7.1 : En el corporativo, en las áreas seguras se indica que se maneja el formato "Bitácora de acceso a las áreas seguras" FOR GSI 004 para registro de personal que ingresa a dichas áreas, sin embargo, al revisar las áreas seguras, se identificó que en el archivo muerto no se cuenta con dicha bitácora y en el archivo temporal, si está la bitácora, pero no cuenta con ningún registro y tampoco se encuentra actualizada a la última versión del formato.

Plan de Acción :Implemento el equipo de sistemas en las áreas seguras restantes el formato de bitácora de acceso a áreas seguras
Estado: Cerrado: 28 de Agosto del 2024

NC: A.7.1.4.: Durante el recorrido de la sucursal de Toluca se identifican que los sensores de humo no funcionan ya que no tiene sus batería instalada

Plan de Acción : Se realizo la cotización en Steren para adquisición de baterías y se compran las pilas y se muestra correo con el seguimiento de las compras de las Pilas 6 de Septiembre del 2024
Estado : Cerrado 9 de Septiembre del 2024

NC: A.7.7 En la Sucursal de Toluca se identifica se detecto que personal de Toluca al ausentarse no bloquea el equipo

Plan de Acción : Se realiza una campaña interna enfocada a la ubicación y comprensión de la Política y objetivos de seguridad de la información , incluir la política y objetivos de seguridad de la información del SGSI
Estado : Abierto

NC: 5.14 Transferencia de Información; Se detectó que el auxiliar administrativo y abogado de la sucursal de Toluca pueden enviar correos electrónicos a dominios distintos a clasc.mx contrario a lo que indican las políticas generales de seguridad de la información POL GSI 001

Plan de Acción : : El gerente de TI administrativo y el coordinador TI Realizaron un monitoreo general a los equipos de cómputo de Nezahualcóyotl insurgente y Toluca con el fin de identificar todos los equipos que pudiera tener configuraciones distintas
Estado : Cerrado: 30 de Agosto del 2024

OBSERVACION: A.6.8 : En el procedimiento "Gestión de incidentes " PRO GSI 020, no está definido el lapso que se tiene para documentar el incidente a partir de que se presenta el evento. Se revisó un incidente documentado en el mes de marzo, el cual inicio el 19-03-24 y finalizo el 20-03-24, pero la fecha en que se documento es del 19-04-24 (un mes después).

Plan de Acción :Se realizo una sesión con todo el equipo de sistemas para poder concientizar al equipo de los riesgos y oportunidades y su contribución

NC: A5.36 : Al revisar aleatoriamente las licencias de los equipos se encontró en las tres sucursales que no todo el personal tiene activada la licencia de Windows

Plan de Acción :Se levanto un ticket al Proveedor Ansiami con el fin de recibir soporte técnico con la herramienta sentinel one : ya que se identificó que el sistemas XDR estaba bloqueándolo
Estado : Cerrado 29 de Agosto del 2024

Se identifica el documento Plan de auditoría interna FOR-CAL-013 Versión 2 Mayo 2024 Se identifican todos los requisitos del esquema de ISO 27001
Las auditorías internas se realizan solo una vez al año

Se identifica el documento FOR CA 014 Calendario de auditorías, versión 01, Enero 2023 se realizó en agosto 2023
Se menciona la auditoría externa de ISO 27001

Informe de auditoría: Porcentaje de Cumplimiento Total : 93:43
FOR CA 014 Calendario de auditorías, versión 01, Enero 2024 Porcentaje de cumplimiento total = 98.64%
Perfil auditor:
Auditor Líder : Fundamentos de SGSI FAMILIA ISO 27001 | Fecha :09/2021 |Proveedor AENOR
Seminario : Actualización de las Normas ISO/IEC 27001:2022 con fecha del 23 de Enero del 2023

Auditor Ana Laura Hernández Montaño

Se identifico el documento FOR-REH-001 Formato descripción de puesto, versión 3, Enero 2024 Formación y actitudes Fundamentos jurídicos de seguridad e la información Gestión de riesgos de seguridad de la información
Gobierno y gestión de sistemas de seguridad de la información Seminario de actualización de las normas ISO 27001 versión 2022 Implementación y Auditoria a un SGSI ISO 27001:2013 19 a 27 Julio 2021

Se muestra evidencia de Adriana Munive Montes : Auditor :
Capacitación en SGSI
Se muestra capacitación de Reyna Sánchez Mota
Fecha 28 de Junio del 2024
Se muestra capacitación de Luis Gerardo Torres Flores

Se muestra Curso en ISO 19011:2018 Directrices para la Auditoria de los sistemas de gestión
Fecha : 17 de junio del 2024
Adriana Munive Montes : Auditor

Se muestra Curso en ISO 19011:2018 Directrices para la Auditoria de los sistemas de gestión
Fecha : 17 de junio del 2024

Rafael Fernando Mendoza : Auditor

10.1 No conformidad y acción correctiva | 10.2 Mejora continua
Se identifica el documento FOR-GSI -048 Plan de acción Agosto 2024 v03
NC Mayor: Durante la auditoría, se solicitó al Coordinador de Capitación y Comunicación el seguimiento al Programa Anual de Capacitación (PAC); sin embargo, únicamente se tienen las capacitaciones realizadas en la plataforma UNIVERCIA, del resto de las capacitaciones no se cuenta con evidencia, porque no se han llevado a cabo.

Se realizo análisis 5 porques

Acción correctiva: se debió a la falta de interés del responsable
Se reagendarán las capacitaciones

NC Menor: Durante la auditoría se notó que el Formato de Recursos Humanos FOR REH 003, no es adecuado para la operación, ya que no tiene la información necesaria y está desactualizado, además de no llenarse correctamente. Por otro lado, no se tiene el formato FOR GDO 002 para el personal de nuevo ingreso del área de gestión domiciliaria y para el

empleado 6165, no se cuenta lleno el formato de referencias laborales FOR REH 007, por último se detectó que en el mapa de procesos de recursos humanos se indica que se investiga el buró de crédito, sin embargo, a la fecha ya no es un requisito para ingresar a la empresa.

Se realizo análisis 5 porques

Acción correctiva: No se encuentra actualizado el documento

NC Mayor: Se identificó que el colaborador 6165, quien ocupa el puesto de asesor domiciliario, no cuenta con referencias declaradas en el formato FOR REH 003 Referencias laborales, y dicho formato se encuentra anexado al expediente en blanco.

Se identificó que el personal de nuevo ingreso del proceso operativo "gestión domiciliaria", no firmo el documento FOR GDO 002 Carta de Confidencialidad CitiBanamex.

Se realizo análisis 5 porques

Acción correctiva: Se contratará a un becario que revise y actualice los expedientes de personal.

NC Mayor: Durante el recorrido aleatorio se identificó que personal no porta su credencial corporativa. Se realizo análisis 5 porques
Acción correctiva: Se realizará comunicación sobre la importancia de usar el gafete.

NC Mayor: Se identifica que el celular de la gerente de recursos humanos, si puede descargar aplicaciones desde la Play store.

NC Menor: Se muestra el inventario LIS GSI 023 con la información diferente a las cartas responsivas FOR GSI 031 y los números de serie son diferentes a los reales.
Se muestran cartas responsivas con número de serie diferentes (David y Leydi) y no están registrados los no break. Hasta el momento se encuentran todas las no conformidades cerradas y solo una en proceso
Mejora continua:

Se muestra el Documento FOR-CALL-011 Plan de Cambios y Mejoras 02 con fecha de Junio 2024
Se inicia desde el levantamiento del Ticket por medio del sistema que se cuenta internamente

Tipo de Cambio: Cambio Tecnológico
Clasificación: Cambios e Innovación

Descripción del Cambio :Derivado de la creciente demanda y constante número de clientes en el procesos de investigación de crédito surge la necesidad de desarrollar el sistema ERP a fin de que permita la sustituir por la empresa el proceso de captura como el de negocio Publico
Beneficios:
Impacto Cuantitativo: Reducir los costos y tiempo de mantenimiento de las Aplicaciones
Reducir los errores durante la Operación
Mejorar el Desarrollo

Impacto Cualitativo:
Mejorar la Seguridad de la Operación
Monitoreas la disponibilidad de la información

Unificar la información de las diversas operaciones y no hacer tanta búsquedas

Actividad | Descripción de la Actividad | Responsable

- Planear
- Hacer

Actuar

Resultado de la Evaluación:	Conforme
Auditor:	Karina Alonso Sánchez

Proceso / Servicio:	**CONTROLES TECNOLÓGICOS**
Departamento, Área o Unidad de Negocio:	Sistemas de Gestión
Personal Relacionado:	Salvador Santiago Araujo- Gerente Administrativa Ana Laura Hernández Montaño-Coordinador de Sistemas. Rafael Fernando Mendoza Loza-Coordinador de Sistemas Irais Dafne Mendoza Sánchez-Director General Adjunta

Elementos normativos relacionados

A.8.24 Uso de la criptografía

Información Documentada revisada

A.8.24 Uso de la criptografía

Se muestra POL-SGSI-001 Políticas Generales de Seguridad de la Información Verion 07 con fecha de Agosto del 2024
La empresa busca proteger la información crítica a través de los siguientes controles Criptográfico
Tipo de Información | Herramienta Criptográfica | Algoritmo de Encriptación | Longitud de la Clave | Justificación de Aplicabilidad
Intranet CIA

- EL área de sistemas es la responsable de establecer las siguientes reglas sobre la gestión de claves:
  > Generación de claves criptográficas privadas y públicas.
  Activación de claves criptográficas.
  Destrucción de claves.
  Cambio periódico de claves

Los propietarios de los activos individuales sobre los cuales se aplican controles criptográficos son los responsables por la correcta aplicación de los controles criptográficos particulares.
Nota. La criptografía de CitiBanamex es generada por el cliente cada 30 días, el cual envía el token necesario para la operación al personal correspondiente vía correo electrónico, dicha criptografía para CitiBanamex es AES 256 bits.

Se muestra como evidencia el Certificado SSL TLS RSA CA 01
*.CIASC.MX
Vencimiento : 11 de Abril del 2025

Se muestra evidencia de correo encriptado del cliente Citibanamex
Fecha : Viernes 20 de Septiembre del 2024
Con leyenda " Respuesta Segura"
Y se muestra el acceso al correo a través de una contraseñas

Resultado de la Evaluación:	Conforme
Auditor:	Karina Alonso Sánchez

Proceso / Servicio:	**SOPORTE | CONTROLES ORGANIZATIVOS | CONTROLES DE PERSONAS**
Departamento, Área o Unidad de Negocio:	RH
Personal Relacionado:	Berenice Torres Velazco | Gerente de RH

Elementos normativos relacionados

7.1 Recursos, 7.2 Competencia, 7.3 Concientización, 7.4 Comunicación A.6.1 Chequeo, A.6.2 Términos y Condiciones de empleo, A.5.4 Responsabilidades de Gestión, A.6.3 Sensibilización, educación y formación en materia de seguridad de la información, A.6.4 Proceso disciplinario, A.6.5 Responsabilidades después de la terminación o cambio de empleo, A.6.6 Acuerdos de confidencialidad o no divulgación

Información Documentada revisada

Formato FOR-REH-018 Entrevista Estructurada Versión 06 fecha 02&06/2020, Descripción de Puesto FOR REH 001 Versión 4 de fecha Septiembre 2024 , Requisición de Personal FOR-REH-009 Versión 4 con fecha de Agosto del 2024, Entrevista de Salida FOR-REH-013 Versión 3 con fecha Enero 2019, Carta responsiva de equipos y accesos FOR GSI 031 versión 9 de fecha Octubre 2020,

Descripción de la Evaluación

7.1 RECURSOS

La organización cuenta con el personal y herramientas necesarias para que el colaborador esté capacitado, concientizado en temas de seguridad de la información.

7.4 COMUNICACIÓN

se consideran los requisitos normativos para la comunicación, además se registran actividades de concientización que se evidencianenviado por correo electrónico con frecuencia mensual | Comunicados del tema de seguridad

Se realiza un Matriz de Comunicación

- Tipo de Acción
- Clasificación
- Que Comunicar
- Cuando Comunicar
- A quien Comunicar
- Quien Comunica
- Quien Solicita
- Proceso Responsable de Comunica

Se muestra Correo del Comunica : Política de Seguridad de la Información
Fecha: 16 de Agosto del 2024 .
Correo que envía: comunica@cia.mx

A.7.1.2 INVESTIGACIÓN | 7.2 Competencia |

Se muestra formato de Requisición de Personal FOR-REH-009 Versión 4 con fecha de Agosto del 2024
Fecha de Solicitud: 20 de Septiembre del 2024

Dataos del Solicitante

Requerimiento

- Nuevo Puesto
- Jubilación
- Abandono de Empleo
- Incapacidad

Definiciones del Puesto
Perfil Requerido
Habilidades Requeridas

- Comunicación Afectiva
- Adaptarse a cambios
- Poder Personal
- Autorización

Descripción de Puesto FOR REH 001 Versión 4 de fecha Septiembre 2024
Puesto Abogado | Valle

- Objetivo del Puesto
- Ubicación dentro del organigrama n
- Funciones y Actividades
- Competencias Solicitada | Sección Normas ISO/IEC 9001 e ISO/IEC 27001
- Perfil Educativo | Titulo y Derecho, Cedula , 6 meses de Experiencia

Se muestra Descriptivo de Puesto : Auxiliar Administrativo

- Auxiliar Administrativo
- Objetivo del Puesto
- Ubicación dentro del organigrama n
- Funciones y Actividades | Cumplir con las Normas establecidas en la Organización
- Competencias Solicitada | Sección Normas ISO/IEC 9001 e ISO/IEC 27001
- Perfil de Puesto: Bachillerato

Puesto Asesor Telefónico | TOLUCA

- Objetivo del Puesto
- Ubicación dentro del organigrama n
- Funciones y Actividades
- Competencias Solicitada | Sección Normas ISO/IEC 9001 e ISO/IEC 27001
- Perfil Educativo | Bachillerato Concluido
- Atención al Cliente
- Meses de Experiencia.

Se realiza las Publicaciones en la Bolsa de Talento
OCC
CompuTrabajo

Se muestra la publicación del Perfil Abogado en OCC
Fecha de Publicación : Septiembre 2024

Se muestra Expediente del Perfil Abogado
Formato FOR-REH-018 Entrevista Estructurada Versión 06 fecha 02&06/2020

- Objetivos
- Cual es tu meta en ?
- Menciona 3 cualidades
- Menciona 3 áreas de Oportunidad
- Nombre : Ana Rubí Ortega Barrios
- Fecha:23/09/2024
- Puesto: Abogado
- Candidato
- Experiencia Laboral
- Curriculum

Se muestra Publicación de Perfil Auxiliar Administrativo
Psicotest Herramienta de Test
Psicométricos

- Auxiliar Administrativo | Neza
- SUAREZ MARTINEZ CHRISTIAN ALEJANDRO
- 26 Agosto del 2024
- Se muestra Psicotest
- Pruebas de confianza, Honestidad ética y valores

- Puesto : Abogado :
- Araceli Bautista
- 19 de Junio 2024
- Se muestra Psicotest
- Pruebas de confianza, Honestidad ética y valores

- Asesor Telefónico | Toluca
- De Jesús Chavarrieta Raquel Magdalena ingreso : 15 de Junio del 2024
- Se muestra Psicotest: 10 de Julio del 2024
- Pruebas de confianza, Honestidad ética y valores publicación de vacante | OCC| CompuTrabajo | redes sociales

A.7.1 Términos Y Condiciones Del Empleo

Contrato | convenio de confidencialidad | términos y condiciones

- Contrato individual
- Carta de Aceptación y Lineamiento de Trabajo
- Convenio de confidencialidad
- Aviso de privacidad para empleados
- Promesa de Confidencialidad
- Recepción de la Normativa

En el Contrato se visualiza la siguiente leyenda :
- No haré ningún uso personal en mi beneficio de cualquier herramienta o información proporcionada por la empresa para el buen desarrollo de la prestación de mi trabajo, por ello me haré responsable del uso, manejo y depósito de sus materiales, herramientas y utensilios de trabajo que con motivo de realizar mis actividades dentro de la empresa utilice tales como users

y passwords que me sean asignados, en el entendido que son de mi entera responsabilidad y el posible mal uso que pueda hacerse de ellos.
2 - Comprendo que todos los desarrollos realizados y trabajos creados por mí, o bajo mi dirección, con relación a las tareas asignadas por la organización serán de propiedad absoluta y exclusiva de la empresa; que cualquier y todo derecho de autor e interés sobre la propiedad de tales desarrollos y trabajos pertenecerán a la compañía.
aquel
1 - Me obligo expresamente cumplir los requisitos, controles, políticas, lineamientos, procedimientos y manuales en materia de seguridad de la información que los diversos clientes impongan y exijan a la empresa y que me han sido dados a conocer y en caso de incumplimiento, a cubrir los daños y perjuicios que con motivo del incumplimiento se generen, independientemente de las demás acciones legales a que hubiere lugar, especialmente las de carácter penal que pudieran originarse.
2 - Me obligo a respetar la privacidad de los datos de los clientes de la empresa y de los clientes de los clientes que sólo podré utilizar de conformidad con las instrucciones que dicte la empresa, de conformidad con lo establecido en la Ley Federal de Protección de Datos Personales en Posesión de los Particulares y su reglamento, siendo aplicable únicamente respeto a los datos personales.
En virtud de lo anterior me obligo a que los datos de terceros que se lleguen a recabar, por o para el desempeño de mis funciones y que incluya datos personales y/o datos personales sensibles se sujetarán a los términos y condiciones de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP) y su reglamento.

- Araceli Bautista
- Abogado
- Se muestra contrato
- Convenio de confidencialidad: : 24 de junio del 2024
- Carta de aceptación : : 24 de junio del 2024
- Carta de Recibo de información Normativa : 24 de Junio del 2024
- Aviso de privacidad: Fecha : 24 de junio del 2024
- Promesa de Confidencialidad: : 24 de junio del 2024

- Jesús Chavarrieta Raquel Magdalena : Asesor Telefónico
- Se muestra contrato
- Convenio de confidencialidad: : 15 de julio del 2024
- Carta de aceptación : : 15 de julio del 2024
- Carta de Recibo de información Normativa : 15 de julio del 2024
- Aviso de privacidad: Fecha : 15 de julio del 2024
- Promesa de Confidencialidad: 15 de julio del 2024

- Suarez Martínez Christian Alejandro : Auxiliar Administrativo
- Se muestra contrato
- Convenio de confidencialidad: : 26 de agosto del 2024
- Carta de aceptación : : 26 de agosto del 2024
- Carta de Recibo de información Normativa :26 de agosto del 2024
- Aviso de privacidad: Fecha : 26 de agosto del 2024
- Promesa de Confidencialidad: 26 de agosto del 2024

7.3 Concientización

A.7.2.2 Concientización, Educación Y Capacitación En Seguridad De La Información

Capacitaciones en temas de seguridad de la información, adicional se muestra se utiliza la herramienta UniverCIA que apoya en toda la gestión de las capacitaciones. Desde la asignación hasta la evaluación de las capacitaciones al colaborador.

- Onbording
- SGSI
- Anticorrupción y anti soborno
- Ley de protección de datos personales

Los responsables deben acompañar apoyo a sus colaboradores
- Cursos
- El área administrativa colabora con la dirección de los programas de formación según corresponda
- Los cursos deben basarse dentro de lo posible en un aprendizaje activo Requisitos para aprobar cursos
- Empresa que impartirá la capitación
- Nombre del curso o capacitación programa o agenda del curso o capacitación
- Precio del curso
- Contacto número de cuenta para realizar pago
- Fecha de curso

Plan de capitación PAC 2024
- Numero
- Actividad
- Responsables
- Procedimiento
- Herramienta

Plan anual de capacitación PAC 2024
- Área nombre cursos
- Categoría
- Objetivo de cursos
- Instructor
- Participantes
- Interno
- Modalidad
- Periodo de participación

Se muestra cursos de
- Inducción CIA
- Anticorrupción
- Ley de protección de datos
- Verificación de domicilio
- Actualización : SGSI
- Curso de Reforzamiento de Inducción del SGSI

Se muestra 3 Expedientes 1 por cada Sitio
- Araceli Bautista | VALLE
- Abogado
- Jesús Chavarrieta Raquel Magdalena : Asesor Telefónico | TOLUCA
- Suarez Martínez Christian Alejandro : Auxiliar Administrativo | NEZA

A.7.2.3 Proceso Disciplinario

Evidencia se muestra proceso disciplinario

- Acta administrativa
- Se envía correo

Código de Convivencia 2022
- Incidentes de consecuencia baja
- Incidentes de consecuencia media

- Incidentes e consecuencia alta Herramienta
- UniverCia
- Onboarding
- Código de convivencia
- SGSI
- Datos personales
- Anticorrupción

Se muestra 3 Expediente 1 por cada Sitio

- Araceli Bautista | VALLE
- Abogado
- Jesús Chavarrieta Raquel Magdalena : Asesor Telefónico | TOLUCA
- Suarez Martínez Christian Alejandro : Auxiliar Administrativo | NEZA

A.7.3.1 Responsabilidades En La Terminación O Cambio De Empleo

Se muestra una Baja
Puesto: Programador
Entrevista de Salida FOR-REH-013 Versión 3 con fecha Enero 2019
DCS Delta Corporate Servicies S.A DE C.V
Fecha de Salida : 20 de Septiembre del 2024
Carta Escrita a mano
Carta : Aviso de Rescisión de la Relación Laboral

Se muestra correo de Solicitud de Finiquito 9510 Ibarra Jimenez Brian Kaled
Fecha de Envió : 23 de Septiembre del 2024

Carta responsiva de equipos y accesos FOR GSI 031 versión 9 de fecha Octubre 2020
Empleado : Ibarra Jimenez Brian Kaled

- Aviso de rescisión
- Promesa de confidencialidad
- 2 años de confidencialidad
- Carta Compromiso de Accesos
- Carta Responsiva de Excepciones FOR-GSI-051 Versión 1 con fecha de Julio 2023
-

Se envía correo electrónico donde se da aviso de la baja del colaborador para el retiro de sus accesos y baja del equipo, utilizando la carta responsiva que previamente firmo en la asignación.

6.6 Aviso De Privacidad

Se muestra los Aviso de Privacidad entregados a los Colaboradores:

Se muestra 3 Expedientes 1 por cada Sitio

- Araceli Bautista | VALLE
- Abogado
- Jesús Chavarrieta Raquel Magdalena : Asesor Telefónico | TOLUCA
- Suarez Martínez Christian Alejandro : Auxiliar Administrativo | NEZA

Se muestra la Siguiente Leyenda :

DELTA CORPORATE SERVICES, S.A. DE C.V. no cederá los datos de los solicitantes a terceros salvo solicitud previa y consentimiento expreso del titular, y en los supuestos contemplados por el artículo 37 de la Ley Federal de Protección de Datos Personales en posesión de los Particulares vigente.
Usted tiene derecho a ejercitar sus derechos denominados "ARCO", de acuerdo con lo siguiente:

Acceso: Usted podrá elegir la manera de comunicarse, ya sea vía telefónica o mediante escrito directo, a los teléfonos o al domicilio, según corresponda, que más abajo quedan detallados, para efectos de que DCS DELTA CORPORATE SERVICES, S.A. DE C.V..., le proporcione los Datos Personales y Datos Personales Sensibles, incluyendo, incluso los datos financieros o patrimoniales relacionados con Usted, y que se encuentren en su posesión, de conformidad con la Ley.
Rectificación: Usted podrá solicitar por escrito a DCS DELTA CORPORATE SERVICES, S.A. DE C.V., que cualquiera de sus Datos Personales y Datos Personales Sensibles, incluyendo incluso sus datos financieros o patrimoniales, sean corregidos o modificados, según corresponda, de conformidad con la Ley.
Cancelación: Usted podrá solicitar por escrito a DCS DELTA CORPORATE SERVICES, S.A. DE C.V., que se cancelen o den de baja sus Datos Personales y Datos Sensibles, incluyendo incluso sus datos financieros o patrimoniales, siempre y cuando exista una causa que justifique dicha acción y no tenga usted obligaciones pendientes de cubrir de conformidad con la Ley.
Oposición: En caso de que Usted no tenga relación u obligación legal alguna con DCS DELTA CORPORATE SERVICES, S.A. DE C.V., y decida no contratar para sí ninguno de los servicios que ésta le ofrece, puede hacer uso de este derecho, no compartiendo dato alguno.
Para ejercer los derechos anteriormente mencionados podrá enviar la "Solicitud para atención a los requerimientos ARCO", al correo electrónico r.humanos@ciasc.mx quien le enviará el formulario correspondiente y le dará atención al trámite.
El presente Aviso de Privacidad podrá ser modificado o actualizado en el futuro; en cualquier caso, se hará de su conocimiento mediante el envío de un correo electrónico con el nuevo Aviso, a la cuenta de correo electrónico proporcionada por usted, y en caso de no tener dicho correo, se hará de forma personal.

Se muestra Convenio de Confidencialidad del Proveedor:
DIGICOPIAS. S.A DE C.V : 21 de Abril del 2022
Clausula : Datos Personales

Resultado de la Evaluación:	Conforme
Auditor:	Karina Alonso Sánchez

Proceso / Servicio:	**CONTROLES FÍSICO**
Departamento, Área o Unidad de Negocio:	Sistemas de Gestión
Personal Relacionado:	Salvador Santiago Araujo- Gerente Administrativa Ana Laura Hernández Montaño-Coordinador de Sistemas. Rafael Fernando Mendoza Loza-Coordinador de Sistemas Berenice Torres Velasco-Gerente de RH Irais Dafne Mendoza Sánchez-Director General Adjunta Jesús Eduardo Martínez Padilla : Asistente de Direccion

Elementos normativos relacionados
A.7.1 Perímetros de seguridad física, A.7.2 Entrada Física, A.7.3 Aseguramiento de oficinas, habitaciones e instalaciones., A.7.4 Supervisión de la seguridad física, A.7.5 Protección contra amenazas físicas y ambientales, A.7.6 Trabajar en áreas seguras, A.7.8 Emplazamiento y protección de equipos, A.7.11 Servicios públicos de apoyo, A.7.12 Seguridad del cableado, A.7.13 Mantenimiento de equipos, A.7.9 Seguridad de los bienes fuera de las instalaciones, A.7.14 Eliminación o reutilización segura del equipo, A.7.7 Escritorio limpio y Pantalla limpia

Información Documentada revisada
Check List de Instalaciones Formato FOR-SIS-006 versión 04 con fecha Septiembre del 2019, FOR-SIS-008 Revisión de Seguridad de Instalaciones con fecha de Agosto del 2024, FOR-SIS-001 Conformidad de Mantenimiento Preventivo versión

08 con fecha de Enero 2022, Formato Conformidad de Mantenimiento Preventivo FOR-SIS-001 versión 08 con fecha de Enero del 2022, POL GSI 001 Políticas generales de seguridad de la información, versión 7, Agosto 2024 ,

Descripción de la Evaluación

A.7.1 Perímetros de seguridad física.

Se muestra el Documento de Check List de Instalaciones Formato FOR-SIS-006 versión 04 con fecha Septiembre del 2019
Se realizan cada 3 meses | Fecha 29 del Junio del 2024

- Existe ruta de evacuación a la vista de los Empleados
  Revisión de los Centros de Carga
  Eléctrica
  No existen filtraciones de agua en el techo
  La iluminación es la adecuada en todas las áreas
  Existe señalización referente a los
  Extintores
  Están recargados los Extintores
  Cuenta con Detectores de Humo funcionando adecuadamente
  Cuenta con un lugar visible y accesible del Árbol de Llamadas
  para caso de Siniestro
  Existe letreros de identificación de
  Áreas de Acceso Restringido
  No se encuentran cables sueltos o algún objeto que obstruya la Ruta de Evacuación

Se muestra la Revisión del Sitio de Neza | Fecha 29 de Junio del 2024
Se muestra la Revisión del Sitio Valle Insurgentes | Fecha 06 de Septiembre del 20224
Se muestra la Revisión del Sitio Toluca | Fecha 11 de Julio del 20224| Responsable : Franco Ramírez Magdalena Pilar

A.7.2 Entrada Física.

Se muestra durante el recorrido que se cuenta :

- Gafetes del personal de la organización: cuando se accesan
- Personal de vigilancia que colabora con el registro de bitácora de visitante y equipo: Se muestran bitácoras de registros
- Solicita identificación al personal visitante
- Revisión de pertenencias de personal externo.
- Se identifica la zona de entrega y carga ubicada en: la entrada de empleados

A.7.3 Aseguramiento de oficinas, habitaciones e instalaciones. | A.7.4 Supervisión de la seguridad física.

Se muestra el formato FOR-SIS-008 Revisión de Seguridad de Instalaciones con fecha de Agosto del 2024
Cuenta con chapas seguras en todas las puertas del lugar
Cuenta con sensores de movimiento
Los protectores de puertas y ventanas no muestran señas de violación
Los vidrios de puertas y ventanas están completos
Prueba de activación de alarma
Revisión de las cámaras de seguridad
Revisión del sistema de grabación
¿Se resguarda video de 30 días anteriores?

Se muestra la revisión del Sitio de Neza | Fecha 29 de Agosto del 2024
Se muestra la revisión del Sitio Valle Insurgentes | Fecha 09 de Septiembre del 20224
Se muestra la revisión del Sitio Toluca | Fecha 17 de Septiembre del 20224| Responsable : Franco Ramírez Magdalena Pilar

A.7.5 Protección contra amenazas físicas y ambientales.
Se valida durante el recorrido que se cuenta con diferente equipos contra amenazas físicas

- Extintores
- Detectores de Humo
- Cámaras CCTV

A.7.6 Trabajar en áreas seguras.
Se valida durante el recorrido que se llevan cabo los siguientes elementos.

- Normas de conducta (no se permite persona con aliento alcohólico, con armas, con gorras y lentes, con vestimenta inapropiada) desde la inducción al persona se da a conocer
- Supervisión de personal visitante especialmente de áreas restringidas y se encuentran señaladas estas áreas
- Los visitantes no pueden tomar grabaciones o video.
- Se valida la disponibilidad de manual de interno de protección civil.
- Registro de eventos en el reporte de diario.

A.7.11 Servicios públicos de apoyo.
La redundancia de luz eléctrica cuenta con conexión a No breaks distintos
A.7.12 Seguridad del cableado.
Se valida durante el recorrido que se lleva acomodo e instalación adecuada del Cableado
Se puede observar la separación del cableado eléctrico, y de telecomunicaciones:

- Se encuentra en canaletas metálicas.
- Se encuentra en buenas condiciones.

A.7.13 Mantenimiento de equipos
Solo se realiza mantenimiento preventivo y correctivo a los equipos de cómputo y servidores –
Programa anual de mantenimiento
Se realizan cada 6 meses

Se muestra evidencia de Mantenimiento Preventivo
FOR-SIS-001 Conformidad de Mantenimiento Preventivo versión 08 con fecha de Enero 2022
Fecha : 20/05/2024
SITIO | TOLUCA
Nombre : María de los Ángeles Aguirre García
Puesto: Supervisor

- Numero De Activo | | No Aplica
  Tipo De Activo | Escritorio
  Número De Serie | Mmlxkam0018380b1664233
  Accesorios Incluidos | | No Aplica
  Numero De Activo| | No Aplica
  Tipo De Activo | | No Aplica
  Número De Serie| | No Aplica
  Accesorios Incluidos || No Aplica
  Numero De Activo | No Aplica
  Tipo De Activo | No Break
  Número De Serie | 2421dvhbc788900361
  Accesorios Incluidos: | No Aplica

Hechos Realizados:

- Limpieza física de Hardware
  Desfragmentación de Discos Duros
  Eliminación de Cookies

Verificación del Estado del Antivirus
Check List de Seguridad
Check List de Licenciamiento

Se revisa el formato de Conformidad y Mantenimiento Preventivo FOR-SIS-001 versión 07 con fecha Noviembre del 2019
Fecha : 22/07/2024
SITIO | Neza
Nombre : Gonzales Velasco Luis Alberto
Puesto: Contador

Oportunidad de Mejora : Revisar que se usen los Formatos Actuales en los Mantenimientos de Equipos en los Diferentes Sitios
Se Muestra el Formato Conformidad de Mantenimiento Preventivo FOR-SIS-001 versión 08 con fecha de Enero del 2022
Fecha : 04/05/2024
SITIO | Valle Insurgentes
Nombre : Mendoza Lara Juan Manuel
Puesto: Supervisor

Se realizan 2 mantenimiento al año con contrato al Proveedor ilaayr
Se muestra Factura del Mantenimiento a Aires Acondicionados
Fecha : 20 de Junio del 2024
Numero de Cotización: J-01148-M
Tipo : Mini Split
Numero de Factura : A-260 | Insurgentes Mantenimiento
Numero de Factura : A-259 | Toluca Mantenimiento
Numero de Factura : A- 303| Neza Mantenimiento

Se revisa evidencia del Mantenimiento a Extintores con el Proveedor : Servidores Extinguidores " REYES"
Se muestra carta Responsiva y Garantía
Por este medio, nos permitimos certificar que los extintores y servicio proporcionados por esta empresa, cumplen con lo estipulado en la Normatividad vigente emitida por la Secretaría del
Trabajo y Prevención Social, y entre otras las siguientes:
NOM-002STPS-2010 CONDICIONES DE SEGURIDAD, PREVENCION Y COMBATE DE INCENDIOS EN LOS CENTROS DE TRABAJO.
NOM.100-STPS-2010 SEGURIDAD, EXTINTORES CONTRA INCENDIO DE POLVO QUIMICO SECO TIPO "ABC", A BASE DE FOSFATO MONOAMONICO, AGENTES LIMPIOS Y CO2.
Con la finalidad de dar el cumplimiento a los lineamientos anteriores mencionados y establecer las condiciones mínimas de seguridad que deben existir para los trabajadores en sus centros de trabajo.

MANTENIMIENTO A EXTINTOR TIPO GRANADA DE 4.5 KG EN CONTENIDO HFC-236 PARA FUEGOS TIPO ABC
RECARGA A EXTINTOR DE 4.5 KG EN CONTENIDO P.Q.S. PARA FUEGOS TIPO ABC
RECARGA A EXTINTOR DE 10 LB EN CONTENIDO CO2 (BIÓXIDO DE CARBONO) PARA FUEGOS
TIPO BC
Se revisa Carta Responsiva y Garantía
Sitio Toluca | Fecha 19 de Julio del 2024
Numero de Factura : 00001000000513071097

Se revisa la Factura de Mantenimiento de Extintores | Fecha 22 de Julio del 2024
Numero de Factura : FAC0000000786 | SITIO : Valle Insurgentes

Se revisa la Factura de Mantenimiento de Extintores | Fecha 29 de Julio del 2024
Numero de Factura : FAC0000000796 | SITIO : Neza | 12 Extintores

Se muestran Dictamen Numero : ICN00241 | Fecha : 25 de Febrero del 2024
A.7.9 Seguridad de los bienes fuera de las instalaciones.| A.7.8 Emplazamiento y protección de equipos
Se identifica el documento POL GSI 001 Políticas generales de seguridad de la información, versión 7, Agosto 2024 En esta organización no está permitido el home office.
A.7.14 Eliminación o reutilización segura del equipo.
Se realiza destrucción de discos duros y equipos de cómputo con proveedor Se reviso en A8 Gestión de activos
A.7.7 Escritorio limpio y Pantalla limpia
El tiempo de bloqueo de los equipos de cómputo 2 minutos 30 segundos
Se identifica el documento POL GSI 001 Políticas generales de seguridad de la información, versión 7, Agosto 2024
Todos los colaboradores hemos adoptado una política de puesto de trabajo despejado de papeles y medios de almacenamiento desmontables y una política de pantalla limpia para los recursos de tratamiento de la información. Toda la información clasificada como de uso interno, restringido y confidencial de acuerdo con lo establecido en el Procedimiento de gestión de activos, clasificación y control de la información PRO GSI 015, es considerada sensible en esta política de pantalla y escritorio limpio.
Puesto de trabajo
Si la persona autorizada no se encuentra en su puesto de trabajo, todos los documentos impresos, como también los soportes de almacenamiento de datos, clasificados como confidencial o restringidos, deben ser retirados del escritorio o de otros lugares para evitar el acceso no autorizado a los mismos.

- Pantalla limpia

Si la persona autorizada tiene la necesidad de ausentarse o abandonar su puesto de trabajo, deberá quitar toda la información sensible de la pantalla, y bloquear el acceso para los cuales tiene autorización.

Si la persona autorizada ene la necesidad de ausentarse o abandonar su puesto de trabajo, deberá quitar toda la información sensible de la pantalla, y bloquear el acceso para los cuales tiene autorización (método abreviado en el teclado Windows + L). Independientemente de lo anterior, en el caso de una ausencia corta, la política de pantalla limpia se activa bloqueando la sesión de manera automática:

El tiempo para que se active el screen saver: 2 minutos

Resultado de la Evaluación:	Conforme
Auditor:	Karina Alonso Sánchez

Proceso / Servicio:	**ENTREVISTAS CON EL PERSONAL Y REVISIÓN DE EQUIPOS**
Departamento, Área o Unidad de Negocio:	Operaciones
Personal Relacionado:	Adriana Munive Montes | Encargada de Banco Miguel Ángel López Reyes | Abogado Iris Itzel Plata Azotea | Asesor Telefónico
Elementos normativos relacionados	

6.2 Alcanzando los objetivos y planes de seguridad de la información, 7.3 Concientización, 7.4 Comunicación, 6.2 Objetivos y planificación para lograrlos, 5.2 Política, A.6.3 Sensibilización, educación y formación en materia de seguridad de la información, A.5.10 Uso aceptable de la información y otros activos asociados, A.8.18 Uso de programas de utilidad privilegiados, A.8.19 Instalación de software en sistemas operativos, A.8.20 Seguridad de redes, A.8.17 Sincronización de reloj, A.8.7 Protección contra malware, A.5.36 Cumplimiento de políticas, reglas y estándares de seguridad de la información, A.6.8 Informes de eventos de seguridad de la información, 7.7 Escritorio limpio y pantalla limpia, 7.8 Emplazamiento y protección de equipos

Información Documentada revisada

ENTREVISTA CON EL PERSONAL

Descripción de la Evaluación

ENTREVISTA CON EL PERSONAL 1
Nombre: Adriana Munive Montes | SITIO NEZA
Cargo: Encargada de Banco
Área | Departamento: Investigación de Crédito
Tiempo en la organización: 12 años
Actividades: Atención a clientes bancarios , atención de Solicitudes

INFORMES DE EVENTOS DE SEGURIDAD DE LA INFORMACIÓN
Menciona que se cuenta con brigadas para la atención de eventos que puedan suceder , la colaboradora menciona los procedimientos para ponerse a salvo ante una situación de sismo, Menciona el Protocolo de aviso de incidentes en casos de ataques cibernético
CAPACITACIÓN, CONCIENTIZACIÓN
Menciona que ha recibido capacitación sobre temas de seguridad , y conoce los boletines de seguridad que se difunden en la organización
POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN
La Colaboradora ubica la política de Seguridad de la Información
OBJETIVOS DE SEGURIDAD DE LA INFORMACIÓN
La Colaboradora conoce los objetivos de seguridad de la Organización y los menciona
CONOCIMIENTO Y CONTROLES DE CONTROLES DE SEGURIDAD
Conoce del Procedimiento de Auditoria y menciona las Normas Certificadas en la Organización
ISO/IEC: 27001 : 2022
REVISIÓN DE EQUIPOS
Se revisó el equipo de cómputo y se validó lo siguiente:

PROTECCIÓN CONTRA MALWARE
Herramienta: SENTINEL ONE
SINCRONIZACIÓN DE RELOJ, USO DE PROGRAMAS DE UTILIDAD PRIVILEGIADOS
Se valida la restricción para evitar la modificación de fecha y hora del equipo.
EQUIPO DE USUARIO DESATENDIDO, USO DE PRIVILEGIOS DE LOS PROGRAMAS DE UTILIDADES
Se valida la activación del protector de pantalla al 2 min, se restringe su modificación, funcionalidad gestionada por el administrador
INSTALACIÓN DE SOFTWARE EN SISTEMAS OPERATIVOS
Se valida que el software es adecuado a sus funciones y licenciado
Se restringe la instalación de software
Presentan carta Responsiva de uso adecuado de activos de información
SEGURIDAD DE REDES | USO ACEPTABLE DE LA INFORMACIÓN Y OTROS ACTIVOS ASOCIADOS
Se identifica que el equipo revisado del colaborador se encuentra conectado en la red corporativa :CIASC.MX

ESCRITORIO LIMPIO Y PANTALLA LIMPIA
Se valida el cumplimiento de escritorio limpio de la computadora y almacenamiento de documentos relacionado con las actividades laborales.
EMPLAZAMIENTO Y PROTECCIÓN DE EQUIPOS
Durante el recorrido virtual y revisión de equipos, se validó que los equipos críticos se encuentran condiciones adecuadas para su operación.
USO DE VPN
Se valida conexión de VPN. Herramienta: No se utiliza ya que se cuenta con equipo PC y siempre se encuentra en las Instalaciones

ENTREVISTA CON EL PERSONAL 2 SITIO INSRUGENTES
Nombre: Miguel Angel López Reyes
Cargo: Abogado
Área | Departamento: Jurídico
Tiempo en la organización: 8 Meses
Actividades: Se reciben cuentas que se demandan , ingresar al Juzgado los casos pertinentes , se realizan los escritos de todo el proceso de demanda
INFORMES DE EVENTOS DE SEGURIDAD DE LA INFORMACIÓN
El colaborador Conocer los Protocolos de Seguridad, y ha realizado simulacros en la organización.
CAPACITACIÓN, CONCIENTIZACIÓN
El colaborador menciona haber recibido capacitación de la Seguridad de la Información , recibió su capacitación en el mes de Agosto 2024 , recibe capacitación en el aplicativo de univer
POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN
El colaborador menciona controles de seguridad de la información pertenecientes a la Política y explica la forma en las que lo lleva día a día.
OBJETIVOS DE SEGURIDAD DE LA INFORMACIÓN
No Conoce los Objetivos de Seguridad de la Información y no es muy conciso en lo que menciona
CONOCIMIENTO Y CONTROLES DE CONTROLES DE SEGURIDAD
Desconoce las Normas en las que se encuentra la Empresa Certificada.
Observación: Durante las entrevista al Personal del Sitio : Insurgentes se detecta la necesidad de Reforzar la Concientización de los Colaboradores en la Sede de Valle-Insurgentes ya

REVISIÓN DE EQUIPOS
Se revisó el equipo de cómputo y se validó lo siguiente:
PROTECCIÓN CONTRA MALWARE
Herramienta: SENTINEL ONE
SINCRONIZACIÓN DE RELOJ, USO DE PROGRAMAS DE UTILIDAD PRIVILEGIADOS
Se valida la restricción para evitar la modificación de fecha y hora del equipo.
EQUIPO DE USUARIO DESATENDIDO, USO DE PRIVILEGIOS DE LOS PROGRAMAS DE UTILIDADES
Se valida la activación del protector de pantalla al 1 min, se restringe su modificación, funcionalidad gestionada por el administrador
INSTALACIÓN DE SOFTWARE EN SISTEMAS OPERATIVOS
Se valida que el software es adecuado a sus funciones y licenciado
Se restringe la instalación de software
Presentan carta Responsiva de uso adecuado de activos de información
SEGURIDAD DE REDES | USO ACEPTABLE DE LA INFORMACIÓN Y OTROS ACTIVOS ASOCIADOS
Se identifica que el equipo revisado del colaborador se encuentra conectado en la red corporativa :
ESCRITORIO LIMPIO Y PANTALLA LIMPIA

Se valida el cumplimiento de escritorio limpio de la computadora y almacenamiento de documentos relacionado con las actividades laborales.

EMPLAZAMIENTO Y PROTECCIÓN DE EQUIPOS

Durante el recorrido virtual y revisión de equipos, se validó que los equipos críticos se encuentran condiciones adecuadas para su operación.

USO DE VPN

Se valida conexión de VPN. Herramienta: No se utiliza la VPN ya que se cuenta con equipo de PC con monitor y no salen de las Instalaciones.

ENTREVISTA CON EL PERSONAL 3 SITIO TOLUCA

Nombre: Iris Itzel Plata Azotea
Cargo: Asesor Telefónico
Área | Departamento: Recuperación de Cartera
Tiempo en la organización: 2 años
Actividades: Brindar asesoría mediante el teléfono

INFORMES DE EVENTOS DE SEGURIDAD DE LA INFORMACIÓN

Menciona la Capacitación , Recibió capacitación sobre las a

CAPACITACIÓN, CONCIENTIZACIÓN

Menciona Haber recibido capacitaciones en volúmenes de voz , y la atención a clientes

POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

La Colaboradora conoce la Política de Seguridad de la Información

OBJETIVOS DE SEGURIDAD DE LA INFORMACIÓN

Conoce los Objetivos de Seguridad de la información y los menciona

CONOCIMIENTO Y CONTROLES DE CONTROLES DE SEGURIDAD

REVISIÓN DE EQUIPOS

Se revisó el equipo de cómputo y se validó lo siguiente:

PROTECCIÓN CONTRA MALWARE

Herramienta: SENTINEL ONE

SINCRONIZACIÓN DE RELOJ, USO DE PROGRAMAS DE UTILIDAD PRIVILEGIADOS

Se valida la restricción para evitar la modificación de fecha y hora del equipo.

EQUIPO DE USUARIO DESATENDIDO, USO DE PRIVILEGIOS DE LOS PROGRAMAS DE UTILIDADES

Se valida la activación del protector de pantalla al 2 min, se restringe su modificación, funcionalidad gestionada por el administrador

INSTALACIÓN DE SOFTWARE EN SISTEMAS OPERATIVOS

Se valida que el software es adecuado a sus funciones y licenciado
Se restringe la instalación de software
Presentan carta Responsiva de uso adecuado de activos de información

SEGURIDAD DE REDES | USO ACEPTABLE DE LA INFORMACIÓN Y OTROS ACTIVOS ASOCIADOS

Se identifica que el equipo revisado del colaborador se encuentra conectado en la red corporativa :ciasc.mx

ESCRITORIO LIMPIO Y PANTALLA LIMPIA

Se valida el cumplimiento de escritorio limpio de la computadora y almacenamiento de documentos relacionado con las actividades laborales.

EMPLAZAMIENTO Y PROTECCIÓN DE EQUIPOS

Durante el recorrido virtual y revisión de equipos, se validó que los equipos críticos se encuentran condiciones adecuadas para su operación.

USO DE VPN

Se valida conexión de VPN. Herramienta: No se utiliza la VPN ya que se cuenta con equipo de PC con monitor y no salen de las Instalaciones.

Resultado de la Evaluación:	Conforme
Auditor:	Karina Alonso Sánchez

Proceso / Servicio:	**RECORRIDO VIRTUAL**
Departamento, Área o Unidad de Negocio:	Instalación | NEZA
Personal Relacionado:	Ana Laura Hernández Montaño-Coordinador de Sistemas. Rafael Fernando Mendoza Loza-Coordinador de Sistemas

Elementos normativos relacionados

A.7.1 Perímetros de seguridad física, A.7.2 Entrada Física, A.7.3 Aseguramiento de oficinas, habitaciones e instalaciones., A.7.4 Supervisión de la seguridad física, A.7.5 Protección contra amenazas físicas y ambientales, A.7.6 Trabajar en áreas seguras, A.7.8 Emplazamiento y protección de equipos, A.7.11 Servicios públicos de apoyo, A.7.12 Seguridad del cableado, A.7.13 Mantenimiento de equipos, A.7.9 Seguridad de los bienes fuera de las instalaciones, A.7.14 Eliminación o reutilización segura del equipo, A.8.1 Dispositivos de punto final de usuario, A.7.7 Escritorio limpio y Pantalla limpia, A.5.5 Contacto con las autoridades, A.8.14 Redundancia de las instalaciones de procesamiento de información

Información Documentada revisada

Recorrido Virtual: Sede: Lago Xochimilco No. 283, Ampliación General Vicente Villada, Nezahualcóyotl, C.P. 57760, Edo. De México.

Descripción de la Evaluación

RECORRIDO VIRTUAL

Se realiza un recorrido virtual con apoyo de un dispositivo móvil y se valida:

PERÍMETROS DE SEGURIDAD FÍSICA

- Áreas públicas
- Área reservada
- Área restringida: Site de comunicaciones en buen estado

ASEGURAMIENTO DE OFICINAS, HABITACIONES E INSTALACIONES

- Puertas cerradas
- Control de llaves
- Directorio de teléfonos de emergencia: Localizado en Documentos

SUPERVISIÓN DE LA SEGURIDAD FÍSICA

- Cámaras de emergencia: en todas las Plantas
- Lámparas de emergencia

ENTRADA FÍSICA

- Gafetes del personal de la organización: cuando se accesan
- Personal de vigilancia que colabora con el registro de bitácora de visitante y equipo: Se muestran bitácoras de registros
- Solicita identificación al personal visitante

- Revisión de pertenencias de personal externo.
- Se identifica la zona de entrega y carga ubicada en: la entrada de empleados
- Se valida la identificación de esta zona en el recorrido

TRABAJAR EN ÁREAS SEGURAS

- Normas de conducta (no se permite persona con aliento alcohólico, con armas, con gorras y lentes, con vestimenta inapropiada) desde la inducción al persona se la a conocer
- Supervisión de personal visitante especialmente de áreas restringidas y se encuentran señaladas estas áreas
- Los visitantes no pueden tomar grabaciones o video.
- Se valida la disponibilidad de manual de interno de protección civil.
- Registro de eventos en el reporte de diario.

RETIRO DE ACTIVOS

- Revisión de pertenencias de personal externo.
- Revisión de equipos al ingreso y salida.

PROTECCIÓN CONTRA AMENAZAS FÍSICAS Y AMBIENTALES

- Extintor CO2 – Fecha de servicio: Julio 2024
- Señalética de Ruta de evacuación en todos los pisos
- Señalética del equipo contra amenazas externas y ambientales
- Aires acondicionados, Mini Split : 4

SEGURIDAD DEL CABLEADO

- Se puede observar la separación del cableado eléctrico, y de telecomunicaciones:
- Se encuentra en canaletas metálicas.
- Se encuentra en buenas condiciones.

SERVICIOS PÚBLICOS DE APOYO

- UPS con baterías.

MANTENIMIENTO DE EQUIPOS | CUMPLIMIENTO DE POLÍTICAS, REGLAS Y ESTÁNDARES DE SEGURIDAD DE LA INFORMACIÓN

- Limpieza físico preventivo, limpieza lógica, revisión de activación de antivirus, actualización de SO, desfragmentación del disco, revisión de software autorizado

Resultado de la Evaluación:	Conforme
Auditor:	Karina Alonso Sanchez

Proceso / Servicio:	**CONTROLES ORGANIZATIVOS |CONTROLES FÍSICO | CONTROLES TECNOLÓGICOS**
Departamento, Área o Unidad de Negocio:	Sistemas de Gestión
Personal Relacionado:	Salvador Santiago Araujo- Gerente Administrativa Ana Laura Hernández Montaño-Coordinador de Sistemas. Rafael Fernando Mendoza Loza-Coordinador de Sistemas Irais Dafne Mendoza Sánchez-Director

	General Adjunta

Elementos normativos relacionados

A.5.9 Inventario de información y otros activos asociados, A.5.10 Uso aceptable de la información y otros activos asociados, A.5.11 Devolución de activos, A.5.12 Clasificación de la información, A.5.13 Etiquetado de la información, A.7.10 Medios de almacenamiento, A.8.10 Eliminación de información

Información Documentada revisada

Gestión de Activos y Clasificación y Control de la Información PRO-GSI-015 Versión 10 con fecha de Enero 2024, Política Generales de Seguridad de la Información Versión 07 con fecha de Agosto 2024 .

Descripción de la Evaluación

A.5.9 INVENTARIO DE INFORMACIÓN Y OTROS ACTIVOS ASOCIADOS

Se muestra el Documento de Gestión de Activos y Clasificación y Control de la Información PRO-GSI-015 Versión 10 con fecha de Enero 2024

1. DESARROLLO DE INVENTARIO DE ACTIVOS TECNOLOGICOS Y SOFTWARE
Todos los activos de la Organización están identificados, clasificados y asignados a un responsable, y han sido incluidos en un Inventario y clasificación de activos LIS GSI 023, en este inventario se anexa la fecha de asignación, así como el plan de renovación para cada activo de información de la organización. (Ver lineamientos en el apartado 6. Clasificación de activos de la información de
este documento).
El gerente administrativo será el encargado de darle una vigencia operativa a cada activo de la organización a fin de tener equipos y software eficaces, esta vigencia se declarará dentro del Inventario y clasificación de activos LIS GSI 023, cada que se venza una vigencia de algún equipo este se tendrá que retirar de la operación y será remplazado por un equipo nuevo.

INVENTARIO DE HARDWARE
1. Inventario Completo.
Esta opción es válida para cuando se va a hacer un inventario inicial o cuando se quiere hacer una validación del inventario actual.
2 Planificación del inventario.
3.Gerente Administrativo o el Coordinador de Sistemas TI realiza la planeación de las actividades a desarrollar, tomando como base los activos disponibles para su realización, identifica, correlaciona y organiza los planes del inventario dentro de la organización.
Coordinación del Inventario.
4.coordinador de Sistemas Ti organiza al equipo de trabajo para la ejecución de las actividades de inventario, suministrándoles las
pautas de desarrollo y de control del mismo.
5.Desarrollo de la Actividad
Auditar de sistemas obtener la información básica y necesaria para cumplir con el objetivo del inventario, en la cual encontramos:
A)Información del responsable del equipo (RRHH)
B)Activo
Tipo de Activo
Marca
Modelo

Se muestra el Documento LIS-GSI-023 Inventario y Clasificación de Activos Versión 03 con fecha de Septiembre 2024

- Extensión

- Numero de Empleado
- Responsable
- Departamento
- Puesto
- Activo
- Marca
- Número de Serie
- Accesorio
- Procesador
- IPV4
- MAC
- RAM
- Almacenamiento
- Capacidad
- Clasificación
- Nombre de la Maquina
- Sistema Operativo
- Office
- Antivirus
- Navegador
- Compresor de Archivos

A.5.10 USO ACEPTABLE DE LA INFORMACIÓN Y OTROS ACTIVOS ASOCIADOS

Política Generales de Seguridad de la Información Versión 07 con fecha de Agosto 2024

Uso Aceptable

En todo momento se deben acatar las medidas de seguridad descritas por el área de sistemas para evitar:
Descargar archivos, imágenes o vídeos que no sean relacionados con las actividades de la empresa.
Visitas a páginas web no relacionados con nuestras actividades.
Instalación de software no autorización por el área de sistemas (ninguna computadora de la empresa tiene Privilegios para descargar e instalar software).
Descargar códigos de programa de soportes externos.
Instalar o utilizar dispositivos periféricos como módems, tarjetas de memoria u otros dispositivos para almacenamiento y lectura de datos (todas las computadoras de la empresa tienen restricciones en la trasferencia de datos por puertos USB, SD, PCI).7
Utilidades capaces de invalidar los controles de los sistemas y las aplicaciones.
Nota: En caso de que se necesite realizar alguna de las acciones anteriores, en donde se requiera credenciales de administrador, se deberá dar aviso al área de sistemas para la gestión correspondiente, ya que es la única drea autorizada para manipular los sistemas informáticos de la empresa.

Se muestra Carta responsiva de equipos y accesos FOR GSI 031 versión 9 de fecha Octubre 2020
Empleado : Ibarra Jimenez Brian Kaled

- Aviso de rescisión
- Promesa de confidencialidad
- 2 años de confidencialidad

- Carta Compromiso de Accesos
- Carta Responsiva de Excepciones FOR-GSI-051 Versión 1 con fecha de Julio 2023

A.5.11 DEVOLUCIÓN DE ACTIVOS

7. DEVOLUCIÓN DE ACTIVOS
Una vez que el propietario o usuario se dé de baja de la Organización (de acuerdo al Mapa de proceso de Recursos Humanos MAP REH 001) deberá reasignarse el activo como responsabilidad a otra persona y hacer las modificaciones necesarias en el Inventario y Clasificación de activos LIS GSI 023 de forma inmediata

Baja del Colaborador

Se muestra una Baja
Puesto: Programador
Entrevista de Salida FOR-REH-013 Versión 3 con fecha Enero 2019
DCS Delta Corporate Servicies S.A DE C.V
Fecha de Salida : 20 de Septiembre del 2024
Carta Escrita a mano
Carta : Aviso de Rescisión de la Relación Laboral

Se muestra correo de Solicitud de Finiquito 9510 Ibarra Jimenez Brian Kaled
Fecha de Envió : 23 de Septiembre del 2024

Carta responsiva de equipos y accesos FOR GSI 031 versión 9 de fecha Octubre 2020
Empleado : Ibarra Jimenez Brian Kaled
- Aviso de rescisión
- Promesa de confidencialidad
- 2 años de confidencialidad
- Carta Compromiso de Accesos
- Carta Responsiva de Excepciones FOR-GSI-051 Versión 1 con fecha de Julio 2023
-

Se envía correo electrónico donde se da aviso de la baja del colaborador para el retiro de sus accesos y baja del equipo, utilizando la carta responsiva que previamente firmo en la asignación

A.5.12 CLASIFICACIÓN DE LA INFORMACIÓN | A.5.13 ETIQUETADO DE LA INFORMACIÓN

8. Etiquetado de la Información

ETIQUETADO DE LA INFORMACIÓN
Por funcionalidad para la Organización se declara el tipo de información en todos los mapas de proceso para que el personal tenga conocimiento de la clasificación de la información que maneja y las precauciones que debe tener en todo momento. Declaramos que solo cuando se archiva la información físicamente es cuando será visible el sello de nivel de confidencialidad.

Información | Descripción | Clasificación | Quien tiene acceso | Disposición Final

Los Documentos de Carácter Electrónico | RESTRINGIDO

Base de Datos | RESTRINGIDO

Documentos en Formato de Papel | RESTRINGIDO .

6. Clasificación de Activos de la Información

Para llevar a cabo la clasificación de los activos de la información, dentro del Inventario y clasificación de activos LIS GSI 023 se cuenta con las siguientes indicaciones para su llenado, clasificación, etiquetado y manipulación:
a. No. de serie: Indica el número de serie dado por el fabricante al activo. No aplica para todos los activos.
b. Dirección IP: La dirección IP fija asignado al activo. No aplica para todos los activos.
Identificador: En este campo se debe incluir el código asignado al activo por la Organización (nuevo o preexistente).
Este atributo debe permitir identificar de forma única al activo
d. Nombre del activo: Nombre de identificación del activo de información, en este campo debe incluirse todos los activos de información identificados para la etapa, independiente de su medio de soporte y sus características.
•. Tipo de activo: Este atributo permite establecer la naturaleza del activo, calificándolo según los siguientes valores:
a Equipo: dispositivos que realizan o apoyan la realización de un proceso y contienen información.
b Componente: dispositivo, aparato, o elemento que apoya la realización de los procesos.
1. Usuario del activo: Nombre del usuario autorizado para utilizar el activo. No aplica para todos los activos.
a Descripción del uso del activo: Breve descripción sobre el uso o las funciones que el activo desempeña.
b Propietario del activo: Nombre del propietario autorizado para tomar decisiones respecto al activo. Se puede tratar de una persona concreta o de un área. Esto no implica necesariamente derecho de propiedad sobre el activo.
A Custodio del activo: Nombre del responsable para el resguardo del activo. Se puede tratar de una persona concreta
B o área.
C Información de contacto del custodio del activo: Datos de ubicación o área y extensión o teléfono del custodio del activo

Ubicación: Corresponde al lugar físico o lógico donde se encuentra el activo mientras es utilizado en el proceso, esta descripción debe ser lo suficientemente detallada como para determinar a partir de esta información las condiciones de seguridad física en las que se encuentra el activo.
Estatus del activo: Puede ser desarrollo, producción, en desuso o baja.
m. Clasificación: De acuerdo a lo comentado en punto 5. Criticidad de los Activos de la información.

A.7.10 MEDIOS DE ALMACENAMIENTO

Se muestra en el Documento Políticas Generales de Seguridad de la Información PQL-GSI-001

No se permite el uso de dispositivos USB

Instalar o utilizar dispositivos periféricos como módems, tarjetas de memoria u otros dispositivos para almacenamiento y lectura de datos (todas las computadoras de la empresa tienen restricciones en la
trasferencia de datos por puertos USB, SD, PCI).7

A.8.10 ELIMINACIÓN DE INFORMACIÓN

Se muestra el Documento de Respaldos y Eliminación de Información PRO-GSI-032 Versión 11 con fecha de Septiembre del 2024

3.Eliminacion

Eliminación y/o destrucción de información contenida soportes y equipos móviles
Todos los datos y software con licencia almacenado en todos los equipos móviles (por ej., laptops, teléfonos móviles, etc.) deben ser borrados, antes de ser destruidos o reutilizados.

Eliminación y/o Destrucción en equipos y PC y Servidores

Para la eliminación, el área de sistemas es el responsable de verificar y borrar datos de los equipos y servidores.
Los datos deben ser borrados, teniendo en cuenta la clasificación de la información del procedimiento de gestión de activos, clasificación y control de la información PRO GSI 015 y siendo obligatoria cuando el cliente lo requiera.
Para la destrucción física de equipos pe y servidores se mandará a destrucción con un proveedor externo solicitándole el certificado de destrucción

Se muestra Factura del Proveedor E-WASSTE SYSTEMS
Folio :11807
Fecha y Hora: 14 de Junio del 2024

Se muestra el Destrucción de Información Documentada FOR-CAL-007
Fecha de Destrucción : 12 de Septiembre del 2024
Responsable de Área: Héctor Ramírez
Eliminación: Física
Descripción del Contenido | Periodo que Corresponde la Información | Comentarios
Caja 1
◦ Expedientes de acreditados
Caja 2
◦ Expedientes de acreditados
Caja 3
◦ Expedientes de acreditados
Caja 4
◦ Expedientes de acreditados

Se muestra Documento Destrucción de Información Documentada FOR-CAL-007
Fecha de Destrucción: 16/02/2023
Responsable de Área: Rafael Mendoza Lozada
Descripción del Contenido | Periodo que Corresponde la Información | Comentarios
Información BBVA | 2022-2023 | El equipo presenta fallas y se procede al cambio físico y la destrucción del Reemplazado

Se muestra Certificado de recolección , Destrucción y Traslado de Especialización , Electrónicos

Resultado de la Evaluación:	Conforme
Auditor:	Karina Alonso Sánchez

Proceso / Servicio:	**CONTROLES ORGANIZATIVOS**
Departamento, Área o Unidad de Negocio:	Sistemas de Gestión
Personal Relacionado:	Salvador Santiago Araujo- Gerente Administrativa Ana Laura Hernández Montaño-Coordinador de Sistemas. Rafael Fernando Mendoza Loza-Coordinador de Sistemas Irais Dafne Mendoza Sánchez-Director General Adjunta
Elementos normativos relacionados	

A.5.31 Requisitos legales, reglamentarios y contractuales, A.5.32 Derechos de propiedad intelectual, A.5.33 Protección de registros, A.5.34 Privacidad y protección de la PII, A.5.35 Revisión independiente de la seguridad de la información, A.5.36 Cumplimiento de políticas, reglas y estándares de seguridad de la información

Información Documentada revisada

Documento de Cumplimiento Legal PRO-GSI-029 versión 9 con fecha de Enero del 2024,

Descripción de la Evaluación

A.5.31 REQUISITOS LEGALES, REGLAMENTARIOS Y CONTRACTUALES
Se menciona por la organización que diario se lleva a cabo la Revisión del Diario Oficial
Lista de Requisitos legales.

Se muestra el Documento de Cumplimiento Legal PRO-GSI-029 versión 9 con fecha de Enero del 2024
De acuerdo a los requisitos legales, regulatorios, contractuales y del negocio, se establecen controles para la protección de los registros, y que se encuentran documentados en los siguientes documentos: Políticas generales de seguridad de la Información POL GSI 001, Gestión de activos, clasificación y control de la Información PRO GSI 015, Control de accesos PRO GSI 016, Respaldo y eliminación de información PRO GSI 032 y Control de información documentada PRO CAL 001.

Legales y Reglamentarios:
Ley Federal de Protección de Datos Personales
Leyes Fiscales
Leyes Anticorrupción
Ley Federal de Protección al Consumidor

Regulatorios :
Norma UNE EN ISO/IEC 27001

De la Organización

Se realiza la Revisión de estos requisitos de manera anual

Se muestra Tabla de Requisitos Legales y Contractuales
Información | Legales | Contractuales | Regulaciones y otros
Expedientes Judiciales para Cobranza Especializada |
> Ley de Infonavit.
> Reglamento de la Infonavit.
> Código de ética del Infonavit.
> Código de comercio.
> Código Civil del Estado de México.
> Código Civil de la CDMX.
>Código de procedimientos civiles par
CDMX.
> Ley General de Sociedades
Mercantiles.
> Código de procedimientos civiles del
Estado de México.
> Ley federal de protección al consumidor.

Contractuales :

Contrato de Prestaciones de Servicio con Infonavit

Regulatorios y otros
- Código de Ética
- Políticas
- Procedimiento y manuales de la Organización Aplicables

Bases de Datos deudores y acreditados para la Recuperación de Cartera
> Acuerdo A/002/2015 de la
>Procuraduría Federal del Consumidor
>Disposiciones Generales en Materia de Despachos de Cobranza".
> Ley Federal de Protección de Datos Personales en Posesión de
Particulares.

Expedientes de Personal y RH
> Ley Federal de Protección de Datos Personales en Posesión de
Particulares.
>Ley Federal del Trabajo

Contratos con Clientes: Código Civil

A.5.32 DERECHOS DE PROPIEDAD INTELECTUAL
Se muestra Documento de Cumplimiento Legal PRO-GSI-029 versión 9 con fecha de Enero del 2024

Generales
Se declara con respecto a los DPI, que estos esencialmente se limitan a las licencias para el uso del software (BONSAIF, PRESENCE, ERP, SICOB. OPTI-RISKS y WINDOWS) con las siguientes consideraciones.
a) BONSAIF y PRESENCE: Licencias adquiridas e instaladas de acuerdo con lo establecido con el proveedor.
b) SICOB, OPTI-RISKS, ERP: Sistemas desarrollados para la Organización y para su uso exclusivo.
c) BLUEMESSAGING: Se realiza un pago mensual para el derecho de uso de las licencias adquiridas.
d)MICROSOFT WINDOWS / OFFICE: Se cuenta con una suscripción Microsoft.Action Pack Suscripción como parte de Microsoft.
e)El área de Sistemas supervisa el uso de licencias y cumplimiento con los derechos de autor de toda aplicación que es utilizada en los equipos de la Organización, incluidos en el alcance del SGS.

Se muestra Factura de COMPUEVOLUCION
Serie y Folio : CE-22981

Microsoft 385 Business Basic
Clave Unidad | Concepto
Fecha: 1 Septiembre del 2024
87| Office 365 69
87| Exchange Online (Pian 1)
87| Microsoft 365 Business Standard
87| Exchange Online (Plan 2)
87| Power BI Pro
87| Planner Plan 1
87| Office 385 EG

A.5.33 PROTECCIÓN DE REGISTROS
*De acuerdo con el Capítulo 7.5 Información documentada, se valida este punto de control de manera documental.
* De acuerdo con el Capítulo 7.5 Información documentada, se valida este punto de control

A.5.34 PRIVACIDAD Y PROTECCIÓN DE INFORMACIÓN DE IDENTIFICACIÓN PERSONAL
Se muestra el Documento de Cumplimiento Legal PRO-GSI-029 versión 9 con fecha de Enero del 2024.
Protección y privacidad de la información

Las bases de datos que contienen información de los datos personales de terceros están protegidas a lo largo de su proceso y de manipulación de acuerdo a los requerimientos legales indicados en La Ley Federal de Protección de Datos Personales en Posesión de los Particulares.
Se cuenta con Aviso de privacidad, Derechos ARCO y tratamiento de datos, disponible en la página web de la Organización para su consulta. Asimismo, se tienen definidos procedimientos para el tratamiento de los datos personales de terceros, así como responsable de su manejo.

Se muestra el Aviso de Privacidad en la Pagina : http://www.ciasc.mx/aviso-de-privacidad/

AVISO DE PRIVACIDAD relacionado con los datos personales, recabados por CONSULTORES E INVESTIGADORES EN ADMINISTRACIÓN, S.C.
CONSULTORES E INVESTIGADORES EN ADMINISTRACIÓN, S.C. es una empresa comprometida y respetuosa de los derechos sobre los datos personales de las personas físicas, reconocidos en el artículo 16 fracción II de la Constitución Política de los Estados Unidos Mexicanos, así como de las disposiciones de la ley federal de protección de datos personales en posesión de los particulares, por lo anterior, pone a su disposición el presente aviso de privacidad, en aras de que el titular de los datos personales, se encuentre facultado a ejercitar su derecho a la autodeterminación informativa.
Este aviso de privacidad se pone a disposición de los titulares en la página de internet cuyo nombre de dominio es: www.ciasc.mx en adelante denominada como la página de internet de CONSULTORES E INVESTIGADORES EN ADMINISTRACIÓN, S.C.

DERECHOS ARCO:
Respecto a sus datos personales recabados y referidos en los inciso a), b), c) y d) del apartado denominado tipo de información que recaba, usted podrá ejercer los derechos de Acceso, Rectificación, Cancelación y Oposición (Derechos ARCO), por documento escrito o vía electrónica dirigido al encargado para el ejercicio del Derecho de ARCO, referido en este aviso de privacidad de conformidad al artículo tercero y cuarto de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. Para que se procese su petición, ésta deberá incluir todos y cada uno de los requisitos previstos en los artículos 89 y 90 del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, así como el Artículo 29 de la misma Ley, que a saber son los siguientes:
«…Artículo 29.- La solicitud de acceso, rectificación, cancelación u oposición deberá contener y acompañar lo siguiente:
I.- El nombre del titular y domicilio u otro medio para comunicarle la respuesta a su solicitud;
II.- Los documentos que acrediten la identidad o, en su caso, la representación legal del titular;
III.- La descripción clara y precisa de los datos personales respecto de los que se busca ejercer alguno de los derechos antes mencionados, y
IV.- Cualquier otro elemento o documento que facilite la localización de los datos personales…»
La única persona facultada para ejercer el derecho de ARCO es el Titular de los Datos Personales, quien deberá ejercerlo ante, el responsable del tratamiento de datos personales y si no obtiene respuesta satisfactoria, podrá acudir ante el INAI, a presentar su queja, de conformidad con Ley Federal de Protección de Datos Personales en Posesión de los Particulares.

ENCARGADO PARA EL EJERCICIO DEL DERECHO DE ARCO:

El área encargada para el ejercicio del Derecho de ARCO será el Departamento Jurídico de CONSULTORES E INVESTIGADORES EN ADMINISTRACIÓN, S.C., el cual se ubica en Insurgentes Sur No. 686 Despacho 905, Col. Del Valle, C.P. 03100, Del. Benito Juárez, Ciudad de México, y puede recibir solicitudes de derechos ARCO en la siguiente dirección electrónica: privacidad@ciasc.mx

Se muestra los Aviso de Privacidad entregados a los Colaboradores:
Se muestra 3 Expedientes 1 por cada Sitio

- Araceli Bautista | Abogado | VALLE
- Jesús Chavarrieta Raquel Magdalena : Asesor Telefónico | TOLUCA
- Suarez Martínez Christian Alejandro : Auxiliar Administrativo | NEZA

Se muestra Contrato con el Cliente : Infonavit con fecha del 08 de Diciembre del 2023
VIGÉSIMA QUINTA. - SEGURIDAD DE LA INFORMACIÓN.
"EL PROVEEDOR" se compromete a resguardar la información que le sea proporcionada o que sea generada como consecuencia del cumplimiento del objeto del presente contrato, de acuerdo con las disposiciones en materia de Seguridad de la Información del Infonavit señaladas en las "ESPECIFICACIONES TÉCNICAS", contenidas en las "BASES DE LICITACIÓN" y, en lo aplicable, lo previsto en las Políticas Institucionales para Seguridad de la Información del Infonavit (ANEXO B). En este sentido, los Responsables de Supervisión y Ejecución deberán verificar el cumplimiento de las obligaciones relacionadas con la seguridad de la información.
"EL PROVEEDOR" se obliga a celebrar con "EL INFONAVIT" acuerdos para la transferencia de información y cadena de custodia, a efecto de evitar pérdidas de información, en términos de la Política de Gestión de Activos del Infonavit.

Se muestra contrato con el Cliente Banamex | Con fecha de 12 de Julio del 2024

A.5.35 REVISIÓN INDEPENDIENTE DE LA SEGURIDAD DE LA INFORMACIÓN
*De acuerdo con el Capítulo Evaluación del desempeño “9.3 Revisión por la dirección”, se valida este punto del control de manera documental.
*De acuerdo con el Capítulo Evaluación del desempeño “9.3 Revisión por la dirección”, se valida este punto del control.

A.5.36 CUMPLIMIENTO DE POLÍTICAS, REGLAS Y ESTÁNDARES DE SEGURIDAD DE LA INFORMACIÓN
*De acuerdo con el Capítulo Evaluación del desempeño Evaluación del Desempeño “9.2 Auditoría Interna” y Controles Tecnológicos “A.8.8 Gestión de vulnerabilidades técnicas”, se valida este punto del control de manera documental.
*De acuerdo con el Capítulo Evaluación del desempeño Evaluación del Desempeño “9.2 Auditoría Interna” y Controles Tecnológicos “A.8.8 Gestión de vulnerabilidades técnicas”, se valida este punto del control.

|	Conforme
Auditor:	Karina Alonso Sánchez

Proceso / Servicio:	**RECORRIDO FISICO**
Departamento, Área o Unidad de Negocio:	SITIO | Insurgentes
Personal Relacionado:	Ana Laura Hernández Montaño-Coordinador de Sistemas. Rafael Fernando Mendoza Loza-Coordinador de Sistemas

Elementos normativos relacionados

A.7.1 Perímetros de seguridad física, A.7.2 Entrada Física, A.7.3 Aseguramiento de oficinas, habitaciones e instalaciones., A.7.4 Supervisión de la seguridad física, A.7.5 Protección contra amenazas físicas y ambientales, A.7.6 Trabajar en áreas seguras, A.7.8 Emplazamiento y protección de equipos, A.7.11 Servicios públicos de apoyo, A.7.12 Seguridad del cableado, A.7.13 Mantenimiento de equipos, A.7.9 Seguridad de los bienes fuera de las instalaciones, A.7.14 Eliminación o reutilización segura del equipo, A.8.1 Dispositivos de punto final de usuario, A.7.7 Escritorio limpio y Pantalla limpia, A.5.5 Contacto con las autoridades, A.8.14 Redundancia de las instalaciones de procesamiento de información

Información Documentada revisada

Recorrido Virtual: Sitio 1: Insurgentes Sur 686, despacho 902, colonia del valle, delegación Benito Juárez, ciudad de México, código postal 03100.

Descripción de la Evaluación

RECORRIDO VIRTUAL

Se realiza un recorrido virtual con apoyo de un dispositivo móvil y se valida.

PERÍMETROS DE SEGURIDAD FÍSICA

- Áreas públicas ubicadas correctamente.
- Área reservada: con señalización.
- Área restringida: Site de Comunicaciones con medidas de Seguridad.

ASEGURAMIENTO DE OFICINAS, HABITACIONES E INSTALACIONES

- Puertas cerradas.
- Control de llaves.
- Directorio de teléfonos de emergencia.

SUPERVISIÓN DE LA SEGURIDAD FÍSICA

- Cámaras de emergencia: en todo el Sitio.
- Lámparas de emergencia .

ENTRADA FÍSICA

- Gafetes del personal de la organización: En la recepción se entrega el Gafett.
- Personal de vigilancia que colabora con el registro de bitácora de visitante y equipo en la entrada
- Solicita identificación al personal visitante
- Revisión de pertenencias de personal externo
- Se identifica la zona de entrega y carga ubicada en: en la Entrada Piso 9
- Se valida la identificación de esta zona en el recorrido virtual

TRABAJAR EN ÁREAS SEGURAS

- Normas de conducta (no se permite persona con aliento alcohólico, con armas, con gorras y lentes, con vestimenta inapropiada): colocadas en las diferentes áreas
- Supervisión de personal visitante especialmente de áreas restringidas: con señalización
- Los visitantes no pueden tomar grabaciones o video.
- Se valida la disponibilidad de manual de interno de protección civil.
- Registro de eventos en el reporte de diario

RETIRO DE ACTIVOS

- Revisión de pertenencias de personal externo.
- Revisión de equipos al ingreso y salida.

PROTECCIÓN CONTRA AMENAZAS FÍSICAS Y AMBIENTALES

- Extintor CO2 – Fecha de servicio: Julio 2024
- Señalética de Ruta de evacuación.
- Señalética del equipo contra amenazas externas y ambientales.
- Aires acondicionados, Mini Split.

SEGURIDAD DEL CABLEADO

- Se puede observar la separación del cableado eléctrico, y de telecomunicaciones.
- Se encuentra en canaletas metálicas.

- Se encuentra en buenas condiciones.

SERVICIOS PÚBLICOS DE APOYO

- UPS con baterías en los diferentes áreas

MANTENIMIENTO DE EQUIPOS | CUMPLIMIENTO DE POLÍTICAS, REGLAS Y ESTÁNDARES DE SEGURIDAD DE LA INFORMACIÓN

- Limpieza físico preventivo, limpieza lógica, revisión de activación de antivirus, actualización de SO, desfragmentación del disco, revisión de software autorizado

Resultado de la Evaluación:	Conforme
Auditor:	Karina Alonso Sánchez

Proceso / Servicio:	**RECORRIDO VIRTUAL**
Departamento, Área o Unidad de Negocio:	SITIO | TOLUCA
Personal Relacionado:	Ana Laura Hernández Montaño-Coordinador de Sistemas. Rafael Fernando Mendoza Loza-Coordinador de Sistemas

Elementos normativos relacionados

A.7.1 Perímetros de seguridad física, A.7.2 Entrada Física, A.7.3 Aseguramiento de oficinas, habitaciones e instalaciones., A.7.4 Supervisión de la seguridad física, A.7.5 Protección contra amenazas físicas y ambientales, A.7.6 Trabajar en áreas seguras, A.7.8 Emplazamiento y protección de equipos, A.7.11 Servicios públicos de apoyo, A.7.12 Seguridad del cableado, A.7.13 Mantenimiento de equipos, A.7.9 Seguridad de los bienes fuera de las instalaciones, A.7.14 Eliminación o reutilización segura del equipo, A.8.1 Dispositivos de punto final de usuario, A.7.7 Escritorio limpio y Pantalla limpia, A.5.5 Contacto con las autoridades, A.8.14 Redundancia de las instalaciones de procesamiento de información.

Información Documentada revisada

Recorrido Virtual: Sitio 2: Hermenegildo Galeana No. 204, despacho 3, Col. Centro, C.P. 50000, Toluca, Edo. México

Descripción de la Evaluación

RECORRIDO VIRTUAL

Se realiza un recorrido virtual con apoyo de un dispositivo móvil y se valida:

PERÍMETROS DE SEGURIDAD FÍSICA

- Áreas públicas
- Área reservada
- Área restringida: Site de comunicaciones

ASEGURAMIENTO DE OFICINAS, HABITACIONES E INSTALACIONES

- Puertas cerradas
- Control de llaves: para sitios específicos
- Directorio de teléfonos de emergencia: colocados en las instalaciones

SUPERVISIÓN DE LA SEGURIDAD FÍSICA

- Cámaras de emergencia: en todas las áreas
- Lámparas de emergencia.

ENTRADA FÍSICA

- Gafetes del personal de la organización: se les solicita en el acceso al Personal
- Personal de vigilancia que colabora con el registro de bitácora de visitante y equipo y se muestra la bitácora
- Solicita identificación al personal visitante.
- Revisión de pertenencias de personal externo
- Se identifica la zona de entrega y carga ubicada en la zona de entrada
- Se valida la identificación de esta zona en el recorrido virtual.

TRABAJAR EN ÁREAS SEGURAS

- Normas de conducta (no se permite persona con aliento alcohólico, con armas, con gorras y lentes, con vestimenta inapropiada).
- Supervisión de personal visitante especialmente de áreas restringidas.
- Los visitantes no pueden tomar grabaciones o video:
- Se valida la disponibilidad de manual de interno de protección civil.
- Registro de eventos en el reporte de diario.

RETIRO DE ACTIVOS

- Revisión de pertenencias de personal externo.
- Revisión de equipos al ingreso y salida

PROTECCIÓN CONTRA AMENAZAS FÍSICAS Y AMBIENTALES

- Extintor CO2 – Fecha de servicio: Junio 2024
- Señalética de Ruta de evacuación.
- Señalética del equipo contra amenazas externas y ambientales.
- Aires acondicionados, Mini Split.

SEGURIDAD DEL CABLEADO

- Se puede observar la separación del cableado eléctrico, y de telecomunicaciones:
- Se encuentra en canaletas metálicas Julio
- Se encuentra en buenas condiciones.

SERVICIOS PÚBLICOS DE APOYO

- UPS con baterías: en los diferentes lugares

MANTENIMIENTO DE EQUIPOS | CUMPLIMIENTO DE POLÍTICAS, REGLAS Y ESTÁNDARES DE SEGURIDAD DE LA INFORMACIÓN

- Limpieza físico preventivo, limpieza lógica, revisión de activación de antivirus, actualización de SO, desfragmentación del disco, revisión de software autorizado

Resultado de la Evaluación:	Conforme
Auditor:	Karina Alonso Sánchez

Proceso / Servicio:	**PLANEACIÓN** **OPERACIÓN**
Departamento, Área o Unidad de Negocio:	Administración y dirección
Personal Relacionado:	Salvador Santiago Araujo Iraís Dafne Mendoza Sánchez

Elementos normativos relacionados

6.1.1 Generalidades
6.1.2 Evaluación de riesgos de seguridad de la información
6.1.3 Tratamiento de riesgos de seguridad de la información
6.3 planificación de cambios
8.1 Planeación y Control operativo
8.2 Evaluación de riesgos de seguridad de la información
8.3 Tratamiento de riesgos de seguridad de la información

Información Documentada revisada

PRO-CAL 009 Procedimiento para el tratamiento de riesgos y oportunidades del SGC YSGSI abril 2024 V4
matriz de riesgos y oportunidades para el SGC y SGSI FOR-CAL 016
plan de tratamiento para riesgos y oportunidades FOR-CAL-017

Descripción de la Evaluación

6.1.1 GENERALIDADES | 8.1 PLANEACIÓN Y CONTROL OPERATIVO | 6.1.2 EVALUACIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN | 8.2 EVALUACIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN | 6.1.3 TRATAMIENTO DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN | 8.3 TRATAMIENTO DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN
PRO-CAL 009 Procedimiento para el tratamiento de riesgos y oportunidades del SGC YSGSI abril 2024 V4
Se muestra riesgos y actividades
No
Descripción
Responsabilidades
Se muestra calendario de revisiones
Se registrada matriz de riesgo FOR-CAL 016

Capacitadores de nuevos clientes
Costos competidores
Perdida de contratos
Riesgos y oportunidades operacionales

- Tecnologías
- financieros
- Leales
- ambientales
- Estructuradas
- Identificación del riesgo acorde a

- 0 controlado
- -1 controlado con vulnerabilidades
- -2 sin control con vulnerabilidades

A =1 se acepta oportunidad
R= se rechaza oportunidad

matriz de riesgos y oportunidades para el SGC y SGSI FOR-CAL 016
falla eléctrica
probabilidad -1

impacto -2

- Identificación de riesgo
- Tipo de riesgo
- Áreas de impacto por riesgo
- financiero
- imagen
- normativo
- Operativo
- Legal

- Riego residual
- Área de sistemas
- -10
- Nivel asignado
- Riesgo residual
- Monitoreo semestral

Riesgos identificados

- Incendio dentro de las instalaciones
- Falla eléctrico
- Sismos
- Epidemiológico
- Fallas de plataformas
- Servicios de internet
- Virus informáticos
- Falta de capacitación malas practicas
- Resistencia al cambio
- Vandalismo
- Procesos internos
- Cambios en el marco legal

Se cuenta con riesgos de controles en nivel bajo
plan de tratamiento para riesgos y oportunidades FOR-CAL-017

Se identifica el documento PRO-CAL 016 Procedimiento para el tratamiento de riesgos y oportunidades del SGC YSGSI abril 2024 versión 04

Marzo 2023
Abril 2024
Octubre 2024
Abril 2025
Octubre 2025
Una vez identificados los riesgos y oportunidades de la empresa a tratar se clasificarán de acuerdo a con su tipo y se registra en la matriz de riesgos y oportunidades para el SGC y SGSI FOR-CAL 016
Se dará justificación en caso de que se rechace las oportunidades
Captación de nuevos clientes
Mercadotecnia
Costos competitivos
Perdida de contratos
Incumplimientos de procesos
Se identifica el plan de tratamiento para riesgos y oportunidades FOR-CAL-017 versión 3 abril 2024

- Riesgo alto
- Riesgo medio

- Riego bajo

Aceptar el riesgo
• Transferir o compartir el riesgo

Reducir el riesgo
• Eliminar el riesgos
Oportunidades
- Aceptar la oportunidad
- Rechazar la oportunidad

Ejemplo:
Virus informático – 8 | aceptar
Fuga de información – 6 |Aceptar
Daño a la información
Phishing – 7 | Aceptar

SOA
Declaración de Aplicabilidad versión

- Controles
- Objetivo
- Justificación de aplicabilidad
- Implementado
- Riesgos por evento

Se consideran los 91 controles aplicados
5.23 control excluido
Descripción del alcance:
Los servicios de investigación de crédito (referencias comerciales, verificación de propiedad y sociedades en el RPPYC), recuperación de cartera (extrajudicial y judicial), cobranza punta-punta y gestión domiciliaria, soportado por los procesos de sistemas, compras, recursos humanos, contabilidad y tesorería. De acuerdo con la declaración de aplicabilidad (SOA) LIS-GSI_007, versión 10, de agosto 2024

Resultado de la Evaluación:	Conforme
Auditor:	David Abraham Nieto López

Proceso / Servicio:	**CONTROLES ORGANIZACIONALES Y DE PERSONAS.** **INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN**
Departamento, Área o Unidad de Negocio:	Administración y dirección
Personal Relacionado:	Salvador Santiago Araujo Iraís Dafne Mendoza Sánchez

Elementos normativos relacionados
A.5.29 Seguridad de la información durante la interrupción A.5.30 Preparación de las TIC para la continuidad de las negocio A.8.14 Redundancia de las instalaciones de procesamiento de información

Información Documentada revisada
Continuidad de la Seguridad de la información PRO GSI 019 versión 7 agosto 2024 Simulacro FOR-GSI-050 fecha de actualización agosto 2023 versión 02 operativo para las TIC PRO-GSI-037 versión 7 Generación de minuta FOR-CAL-001

Descripción de la Evaluación
A.5.29 SEGURIDAD DE LA INFORMACIÓN DURANTE LA INTERRUPCIÓN | A.5.30 PREPARACIÓN DE LAS TIC PARA LA CONTINUIDAD DE LAS NEGOCIO | A.8.14 REDUNDANCIA DE LAS INSTALACIONES DE PROCESAMIENTO DE INFORMACIÓN Se identificó Documento Continuidad de la Seguridad de la información PRO GSI 019 versión 7 agosto 2024 Que menciona • Planificación de la Continuidad • Planes de prueba • Matriz de Responsabilidades • Tipo de eventos que pone en riesgos • Identificación de bienes y servicios La organización determina su necesidad de seguridad de la información de acuerdo con el contexto interno y externo, así como requisitos de los clientes De acuerdo con su alcance establecido para el SGSI la parte critica se debe asegurar en todo momento y la confidencialidad, integridad del base de datos que se encuentran en el Servidor. A continuación, se presentan los escenarios para los que se tienen los planes de continuidad • Falla eléctrica • Falla de aplicaciones web • Sismos y desastres naturales • Caída de servidor de correo electrónico • Caída de dominio • Falla en la red • Falla en internet • Caída de telefonía Se realizó prueba de sobrecarga, generando una sobre carga eléctrica Se realiza dinámica de configuración Se levanta ambiente espejo Con información de prueba Y evidencia de los sistemas ocupados simulacros anuales Manual de seguridad de la documentación MAG-GSI-001 Se muestra el proceso de las continuidad de la seguridad de la información Protección de base de datos y servidores Concientización del personal Servidores | sistemas críticos Proceso de respaldos y mantenimiento de la información Infraestructura de operatividad Centro espejo Simulacro FOR-GSI-050 Directores de soporte especializado requerido Coordinación de dirección y gerencia administrativa Brigadas de protección civil | personal administrativo | ejercicios de emergencia Replica de información en centros espejo entre los 3 sitos y sede Vuelta a la normalidad Autorización para reanudar operaciones Verificación disponibilidad integridad y confidencialidad de la información Generación de minuta FOR-CAL-001 - Servidores - redes - equipo de computo - instalaciones operativo para las TIC PRO-GSI-037 versión 7 redundancias de alta disponibilidad

- equipos de Fortinet
- IPS
- Antivirus
- Control de aplicaciones
- PVN

Telmex y total play responsables de monitoreo | comunicación por llamada telefónica
Responsable de generar análisis de vulnerabilidades cada 180 días
Plan de contingencia versión 15 PRO-CAL-006
Plan de recuperación de desastres versión 2

- RTO
- Funciones de cada puesto
- Simulacros
- BIA

Se muestra RTO

- Procesos de recursos humanos | 2 horas
- Cartera | 1 hora
- Cobranza punta a punta |1
- Se muestra procesos de criticidad

Recuperación de aplicativo WEB

- Una hora recuperación
- Criticidad media
- Corte de energía
- Falla no-break
- Corte de red

Simulacro FOR-GSI-050 fecha de actualización agosto 2023 versión 02
Fecha 02/07/2024

Corte de energía
Aplicaciones web
Servidor | falla de internet protección civil
Tiempo lastimado de respuesta 20 min
Tiempo estimado de simulacro 30 min
Se muestra correo de 2 julio 2024
Se reporte mediante correo electrónico se reporta del área de banco la presencia de un correo sospechosos y se solicita que se confirma si es autentico
Se responde el correo explicando el correo es falso y como idéntica un correo autentico del sitio para aclarado que no se solicita renovación de contraseña por correo 36 minutos para su recuperación

Fecha 08/03/2024
Comprobar tiempo de respuesta del equipo de sistema a múltiples caídas de sistemas
corroborar si el personal de sistemas realiza un análisis de la causa
Corroborar si el área del sistema realice un buen diagnóstico encuentre la verdadera causa del problema
• Recuperación se realizará en el centro de datos
• El centro de datos debe encontrarse en línea y operando y controlado desde un monitoreo
• Se debe seguir el Plan de Protección Civil PRO DIR 001
• Las operaciones deben ser restablecidas en un centro de datos alterno a ser definido por la dirección general
Falla de reporte de SGC file maker portal de ticket presentan inconvenientes al abrirlos
Se realiza corto de energía
Se reporta inaccesibilidad da portales y aplicaciones SGC CIA desk file maker
Se realiza revisión el personal revisan servidores físicos
Se realiza cambio de baterías

Se reinicia servidor y se revisa funcionamiento
Tomo 40 min para su recuperación

Dada la naturaleza de las operaciones de la organización se cuentan con 3 centros de datos en las oficinas principales para proteger en todo momento la seguridad de la información se establecieron acuerdos comerciales con las empresas TOTAL SEC y Scitum con el fin de adquirir los servicios de seguridad perimetral en los centros de datos de la organización actualmente a los centros de datos declarados son los siguientes:
• Oficina Nezahualcóyotl
Oficina del VALLE
• Oficina Toluca
Cada centro de datos cuenta con sistemas de redundancia, la configuración entre los equipos de operaciones y redundantes se encuentran en alta disponibilidad.

Resultado de la Evaluación:	Conforme
Auditor:	David Abraham Nieto López

Proceso / Servicio:	**CONTROL DE INFORMACIÓN DOCUMENTADA.**
Departamento, Área o Unidad de Negocio:	Administración y dirección
Personal Relacionado:	Salvador Santiago Araujo Iraís Dafne Mendoza Sánchez

Elementos normativos relacionados

7.5.1 Generalidades
7.5.2 Creación y actualización.
7.5.3 Control de la información documentada.

Información Documentada revisada

Lista de información documentada controlada LIS CAL 001 de fecha agosto 2023 versión 06
Gestión de activos y clasificación de control de la información PRO SGSI 15
Lista de información documentada controlada agosto 2023 LIS-CAL-001 versión 6
Lista de información documentación externa controlada Julio 2023 versión 03 lis CAL 002
Gestión de activos clasificación y control de la información PRO GSI 015 versión 10 d fecha enero 2024

Descripción de la Evaluación

7.5.1 GENERALIDADES
Información documentada
Control de información documentada PRO CAL 001 versión 18 de fecha agosto 2024
Tipografía:
Codificación de nuevos documentos
La información documentada que integran ambos Sistemas de Gestión se clasificará y codificará de la siguiente forma:
DDD XXX ZZZ
- De donde:
- DDD: Son 3 caracteres que indican el tipo de documento, los grupos de documentos, se
- identifican por las abreviaciones siguientes:
- Manual
- . MAN
- . MAP
- PRO
- INS
- FOR
- . LIS

- POL
- REG
- DOC
- DOM

Procedimiento
- Instrucción de trabajo
- Formato
- Listado
- Política
- Registro
- Documento
- Documentación
- XXX: Son 3 caracteres que indican el área al que pertenece el documento:
- . DIR | Dirección
- . CAL | Calidad
- . CON | Contabilidad y Tesorería
- 3 caracteres número consecutivo

Desarrollo de actividades

Gestión de activos y clasificación de control de la información PRO SGSI 15
- Cambios de documentos
- Correo electrónico
- Se realiza revisión
- Coordinador se cambia número de versión
- Se firma elaboro reviso aprobó
- Se publica
- Se necesitara revisar una vez al año la documentación

Se establecen lineamientos para la revisión y aprobación de documentos:
- Se muestran el repositorio
- que se encuentra alojado en servidor físico
- Se tiene los documentos editables
- Tener disponible hacia personal es a través de la intranet
- Públicos

Nombre del documentos registros
- Tipo de documento
- Identificación
- Origen
- Versión
- Fecha de emisión
- Fecha última versión
- Responsable de resguardo
- Resguardo de versión
- Versión publica
- Tiempo de retención

Nombre del documentos registros
- Tipo de documento
- Identificación
- Origen
- Versión
- Fecha de emisión
- Fecha última versión
- Responsable de resguardo
- Resguardo de versión
- Versión publica

- Tiempo de retención
- Disposición final
- Tipo de información

Lista de información de documentos LIS- CA_001
Se revisan de forma una vez al año
Lista de información documentada controlada agosto 2023 LIS-CAL-001 versión 6

- 27001
- Q43q
- Código
- Nombre
- Revisión actual
- Fecha de emisión
- Fecha de revisión
- Ubicación
- Responsable
- Tiempo de resguardo

Se revisa

- Políticas generales de seguridad de la información Revisión 7 agosto 2024
- Desarrollo seguro pro GES 002 versión 8 versión 2024
- Crear modificar
- Asignar
- eliminar

7.5.2 CREACIÓN Y ACTUALIZACIÓN
Requisito de la norma
- Área
- Código
- Nombre
- Revisión actual
- Fecha de emisión
- Fecha de revisión
- Ubicación
- Responsable del documento
- Tipo de resguardo
- Versión 10
- Gestión de activos clasificación y control de la información
- PRO GSI 015
- Desarrollo seguro
- Versión 08
- PROGSI 046

Documentación externa
Lista de información documentación externa controlada Julio 2023 versión 03 lis CAL 002
- Emite
- Año de edición
- Responsable del documento

Medio de resguardo
- Ubicación
- Tiempo de resguardo
- Nombre
- No
- Disposición final

Control de actualizaciones
- Tipo de documento

- Identificación
- Pública o privada
- Versión publicada
- Fecha de creación
- Responsable
- Tipo de resguardo
- Tipo de información

Se muestran el repositorio - que se encuentra alojado en servidor físico
Se tiene los documentos editables
Tener disponible hacia personal es a través de la intranet

- Se muestra correo de anal Laura
- Revisión y actualización de documentación
- 1 Junio 2023 se muestra solicitud de actualización
- Junta para actualizar estatus de actualización de documentos
- Lunes reunión de lideres avance y reforzamiento de seguimiento
- Cifrado con acrobat Reader cifrado se muestra procedimiento de certificado
- Mesa de trabajo para revisor y publicar
- Cada dueño del proceso se encarga de sus documentación

7.5.3 CONTROL DE INFORMACIÓN DOCUMENTADA

Se revisan elementos siguientes en los documentos:
- Control de versiones, códigos, clasificación.
- Documentos externos
- ISO 27001
- Ley de protección de datos personales.

Se muestra
Tipo de registros considerados su clasificación medios de almacenamientos y responsables
- Tipo de registro
- Clasificación
- medio de registro
- área responsable

Se revisan elementos siguientes en los documentos:
- Control de versiones, códigos, clasificación.
- Documentos externos
- Muestran documento LIS CAL 002

Mapa de procesos de sistemas Septiembre 2023 Versión 05 MAP SIS 001
Consideración de seguridad de la información
Información referida en este documento
- Tipo de información
- Medios
- Personal que puede tener acceso a la información

Clasificación
- Interna | restringida | publico | clasificado

Gestión de activos clasificación y control de la información PRO GSI 015 versión 10 d fecha enero 2024
- Información
- Descripción
- Calificación

Quien tiene acceso
- Dispositivos final

Resultado de la Evaluación:	Conforme
Auditor:	David Abraham Nieto López

Proceso / Servicio:	**CONTROLES ORGANIZACIONALES Y TECNOLÓGICOS.**
Departamento, Área o Unidad de Negocio:	Gerente Administrativo | Coordinador Ti
Personal Relacionado:	Salvador Santiago Araujo Rafael Fernando Mendoza Loza

Elementos normativos relacionados

A.5.7 Inteligencia de amenazas
A.5.37 Procedimientos operativos documentados.
A.8.6 Gestión de capacidad
A.8.7 Protección contra malware.
A.8.8 Gestión de vulnerabilidades técnicas.
A.8.13 Copias de seguridad de la información
A.8.15 Registros.
A.8.16 Actividades de seguimiento
A.8.17 Sincronización del reloj.
A.8.19 Instalación de software en sistemas operativos.
A.8.32 Gestión de cambios
A.8.34 Protección de los sistemas de información durante las pruebas de auditoría.

Información Documentada revisada

Gestión de activos clasificación y control de la información PRO-GSI-015 versión 10 de fecha enero 2024
PRO GSI 032 Procedimiento respaldos y eliminación de información, versión 11 septiembre 202
LIS GSI 002 Revisión de logs versión 3 enero 2024
Actividades documentado en actividades de log LIS-GSI-002

Descripción de la Evaluación

A.5.37 PROCEDIMIENTOS OPERATIVOS DOCUMENTADOS.
PRO GSI 001 Procedimiento de sistemas
PRO GSI 020 Gestión de incidentes
PRO GSI 015 Gestión de activos, clasificación y control de la información
PRO GSI 032 Procedimiento respaldos y eliminación de información,

A.8.6 GESTIÓN DE CAPACIDAD
Asegurar la capacidad de capacidades de todas las áreas y de los recursos necesarios
Se gestiona a partir del inventario de activos, los requerimientos de los clientes y del negocio para una ampliación de plantilla de personal o de recursos tecnológicos.
Gestión de activos clasificación y control de la información PRO-GSI-015 versión 10 de fecha enero 2024
Fecha de asignación plan de renovación para cada archivo
Mantenimiento
Conservación del inventario
Catálogo de software
Almacenamiento y tratamiento de la información
Propiedad de los activos
Garantizar la confidencialidad y disponibilidad de los activos
Toda capacidad de los recursos es gestionada por necesidades del cliente y en cada licitación se definen los recursos
Se muestra check lis de monitoreo de capacidades que se efectúa cada 15 días
Se muestra correo de monitoreo de FOTINET |solicitud de afectación totalplay fecha de inicio y termino 9 julio 2024
Oportunidad de mejora Fortalecer y definir lumbrales de capacidades internos para documentar límites aceptables de operatividad y su procedimiento.
Se muestra correo de solicitud de discos duros | operación lenta e intermitencia | 20 octubre 2020
A.8.7 PROTECCIÓN CONTRA MALWARE. | A.5.7 INTELIGENCIA DE AMENAZAS | A.8.8 GESTIÓN DE VULNERABILIDADES TÉCNICAS.
El antivirus que se utiliza centinela ONE XDR
Se muestra compra de centinela ONE

Se encuentra diferentes servidores para mitigar afectación
Con centinela ONE se cuenta con protección y monitoreo a través de directivas y políticas establecidas
Se muestra consola cuenta con autenticación de doble factor
Se muestra consola
Se muestra monitoreo de equipos

Alertamiento de malware
Graficas de monitoreo
Detector
Módulos activos
Agentes se muestra configuraciones de activaciones
Registro de incidentes para pos-morten
Se analiza muestra | para realizar pruebas del incidente
Evaluación y decisión sobre los eventos de seguridad de información | aprendizaje recopilación de amenazas
Revisar incidentes relevantes para su análisis
Se realiza patrones de conducta con el aplicativo centinela ONE XDR

- Se revisan log periódicamente
- Se muestra procedimiento de afectación de ransomware
- Se muestra reporte enviado a Banorte y alta dirección
- Se muestra procedimiento de mitigación
- 18 diciembre 2023 fecha de afectación
- Carta enviada enero 2024
- Se realiza análisis forense | SCITUM
- Se procede a realiza análisis de inteligencia de amenazas
- Se procede a comprar centinela
- 6 meses se realiza análisis de vulnerabilidades
- Se muestra mayo 2024 análisis de vulnerabilidades
- 59 informativos
- 0 | altos medios bajos
- NESSUS

A.8.13 COPIAS DE SEGURIDAD DE LA INFORMACIÓN
Se identificó el documento PRO GSI 032 Procedimiento respaldos y eliminación de información, versión 11 septiembre 202
Se realiza una copia de seguridad completa y copias de seguridad diferenciales de manera diaria, con la herramienta Robocopy.
Todas las carpetas de los servidores
Pruebas de las copias de seguridad
Los respaldos de los sistemas críticos (SICOB, Opti-Risks, G-DOOM, filemaker, ASPEL, SGC, SGCI y CIADESK, ERP) Así como las carpetas del servidor son monitoreados.
Muestran logs de la realización de pruebas de respaldos.
También se cuenta con NAS
Se monitorean los logs de la NAS para ver que se hayan hecho de manera correcta
Se muestra log

- NAS respaldos automáticos
- Diario respaldos
- Realizado el ultimo 23/09/2024 registro de carpetas
- Investigación y cobranza
- Respaldos diferenciales
- AES 256 encriptado de encriptación
- Se realiza pruebas periódicas diariamente
- Arreglo RAID servidores

A.8.15 REGISTROS. | A.8.16 ACTIVIDADES DE SEGUIMIENTO
Todos los servidores tienen un visor de eventos
Se identifican el documento LIS GSI 002 Revisión de logs versión 3 enero 2024 donde se registran los servidores, IP servidor, fecha de revisión, se registraron eventos de impacto (si/no), criticidad del evento, resumen evento, usuario/equipo que detono evento, id del evento

Se identifica revisión de visor
- Se revisa usuario
- IP equipo
- XDR activo
- Acceso
- Unidades externas
- Paginas restringidas
- Protector de pantalla
- Se realiza cada 3 meses
- Se realiza log
- Se revisa lo cada 15 días

Actividades documentado en actividades de log LIS-GSI-002

A.8.17 SINCRONIZACIÓN DEL RELOJ.

Se muestra en consola sincronización de reloj frece-running system clock

A.8.19 INSTALACIÓN DE SOFTWARE EN SISTEMAS OPERATIVOS.

Se muestra catálogo de software permitidos

LIS -GSI -004 versión 1 de fecha junio 2024 catálogo de software y aplicaciones permitidos en CIA

- Nombre | aplicación
- Dispositivo
- Fabricante
- Versión
- Fecha
- Licenciamiento
- Tipo
- acrobat reader
- Apolo
- CamScaner
- Clawin
- Geany
- Leycera
- macAffe
- office
- netbeats
- SAE
- Smart forms
- SQL manager

A.8.32 GESTIÓN DE CAMBIOS

Se identifica el documento PRO GSI 039 Operativo para las TICs, versión 7 enero 2024

Se identifica que los cambios pueden

Cualquier cambio sobre sistemas operativos o de producción debe ser realizado de la siguiente forma:

Los cambios pueden ser propuestos por cualquier usuario y/o partes interesadas

Los cambios deben ser aprobados por dirección

El área de sistemas es el responsable de verificar que los cambios se han implementado de acuerdo con el requerimiento

La implementación de los cambios deber ser reportada a los responsables de las áreas o procesos involucrados en los cambios o adecuaciones.

Los cambios se registran en un plan de mejoras

- 13 agosto 2024
- Actualización
- Levantamiento por Rafael
- Compilación de lindos
- Pila de mantenimiento
- DG!RWA 1 w59

- 9719
- 13 agosto 2024 abierto y cerrado

- 13 agosto 2024
- Herramienta de actualización de eliminación de software malicioso
- No se instala servidor corrupta
- Microsoft no ha notificado actualización del CAF
- Z2AZ69Ja ID
- 9727 ticket

A.8.34 PROTECCIÓN DE LOS SISTEMAS DE INFORMACIÓN DURANTE LAS PRUEBAS DE AUDITORÍA.

- Se realiza con el monitoreo de actividades
- Con el visor de eventos
- Se realiza de manera trimestral
- Recertificación de accesos

Resultado de la Evaluación:	Conforme
Auditor:	David Abraham Nieto López

Proceso / Servicio:	**CONTROLES TECNOLÓGICOS.**
Departamento, Área o Unidad de Negocio:	Programador | Gerente Administrativo | Coordinador Ti
Personal Relacionado:	Salvador Santiago Araujo Rafael Fernando Mendoza Loza Alan Hernández Ramírez

Elementos normativos relacionados

A.8.25 Ciclo de vida de desarrollo seguro.
A.8.26 Requisitos de seguridad de la aplicación.
A.8.27 Arquitectura del sistema seguro y principios de ingeniería.
A.8.28 Codificación segura.
A.8.29 Pruebas de seguridad y aceptación del desarrollo.
A.8.30 Desarrollo subcontratado.
A.8.33 Información de prueba.
A.8.11 Enmascaramiento de datos.

Información Documentada revisada

PRO-GSI-046 Desarrollo Seguro Versión 8 con fecha de Agosto del 2024
Hoja de Vida e Implementación FOR-GSI-002 Versión 2 con fecha de Mayo 2024

Descripción de la Evaluación

A.8.25 CICLO DE VIDA DE DESARROLLO SEGURO. | A.8.27 ARQUITECTURA DEL SISTEMA SEGURO Y PRINCIPIOS DE INGENIERÍA.
1.2 Los requisitos para el desarrollo de nuevos sistemas o para la realización de mejoras a los existentes se especifiquen y documenten formalmente
en la hoja de vida e implementación FOR GSI 002 y en el sistema de tickets (CIA-Desk)
Se revisan registros y su trazabilidad, en el documento FOR GSI 002 hoja de vida e implementación, donde se registra lo siguiente:
Área solicitante: Investigación de crédito
Descripción del requerimiento
Análisis de proyecto
Dictamen del proyecto
Etapa | Análisis de requerimientos de requisitos | Diseño y arquitectura | Programación | Pruebas | Documentación | Mantenimiento.
A.8.26 REQUISITOS DE SEGURIDAD DE LA APLICACIÓN. | A.8.28 CODIFICACIÓN SEGURA. | A.8.11 ENMASCARAMIENTO DE DATOS.

7. Hay que asegurar que todo desarrollo organizacional cuente con una arquitectura documentada que contenga al menos los siguientes aspectos:
Modularidad
- Escalabilidad
- Integración con sistemas legados
- Disponibilidad
- Confidencialidad
- Soporte

Se muestra el Documento PRO-GSI-046 Desarrollo Seguro Versión 8 con fecha de Agosto del 2024
Derivado a la naturaleza de los servicios que proporcionamos en la Organización, debemos contar con un área dedicada al desarrollo de aplicaciones y/o software, el área de Sistemas debe de establecer un marco organizacional para el desarrollo de software, en el cual se establezca una metodología para todo el ciclo de vida del desarrollo.
Sistemas
Todos los proyectos de creación de software creados o desarrollado por el personal es propiedad de la organización.
Sistemas
La organización cuenta con un ambiente de ejecución aislado, donde cada aplicativo, información y herramienta se encuentran en diferentes servidores con el fin de mitigar.

Todas las aplicaciones cuenten con un módulo de seguridad, mediante el cual solo sé administre y gestione el ABC (altas, bajas y cambios) de usuarios, asegurando la trazabilidad de las sesiones de cada usuario. Este módulo debe contar con herramientas para la generación de reportes del control de acceso y gestión de usuarios.
El módulo de seguridad deberá alimentarse desde la base de datos de recursos humanos y mantenerse actualizada.

El personal de desarrollo deberá:
1 Establecer un marco organizacional para el desarrollo de software, en el cual se establezca una metodología para todo el ciclo de vida del desarrollo.
2 Documentar todas las etapas del proceso de desarrollo de software en el formato de Hoja de vida e implementación FOR GSI 002.
3. Adoptar las metodologías organizacionales para el desarrollo de proyectos y cumplir con los lineamientos definidos por la organización.
4. Asegurar su participación continua durante el proyecto de desarrollo.
5.Proveer ambientes controlados para el desarrollo de software organizacional como son:

- Entorno de desarrollo.
- Entorno de Testing
- Entorno de UAT.
- Entorno de producción.

Todos los datos de prueba deberán contar con un mecanismo de enmascaramiento de la información reservada y/o confidencial. Una vez utilizados los datos de prueba, el desarrollador deberá borrados antes de su pase a producción

Se muestra la Hoja de Vida e Implementación FOR-GSI-002 Versión 2 con fecha de Mayo 2024
Fecha de Solicitu:26 de Agosto del 2024
Área Solicitante: Investigadores de Crédito
Etapas
1. Análisis de Requisitos
2. Diseño y Arquitectura
3. Programación
4. Pruebas
5. Documentación
Fecha de Término: 12/10 /2024
Fecha | Prueba a Realizar | Persona que realiza | Dictamen | Firma de Aprobación | Observaciones
Se muestra el Documento de Plan FOR-CALL-011 Cambios y Mejoras

A.8.29 PRUEBAS DE SEGURIDAD Y ACEPTACIÓN DEL DESARROLLO. | A.8.33 INFORMACIÓN DE PRUEBA.

10.1 En caso de que, en la realización de pruebas al software, por ser nuevos o por ser actualizadas las versiones, se utilizarán datos ficticios u obsoletos para tal fin, por lo tanto, no se utilizarán datos reales que deban de ser protegidos.

PRO SI 046 desarrollo seguro, versión 8 agosto 2024
Durante el análisis del previo se establecen aquellas etapas relevantes para la revisión de funcionalidad y seguridad de los sistemas.
a) El área de sistemas deberá establecer los criterios para la aceptación de nuevos sistemas, así como para las nuevas versiones y la programación de la realización pruebas de acuerdo con los cambios que se van generando.
b) La liberación de las herramientas creadas se realiza a través de correo electrónico solicitando la aceptación y revisión de este con el área solicitarte.
Totas las pruebas se documentan en la bitácora de pruebas LIS GSI 012
las pruebas de deben documentar
Realizar análisis de seguridad en cada etapa
Pruebas en ambientes
Pruebas periódicas para sistemas
Revisar y mitigar posibles vulnerabilidades
Escalar privilegios
Control de cambios altas y bajas de usuarios

- ERP se realiza análisis |
- Proyecto desde cero
- Lenguaje Python
- CSS
- HTML5
- Java script

Se muestra hoja de vida de implementación FOPR-GSI-002
Se comienza provecho 24 abril 2023
Última actualización de fecha 26 agosto 2024
Actualización de funciones
Incorporación de funcionalidades
Versión a liberar 0.14

- Jira
- Tablero de TX
- Funciones guardo en función
- Repositorio de GitHub
- Versiones
- Pruebas de funcionalidad
- Redes segregados VLAN
- Red separada de local
- Formato dinámico
- Mapeo de puertos
- SQL MANAGEMENT prevención de seguridad
- Pruebas con datos dummy
- Tarea D-120

A.8.30 DESARROLLO SUBCONTRATADO.
Control excluido aceptado

Resultado de la Evaluación:	Conforme
Auditor:	David Abraham Nieto López

Proceso / Servicio:	**CONTROLES ORGANIZACIONALES**

Departamento, Área o Unidad de Negocio:	Gerente Administrativo Coordinador Ti
Personal Relacionado:	Salvador Santiago Araujo Rafael Fernando Mendoza Loza

Elementos normativos relacionados

A.5.14 Transferencia de información
A.8.20 Seguridad de las redes
A.8.21Seguridad de los servicios de red
A.8.22 Segregación de redes

Información Documentada revisada

Pol GSI -001 agosto 204 versión 7 políticas generales de seguridad de la información
PRO SIS 001 Procedimiento de sistemas versión 22 Enero 2022
Plan de mantenimiento preventivo febrero 2024 versión 1 LIS GSI -010
Plan de mantenimiento preventivo febrero 2024 versión 1 LIS GSI -010
Pol GSI -001 agosto 204 versión 7 políticas generales de seguridad de la información

Descripción de la Evaluación

A.8.20 SEGURIDAD DE LAS REDES

- Enlace de seguridad
- Servicios de sed aseguramiento
- Verificar el funcionamiento de cada servidor
- Red para invitador
- Red colaboradores
- Redes segregadas
- 3 centro de datos
- Oficina de Toluca valle e insurgentes
- Sistemas redundantes en alta disponibilidad
- FORTINET IPS | filtrado de páginas web aplicaciones VPN
- Monitoreo 24/07
- Bloqueo de actividades sospechosos
- Seguimiento 48 horas

Los equipos FORTINET cuenta con las características habilidades siguiente:
- IDS/IPS
- Antivirus
- Filtrado de páginas web
- Filtrado de puertos
- Control de aplicaciones
- VPN

- Se muestra diagrama de red
- Insurgentes Toluca valle
- Enlace simétrico de total play
- Enlace simétrico de Telmex
- Fortigate
- Filtrado WEB

- Asignación y uso adecuado de credenciales y controles de acceso complementarios o temporales a usuario
- Mantener actualizado los documentos relacionadas con las redes de la firma como diagrama de red, lista de configuración de los dispositivos de res
- Establecimiento de responsabilidades y procedimientos para la gestión de las redes
- Monitoreo y registro de los logs de uso de la red
- Sistemas de autenticación de la red sistemas y filtrado de conexión a la red firewall
- Vigilar constantemente la red y control

Se muestra Plan de mantenimiento preventivo febrero 2024 versión 1 LIS GSI -010
22 /07/2024
Se muestra mantenimiento prevenido
Se muestra mantenimiento por áreas RRH contabilidad publico bancos
check lis de seguridad
Licenciamiento
Estado de antivirus
Desfragmentación de discos duros
Limpieza de discos

Se muestra Fortinet de NEZA IPS
Se muestra control de bloqueo
Monitoreo
Se muestra políticas investigación

- Antivirus
- Web filtres
- IPS
- Expedición de certificados
- Black lista
- Drogas
- Sexual
- Terrorismo
- Juegos
- Adultos
- Armas
- Drogas
- Internet
- Spam

Se muestra segregación de redes

A.8.21SEGURIDAD DE LOS SERVICIOS DE RED

- Aprovisionamiento.
- Monitoreo.
- Gestión
- Respaldos y recuperaciones
- Ticket para modificaciones
- Filtrado de contenido
- IPS status
- Antivirus
- Prevención de intrusos
- Antispyware
- Captura de ATP.

A.8.22 SEGREGACIÓN DE REDES

Muestran documento: Diagrama de red que representan su infraestructura donde se registra la redundancia y segregación de redes.
Enlace dedicados
- Telmex
- Totalplay
- Bestel

Firewall
Servidores
La organización cuenta con dos redes inalámbricas con acceso a internet
Red interna (CIA interno)
Red para invitados (CIA Guest)

Propiedad de
- Seguridad de la información
- Conceptos de Ciberseguridad
- Capacidades de operación

La red se segmenta de la siguiente manera
- Control de entrada de los usuarios que ingresas a cada segmento
- Control de salida de la información disponible en cada segmento
- Segmentación por dispositivos físico o lógico
- Acceso a las redes inalámbricas por categoría área u operación

A.5.14 TRANSFERENCIA DE INFORMACIÓN

5 Políticas para canales de comunicación

Electrónica.- correo electrónico, descarga de archivos desde internet, VPN y/o FTP.

En papel.- Debe controlarse mediante el procedimiento de clasificación de la información.

Pol GSI -001 agosto 204 versión 7 políticas generales de seguridad de la información

- Política de intercambio de información
- No puede ser compartida la información
- La red está configurada por reglas y roles de usuario
- Protección de antivirus

Resultado de la Evaluación:	Conforme
Auditor:	David Abraham Nieto López

Proceso / Servicio:	**CONTROLES ORGANIZACIONALES Y TECNOLÓGICOS**
Departamento, Área o Unidad de Negocio:	Gerente Administrativo Coordinador Ti
Personal Relacionado:	Salvador Santiago Araujo Rafael Fernando Mendoza Loza

Elementos normativos relacionados

A.5.15 Control de acceso.
A.5.16 Gestión de identidad.
A.5.17 Información de autenticación
A.5.18 Derechos de acceso
A.8.2 Derechos de acceso privilegiado
A.8.3 Restricción de acceso a la información.
A.8.4 Acceso al código fuente.
A.8.5 Autenticación segura.
A.8.12 Prevención de fuga de datos.
A.8.18 Uso de programas de utilidad privilegiados.

Información Documentada revisada

Pol GSI -001 agosto 204 versión 7 políticas generales de seguridad de la información
Procedimiento de control de accesos PRO-GSI-012 versión 10 de fecha agosto 2024
FOR-GSI-009 enero 2024 excepciones por puesto versión 1

Descripción de la Evaluación

A.5.15 CONTROL DE ACCESO.

El acceso a la red se encuentra debida mente protegido con las restricciones físicas, control de usuarios, con las políticas, procedimientos y documentos complementarios establecidos en materia de seguridad. Para el acceso a la red, al software, aplicaciones y bases de datos almacenados en los servidores que están ubicados en el site dentro de las mismas instalaciones físicas de la organización son administrados por el ara de sistemas, las conexiones con las que la organización cuenta son:
- Redes inalámbricas

- VPN's
- Acceso a bases de datos de filemaker

Se debe designar para control de personal
Personal interno que accedan a la información deberá contar con los lineamientos de control de accesos
Todo acceso a base de datos información sensible y áreas restringida solo podrá acceder personal autorizada
Procedimiento de control de accesos PRO-GSI-012 versión 10 de fecha agosto 2024
Lógico y físico

A.5.16 GESTIÓN DE IDENTIDAD. | A.5.17 INFORMACIÓN DE AUTENTICACIÓN | A.8.5 AUTENTICACIÓN SEGURA.

Muestran documento: Carta responsiva donde existen clausulas con respecto al uso de las contraseñas para el colaborador "Por este medio me doy por enterado que el usuario y contraseña asignados para la realización de mi trabajo quedan bajo mi completa responsabilidad a partir del día de hoy y los únicamente para los fines asignados, en caso de hacer mal uso usuarios y contraseñas la compañía podrá reclamar la reparación de los daño ocasionados mediante instancias legales aplicables en los estados unidos mexicanos."
Ninguna PC puede ser movido de su lugar
Solicitud de accesos
Accesos proveedores e invitados
Empleados
Todo personal deberá contar con contraseñas seguras para los accesos a sistemas internos
Se cuenta con las siguientes características para las contraseñas

- 8 caracteres
- Alfanumérico
- No contar con números consecutivos ni contraseñas fáciles de adivinar

A.5.18 DERECHOS DE ACCESO | A.8.2 DERECHOS DE ACCESO PRIVILEGIADO | A.8.18 USO DE PROGRAMAS DE UTILIDAD PRIVILEGIADOS.

Se valida que la organización cuenta con perfiles de usuario que en la herramienta active directory agrupan bajo ciertas políticas que controlan los accesos a los programas de utilidades y acceso a la información que no requiera para su puesto.
Se muestra autorización para herramientas
Insurgentes
Carta responsiva de excepciones FOR-GSI-051
Fecha de asignación 10 06 2024
Ortiz duran patricia
Solicitud de acepciones | WhatsApp medios extraíbles unidad C
"declaro que se ha proporcionado leído y explicado el comprometerme con cumplir los lineamientos de confidencialidad y disponibilidad de sistemas "
Se firma cada 3 meses

- Ramírez Héctor
- 10 06 2023
- Cruz mantones José Ricardo
- 10/06/2023
- Nezahualcóyotl

- Santiago Araujo salvador
- 01/07/2023
- Acceso a internet sin limitaciones
- Acceso a medios extraíbles
- Pérez Sánchez Fernando
- 03/05/2024

A.8.3 RESTRICCIÓN DE ACCESO A LA INFORMACIÓN.

Donde se observa el registro de los siguientes campos en el documento:
Usuario | Área | Dirección IP | Sistema Operativo | Microsoft Office | No-break | antivirus | Acceso a Unidad C: | Unidades externas | Páginas restringidas | Protector de pantalla | Fondo de política | Usuarios actualizados | Recordatorio de usuario WEB
FOR-GSI-009 enero 2024 excepciones por puesto versión 1

A.8.4 ACCESO AL CÓDIGO FUENTE.

Durante la entrevista con el personal, manifestó que actualmente solo cuentan con un desarrollador de software que cuenta con el acceso al código fuente que es controlado mediante la herramienta GitHub.

A.8.12 PREVENCIÓN DE FUGA DE DATOS.

Monitoreo de accesos a servicios, configuraciones.
Negación de uso de USB, servicios en páginas de nube, comunicación no oficial y los procesos de solicitudes de acceso a servicios de periféricos específicos.
· Monitoreo de información

Resultado de la Evaluación:	Conforme
Auditor:	David Abraham Nieto López

Proceso / Servicio:	**CONTROLES ORGANIZACIONALES Y DE PERSONAS.** **INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN**
Departamento, Área o Unidad de Negocio:	Gerente Administrativo Coordinador Ti
Personal Relacionado:	Salvador Santiago Araujo Rafael Fernando Mendoza Loza

Elementos normativos relacionados

A.5.24 Planificación y preparación de la gestión de incidentes de seguridad de la información.
A.5.25 Evaluación y decisión sobre eventos de seguridad de la información.
A.5.26 Respuesta a incidentes de seguridad de la información
A.5.27 Aprendizaje de incidentes de seguridad de la información.
A.5.28 Recopilación de pruebas.
A.6.8 Informes de eventos de seguridad de la información.

Información Documentada revisada

PRO GSI 020 Gestión de incidentes versión 7 enero 2024

Descripción de la Evaluación

A.5.24 PLANIFICACIÓN Y PREPARACIÓN DE LA GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN.
PRO GSI 020 Gestión de incidentes versión 7 enero 2024
Se puede levantar reporte de incidentes en cualquier momento al correo soporte@cia.mx
A.5.25 EVALUACIÓN Y DECISIÓN SOBRE EVENTOS DE SEGURIDAD DE LA INFORMACIÓN.| A.5.26 RESPUESTA A INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN
Loa hallazgos que derivados de la realización y/ desarrollo de sus actividades y uso de activos (equipos, redes aplicaciones, servidores bases de datos entre otros) haga el proveedor o contratista para la organización y considere que potencialmente el hallazgo, suceso o situación que se le presenta, puede vulnerar la seguridad de la información de acuerdo con el alcance del SGSI definido.
Ante cualquier incidente de seguridad de la información se deberá emprender acciones inmediatas que mitiguen de manera parcial o total las afectaciones de acuerdo con los tiempos de solución establecidos
En caso de ser incidente relevante se deberán emprender acciones adicionales y verificación de estas mismas de acuerdo con el formato de incidentes de SI-FOR-GSI-024
Se considera como relevante aquellos incidentes que tengan un impacto directo en algún aspecto de seguridad de la información
Disponibilidad
Cuando la afectación haya excedido el tiempo de respuesta establecido y se haya tenido afectaciones consideradas a los procesos
integridad: ante cualquier evento que afecta a este aspecto de la seguridad de la información
Confidencialidad: ante cualquier evento que afecte a este aspecto de la seguridad de la información
A.5.27 APRENDIZAJE DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN. | A.5.28 RECOPILACIÓN DE PRUEBAS.
Se realiza patrones de conducta con el aplicativo centinela ONE XDR

- Se revisan log periódicamente
- Se muestra procedimiento de afectación de ransomware
- Se muestra reporte enviado a Banorte y alta dirección
- Se muestra procedimiento de mitigación
- 18 diciembre 2023 fecha de afectación
- Carta enviada enero 2024
- Se realiza análisis forense | SCITUM

- Se procede a realiza análisis de inteligencia de amenazas
- Se procede a comprar centinela
- 6 meses se realiza análisis de vulnerabilidades
- Se muestra mayo 2024 análisis de vulnerabilidades
- 59 informativos
- 0 | altos medios bajos
- Nessus

A.6.8 INFORMES DE EVENTOS DE SEGURIDAD DE LA INFORMACIÓN.
Se identificó el documento PRO GSI 020 Gestión de incidentes versión 7 enero 2024
Cada personal que presento un incidente debe notificarlo al área de Sistemas a través de:
Portal de Soporte (CIA-DESK)
• Liga del Portal http://ciadesk.ciac.mx:8080/helpdesk/
• Enviar correo electrónico a soporte@ciasc.mx
Llamada Telefónica a las extensiones 169,170,179
Horario de Respuesta de Lunes a viernes de 7:00 a 22:00 horas y sábado de 7:00 a 14:00
Se cuenta con 15 días para responder las incidencias.

Resultado de la Evaluación:	Conforme
Auditor:	David Abraham Nieto López

Proceso / Servicio:	**CONTROLES ORGANIZACIONALES PROVEEDORES**
Departamento, Área o Unidad de Negocio:	Gerente Administrativo Coordinador Ti
Personal Relacionado:	Salvador Santiago Araujo Rafael Fernando Mendoza Loza

Elementos normativos relacionados

A.5.19 Seguridad de la información en relación con proveedores
A.5.20 Abordaje de la seguridad de la información dentro de los acuerdos de proveedores
A.5.21 Gestión de la seguridad de la información en la cadena de suministro de las TIC
A.5.22 Seguimiento, revisión y gestión del cambio de los servicios de los proveedores
A.5.23 Seguridad de la información para uso de servicios en la nube

Información Documentada revisada

Proveedores PRO-GSI-030 enero 2024 versión 6

Descripción de la Evaluación

A.5.19 SEGURIDAD DE LA INFORMACIÓN EN RELACIÓN CON PROVEEDORES | A.5.20 ABORDAJE DE LA SEGURIDAD DE LA INFORMACIÓN DENTRO DE LOS ACUERDOS DE PROVEEDORES | A.5.21 GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN EN LA CADENA DE SUMINISTRO DE LAS TIC | A.5.22 SEGUIMIENTO, REVISIÓN Y GESTIÓN DEL CAMBIO DE LOS SERVICIOS DE LOS PROVEEDORES
Proveedores PRO-GSI-030 enero 2024 versión 6
Mitigación de riesgos a los activos critica de la información
Se estipula en el contrato serie de lineamientos para su seguridad
Convenio de confidencialidad
Requisitos de seguridad
Se tiene estipulado en los servicios
Se declara no tiene acceso a información remota ni física
Protección de datos personales
Región de incidentes y SLA

Contrato con proveedores cuenta restricciones de acceso
Internet y equipos de computo
Control de provisión de servicios
Se realiza de forma periódica evaluación
Cambio de proveedor | evaluación de lo ocurrido

- Contrato de arrendamiento de DIGICOPIAS arrendamiento laptops
- Protección de datos personales | se estipula que no podrá resguardar ni contar con información imágenes del cliente
- Se debe correr y sobre escribir datos una vez finalizado el servicio
- Se muestra sanciones en caso de no cumplir con las clausulas
- Se muestra firmas 11 abril 2021
- Se muestra Convenio de confidencialidad
- 21 abril 2022

- Se muestra contrato de teléfonos de México SA de CV
- Convenio de confidencialidad
- Transferencia de la información
- Sanciones
- Decima quinta confidencialidad
- 18 agosto 2014
- Se muestra convenio de confidencialidad de Telmex
- 21 abril 2020

- REVZEN
- Aviso de confidencialidad y servicios
- Confidencialidad
- Protección de datos
- Se muestra firmas
- Mayo 2021

FOR-COM 004 evaluación de proveedores

- Se muestra evaluación de proveedor de teléfonos de México
- De fecha 01/08/2024
- Calificación 50
- Comentarios
- Buena atención
- Mayo de 35 puntos se mantiene
- Menor se descarta

- Se muestra evaluación de REVZEN GROUP SA de CV
- Calificación de 50
- 01 /08/2024

- Se muestra evaluación de DIGICOPIAS
- Calificación de 46
- 01 /08/2024

Oportunidad de mejora considerar integrar en la evaluación de proveedores, preguntas relacionadas a la seguridad de la información

Los requisitos de seguridad de la información con los proveedores se encuentran estipulados en los contratos de prestación de servicios que se negocia y firma con cada uno de ellos.
Asimismo, se declara que los proveedores no tienen acceso a la información crítica de forma remota ni física.
En los contratos, y en caso de ser necesario, se estipulan los requisitos legales, la protección de datos personales, los derechos de propiedad intelectual y de autor.
Se establecen el procedimiento para la Gestión de incidentes PRO GSI 020 y los acuerdos

SLA con el proveedor.
Se solicita la siguiente documentación:
Comprobante de domicilio.
◦ RFC.
◦ Identificación oficial del representante legal.
◦ Poder notarial.
◦ Acta constitutiva.

Los proveedores son controlados y supervisados mediante las siguientes acciones:
◦ Respecto al servicio proporcionado por el proveedor, se lleva a cabo de forma periódica una evaluación sobre el servicio y la calidad del mismo, de acuerdo con lo estipulado en el Mapa de proceso Compras MAP COM 001.
◦ Para los incidentes de seguridad de la información detectados se solicitarán acciones inmediatas al proveedor del servicio en cuestión y en caso de ser necesario se someterá con Dirección la posibilidad del cambio de proveedor, realizando una evaluación de lo ocurrido y de las cláusulas de rescisión del contrato.
Se estipula en los contratos con los proveedores que se requiera, los mecanismos mediante los cuales se reportarían los cambios y mejoras de los servicios provistos que puedan llegar a tener impacto directo en la operación, estos deben ser aceptados previos a su implementación.

Los proveedores son controlados y supervisados mediante las siguientes acciones:
• Respecto al servicio proporcionado por el proveedor, se lleva a cabo de forma periódica una evaluación sobre el servicio y la calidad del mismo, de acuerdo con lo estipulado en el Mapa de proceso Compras MAP COM 001.
◦ Para los incidentes de seguridad de la información detectados se solicitarán acciones inmediatas al proveedor del servicio en cuestión y en caso de ser necesario se someterá con Dirección la posibilidad del cambio de proveedor, realizando una evaluación de lo ocurrido y de las cláusulas de rescisión del contrato.
◦ Se estipula en los contratos con los proveedores que se requiera, los mecanismos mediante los cuales se reportarían los cambios y mejoras de los servicios provistos que puedan llegar a tener impacto directo en la operación, estos deben ser aceptados previos a su implementación.

A.5.23 SEGURIDAD DE LA INFORMACIÓN PARA USO DE SERVICIOS EN LA NUBE
Numeral excluido Aceptado

Resultado de la Evaluación:	Conforme
Auditor:	David Abraham Nieto López

PROGRAMA DE AUDITORÍA

FORCSG-P12.31.7	Organización:	CONSULTORES E INVESTIGADORES EN ADMINISTRACIÓN S.C. AEQUITAS ADMINISTRADORA DE ACTIVOS S.R.L. DE C.V.CIA INTEGRACIÓN EN ADMON S.R.L. DE C.V.			
	Tipo de vigilancia:	ANUAL			
	Número de vigilancia:	RENOVACION	1RA VIGILANCIA	2DA VIGILANCIA	RENOVACIÓN
	Mes:	sep-24	sep-25	sep-26	sep-27
	Porcentaje de Auditoría Remota:	PRESENCIAL	POR DEFINIR	POR DEFINIR	POR DEFINIR
	Áreas a revisar:	'Estipulados en el plan de auditoria de cada ejercicio			
	Sitios a revisar:	Sede: Lago Xochimilco No. 283, Ampliación General Vicente Villada, Nezahualcóyotl, C.P. 57760, Edo. De México. Sitio1: Insurgentes Sur 686, despacho 902, colonia del valle, delegación Benito Juárez, ciudad de México, código postal 03100. Sitio 2: Hermenegildo Galeana No. 204, despacho 3, Col. Centro, C.P. 50000, Toluca, Edo. México			
		L-V 9:00 am a 7:00 pm			
		El número de personas dentro del alcance es: 82			
		servicios de investigación de crédito			
	Alcance del Sistema de Gestión:	Los servicios de investigación de crédito (referencias comerciales, verificación de propiedad y sociedades en el RPPYC), recuperación de cartera (extrajudicial y judicial), cobranza punta-punta y gestión domiciliaria, soportado por los procesos de sistemas, compras, recursos humanos, contabilidad y tesorería. De acuerdo con la declaración de aplicabilidad (SoA) LIS GSI 007, versión 10, de Septiembre 2024.”			
	Procesos o actividades a revisar:	Los Incluidos en el Sistema de Gestión			
REQUISITOS DE NYCE					
Revisión del cumplimiento del reglamento de uso de marca y logo NYCE, Acreditaciones emitidas, IAF, ISO		✓	✓	✓	✓
Revisión de hallazgos previos			✓	✓	✓
Quejas, cambios en los requisitos de certificación o legales		✓	✓	✓	✓
CONTEXTO DE LA ORGANIZACIÓN	ISO/IEC 27001:2022				
Comprensión de la organización y su contexto	4.1	✓	✓	✓	✓
Comprensión de las necesidades y expectativas de las partes interesadas	4.2	✓	✓	✓	✓
Determinación del alcance del sistema de gestión	4.3	✓	✓	✓	✓
Sistema de Gestión	4.4	✓	✓	✓	✓
LIDERAZGO					
Liderazgo y Compromiso	5.1	✓	✓	✓	✓
Revisión por la dirección	9.3	✓	✓	✓	✓
OBJETIVOS DEL SG Y PLANIFICACIÓN PARA LOGRARLOS					
Establecer objetivos	6.2	✓	✓	✓	✓
Plan para el logro de objetivos	6.2	✓	✓	✓	✓
Acciones para abordar riesgos y oportunidades	6.1	✓	✓		✓
Planificación de los cambios	6.3	✓	✓		✓

POLÍTICAS DEL SISTEMA DE GESTIÓN					
Establecimiento de la política	5.2	✓	✓		✓
Comunicación de la política de gestión	5.2	✓	✓		✓
Políticas de seguridad de la información | Políticas para la seguridad de la información / Revisión de políticas de seguridad de la información.	A.5.1	✓	✓		✓
ORGANIZACIÓN INTERNA, PLANIFICACIÓN Y CONTROL OPERACIONAL					
Roles, responsabilidades y autoridades de la organización	5.3	✓	✓	✓	✓
Funciones y responsabilidades de seguridad de la información | Roles y responsabilidades para la seguridad de la información	A.5.2	✓	✓		✓
Segregación de responsabilidades | Segregación de tareas	A.5.3	✓	✓		✓
Contacto con autoridades	A.5.5	✓		✓	✓
Contacto con grupos de especial interés	A.5.6	✓		✓	✓
Seguridad de la información en gestión de proyectos | Seguridad de la información en la administración de proyectos / Análisis y especificación de requisitos de seguridad	A.5.8	✓	✓	✓	✓
Uso aceptable de la información y otros activos asociados | Uso aceptable de los activos / Manejo de activos	A.5.10	✓	✓		✓
Dispositivos de punto final de usuario | Política de dispositivos móvil	A.8.1	✓		✓	✓
Teletrabajo	A.6.7	✓	✓	✓	✓
Inteligencia de amenazas	A.5.7	✓	✓	✓	✓
Seguridad de la información para el uso de servicios en la nube	A.5.23	✓	✓	✓	✓
Recursos	7.1	✓	✓	✓	✓
Planificación y control operacional	8.1	✓	✓	✓	✓
INFORMACIÓN DOCUMENTADA					
Generalidades	7.5.1	✓	✓		✓
Creación y actualización	7.5.2	✓	✓		✓
Control de la información documentada	7.5.3	✓	✓		✓
EVALUACIÓN DEL DESEMPEÑO					
Seguimiento, medición, análisis y evaluación	9.1	✓	✓	✓	✓
AUDITORÍA INTERNA Y MEJORA CONTINUA					
Cumplimiento de políticas, reglas y estándares de seguridad de la información | Cumplimiento con políticas y normas de seguridad	A.5.36	✓	✓	✓	✓
Auditoria interna	9.2	✓	✓	✓	✓
No conformidad y acción correctiva	10.2	✓	✓	✓	✓
Mejora continua	10.1	✓	✓	✓	✓
RECURSOS HUMANOS Y COMPETENCIA					
Competencia	7.2	✓	✓		✓
Chequeo | Investigación	A.6.1	✓	✓		✓
Términios y condiciones del empleo	A.6.2	✓	✓		✓
Responsabilidades de gestión | Responsabilidades de la Dirección	A.5.4	✓		✓	✓
Conciencia, educación y capacitación en seguridad de la información	A.6.3	✓	✓		✓
Proceso diciplinario	A.6.4	✓	✓		✓
Responsabilidades en la terminación o cambio de empleo	A.6.5	✓	✓		✓

TOMA DE CONCIENCIA Y COMUNICACIÓN					
Comunicación	7.4	✓		✓	✓
Toma de conciencia y entrevistas con el personal	7.3	✓		✓	✓
Revisión de seguridad en equipos	Varios	✓		✓	✓
GESTIÓN DE ACTIVOS Y GESTIÓN DE LA CONFIGURACIÓN					
Inventario de información y otros activos asociados, Gestión del activo | Inventario de activos / Propiedad de los activos | Gestión del activo	A.5.9	✓	✓		✓
Devolución de activos	A.5.11	✓	✓		✓
Clasificación de la información	A.5.12	✓	✓		✓
Etiquetado de la información	A.5.13	✓	✓		✓
Medios de almacenamiento | Gestión de medios removibles / Disposición medios / Transferencia de medios físicos / Retiro de activos	A.7.10	✓	✓		✓
Gestión de la configuración	A.8.9	✓	✓		✓
Eliminación de la información	A.8.10	✓	✓	✓	✓
Enmascaramiento de datos	A.8.11	✓	✓	✓	✓
Prevención de la fuga de datos	A.8.12	✓	✓	✓	✓
GESTIÓN DE RIESGOS					
Valoración de riesgos	6.1.1, 6.1.2. 8.1, 8.2	✓	✓	✓	✓
Tratamiento de riesgos	6.1.3, 8.3	✓	✓	✓	✓
GESTIÓN DE PROVEEDORES					
Seguridad de la información en las relaciones con los proveedores | Política de seguridad de la información en las relaciones con los proveedores	A.5.19	✓	✓	✓	✓
Abordar la seguridad de la información dentro de los acuerdos con proveedores	A.5.20	✓	✓		✓
Gestión de la seguridad de la información en la cadena de suministro de las TIC | Cadena de suministro de tecnología de la información y de las comunicaciones	A.5.21	✓	✓		✓
Seguimiento, revisión y gestión del cambio de los servicios de los proveedores | Monitoreo y revisión de los servicios de proveedores / Gestión de cambios a los servicios de proveedores	A.5.22	✓	✓		✓
ASEGURAMIENTO DE LOS SERVICIOS					
Seguridad de la información durante la interrupción, Incidentes de seguridad de la información | Planeación de la continuidad de la seguridad de la información / Implementando la continuidad de la seguridad de la información / Verificación, revisión y evaluación de la continuidad de la seguridad de la información	5.29	✓	✓		✓
Redundancia de las instalaciones de procesamiento de información | Disponibilidad de las instalaciones de procesamiento de la información	A.8.14	✓	✓		✓
Preparación de las TIC para la continuidad del negocio	A.5.30	✓	✓	✓	✓

ATENCIÓN Y RESOLUCIÓN					
Planificación y preparación de la gestión de incidentes de seguridad de la información | Responsabilidades y procedimientos	A.5.24	✓	✓	✓	✓
Informes de eventos de seguridad de la información | Reporte de eventos de seguridad de la información / Reporte de debilidades de seguridad de la información	A.6.8	✓	✓	✓	✓
Evaluación y decisión sobre los eventos de seguridad de información	A.5.25	✓	✓	✓	✓
Respuesta a incidentes de seguridad de la información	A.5.26	✓	✓	✓	✓
Aprendizaje de los incidentes de seguridad de la información	A.5.27	✓	✓	✓	✓
Recopilación de evidencias	A.5.28	✓	✓	✓	✓
GESTIÓN DEL CAMBIO					
Política de gestión del cambio | Gestión del cambio / Procedimientos de control de cambios a sistemas / Revisión técnica de aplicaciones después de cambios en la plataforma de operación / Restricciones a los cambios en los paquetes de software	A.8.32	✓	✓	✓	✓
Inicio de la gestión del cambio	A.8.32	✓	✓	✓	✓
Actividades de la gestión del cambio	A.8.32	✓	✓	✓	✓
CONTROLES DE SEGURIDAD DE LA INFORMACIÓN					
Controles de seguridad de la información	NA	✓	✓	✓	✓
Identificación de requerimientos legales, estatutarios, regulatorios y contractuales | Identificación de la legislación aplicable y requisitos contractuales / Regulación de controles criptográficos	A.5.31	✓		✓	✓
Derechos de Propiedad Intelectual (DPI)	A.5.32	✓		✓	✓
Protección de los registros de la organización | Protección de registros	A.5.33	✓		✓	✓
Privacidad y protección de la PII | Privacidad y protección de información de identificación personal	A.5.34	✓		✓	✓
Revisión independiente de la seguridad de la información	A.5.35	✓		✓	✓
Cumplimiento de políticas, reglas y estándares de seguridad de la información | Cumplimiento con políticas y normas de seguridad	A.5.36	✓	✓	✓	✓
Gestión de vulnerabilidades técnicas | Gestión de vulnerabilidades técnicas / Inspección de cumplimiento técnico	A.8.8	✓	✓	✓	✓

Control de acceso | Política de control de acceso / Acceso a las redes y los servicios de la red	A.5.15	✓	✓	✓	✓
Gestión de identidades | Registro y cancelación de usuarios	A.5.16	✓	✓	✓	✓
Derechos de acceso | Provisión de acceso de usuarios / Revisión de los derechos de acceso de usuario / Eliminación o ajuste de los derechos de acceso	A.5.18	✓	✓	✓	✓
Derechos de acceso privilegiado | Gestión de derechos de acceso privilegiado	A.8.2	✓	✓	✓	✓
Información de autenticación | Gestión de información secreta de autenticación de los usuarios / Uso de información secreta de autenticación / Sistema de administración de contraseñas	A.5.17	✓	✓	✓	✓
Restricción del acceso a la información	A.8.3	✓	✓	✓	✓
Procedimientos seguros de inicio de sesión | Procedimientos de inicio de sesión seguros	A.8.5	✓	✓	✓	✓
Uso de programas de utilidad privilegiados | Uso de privilegios de los programas de utilidades	A.8.18	✓	✓	✓	✓
Acceso al código fuente | Control de acceso al código fuente de los programas	A.8.4	✓	✓	✓	✓
Entrada física Perímetro de seguridad física	A.7.1	✓	✓		✓
Entrada física | Controles de entrada física / Áreas de entrega y carga	A.7.2	✓	✓		✓
Aseguramiento de oficinas, salas e instalaciones	A.7.3	✓	✓		✓
Protección contra las amenazas externas y ambientales	A.7.5	✓	✓		✓
El trabajo en áreas seguras	A.7.6	✓	✓		✓
Emplazamiento y protección de equipos | Ubicación y protección de equipo	A.7.8	✓	✓		✓
Instalaciones de suministro | Servicios públicos	A.7.11	✓	✓		✓
Seguridad del cableado	A.7.12	✓	✓		✓
Mantenimiento de los equipos	A.7.13	✓	✓		✓
Seguridad de los equipos y activos fuera de las instalaciones	A.7.9	✓	✓		✓
Reutilización o eliminación segura de equipos	A.7.14	✓	✓		✓
Dispositivos de punto final del usuario | Equipo de usuario desatendido	A.8.1	✓	✓		✓
Escritorio limpio y pantalla limpia | Política de pantalla y escritorio limpio	A.7.7	✓	✓		✓
Supervisión de la seguridad física	A.7.4	✓	✓		✓
Seguridad de redes | Controles de red	A.8.20	✓	✓	✓	✓
Seguridad de los servicios de red	A.8.21	✓	✓	✓	✓
Segregación en redes	A.8.23	✓	✓	✓	✓
Transferencia de información | Políticas y procedimientos de transferencia de información / Acuerdos de transferencia de información / Mensajería electrónica	A.5.14	✓	✓	✓	✓
Acuerdos de confidencialidad o no divulgación	A.6.6	✓	✓	✓	✓
Filtrado Web	A.8.22	✓	✓	✓	✓
Uso de Criptografía | Política sobre el uso de controles criptográficos / Gestión de llaves	A.8.24	✓	✓		✓
Documentación de procedimientos operacionales	A.5.37	✓	✓	✓	✓

Gestión de capacidades	A.8.6	✓	✓	✓	✓
Separación de ambientes de desarrollo, prueba y producción | Separación de ambientes de desarrollo, prueba y producción / Entorno de Desarrollo seguro	A.8.31	✓	✓	✓	✓
Controles contra el código malicioso	A.8.7	✓	✓	✓	✓
Copias de seguridad de la información | Respaldos de la información	A.8.13	✓	✓	✓	✓
Registro | Registro de eventos / Protección de la información del registro / Registros del administrador y operador	A.8.15	✓	✓	✓	✓
Sincronización del reloj	A.8.17	✓	✓	✓	✓
Instalación de software en sistemas operativos | Instalación de software en sistemas operativos / Restricciones en la instalación de software	A.8.19	✓	✓	✓	✓
Protección de los sistemas de información durante las pruebas de auditoría | Controles de auditoría de sistemas de información	A.8.34	✓	✓	✓	✓
Monitoreo de actividades / Actividades de seguimiento	A.8.16	✓	✓		✓
Requisitos de seguridad de las aplicaciones | Servicios de aplicaciones seguras en redes públicas / Protección de aplicaciones de servicios de transacciones	A.8.26	✓	✓	✓	✓
Ciclo de vida de desarrollo seguro | Política de desarrollo seguro	A.8.25	✓	✓	✓	✓
Arquitectura de sistemas seguros y principios de ingeniería | Principios de ingeniería en sistemas seguros	A.8.27	✓	✓	✓	✓
Desarrollo de sistemas subcontratado (outsourcing)	A.8.30	✓	✓	✓	✓
Pruebas de seguridad en el desarrollo y aceptación | Pruebas de seguridad a los sistemas / Pruebas de aceptación a los sistemas	A.8.29	✓	✓	✓	✓
Protección de los datos de prueba	A.8.33	✓	✓	✓	✓
Codificación Segura	A.8.28	✓	✓	✓	✓

Nivel de eficacia	Alto
Desempeño del Sistema de Gestión	Alto
Modificaciones al Programa	Se Genero una transición de norma del esquema ISO/IEC27001:2022 en Septiembre 2024

Notas: 1. Para auditorías de etapa 1, donde se tenga tiempo limitado, es aceptable revisar los elementos, capítulos y/o numerales siguientes: no aplicabilidades, capítulo 4, numeral 5.2, 6.1, 6.2, 8.1, 8.2, 9.2, 9.3

2. La determinación del programa de auditoría y cualquier modificación subsiguiente deben tener en cuenta el tamaño de la organización cliente, el alcance y la complejidad de su sistema de gestión, los productos y procesos, así como el nivel demostrado de eficacia del sistema de gestión y los

3. Dependiendo de los criterios de auditoría se podrán eliminar las columnas y/o filas de las normas de referencia no aplicables en la evaluación.

CONCLUSIONES	
Fortalezas	Durante la evaluación se demostró el compromiso de la alta dirección y de todo el personal entrevistado. El personal conoce sus actividades y cuenta con alto nivel de especialización La organización tiene buena comunicación para la atención y mejora de su SGSI
Áreas de mejora	A.7.13 Mantenimiento de equipos: Revisar que se usen los Formatos Actuales en los Mantenimientos de Equipos en los Diferentes Sitios. A.8.6 Gestión De Capacidad: Fortalecer y definir lumbrales de capacidades internos para documentar límites aceptables de operatividad A.5.22 Monitoreo revisión y gestión del cambio de los servicios de los proveedores: Considerar integrar en la evaluación de proveedores, preguntas relacionadas a la seguridad de la información.
Quejas	La organización cuenta con mecanismos para identificar, documentar, dar seguimiento y cierre a las quejas.
Uso de marca	La organización emplea el logo como organización certificada en Portadas de Documentos Internos
Información para la próxima evaluación	La próxima auditoría es de Vigilancia 1, Sep. 2025 y debe solicitarse de acuerdo con el programa de auditoría. El número de personal de la organización es de: 82 Se confirma que existen condiciones adecuadas para realizar auditorías vía remota considerando la disponibilidad de información, la posibilidad de realizar recorridos virtuales entre otros.
Requisitos necesarios	Ninguno
Información técnica de los Sistemas de Gestión Evaluados	**Alcance:** Indicar si el alcance y sector es adecuado El alcance del Sistema de Gestión se considera adecuado **Código IAF(s) y NACE(s)** IAF: 35 **Objetivos** Se cumplieron los objetivos de esta evaluación. En caso de ser auditoría remota especifique si fue posible cumplir los objetivos en modalidad remota **Aplicabilidad de requisitos y/o controles** De acuerdo con el documento : Declaración de Aplicabilidad (SoA) LIS GSI 007, versión 10, de Septiembre 2024 La organización aplica los 91 controles de la norma de referencia, Exclusiones Aceptadas A.5.23 Seguridad de la información para el uso de servicio en la nube A.8.30 Desarrollo externalizado **Renovaciones** Se revisaron los informes de auditoría del ciclo de certificación y se confirmó que el nivel de madurez y desempeño mostrado
Revisión de requisitos legales e incidentes graves para SGSST	N/A
Grado de eficacia mostrado	*Sistema de Gestión: Alto* *Auditoría interna: Alto.* *Revisión por la dirección: Alto*
Comentarios del equipo auditor	**RECOMENDACION** De acuerdo al análisis mostrado en este informe, el equipo auditor recomienda **RENOVACIÓN y la RESTAURACIÓN** la certificación del Sistema de Gestión de Seguridad de la Información de **CONSULTORES E INVESTIGADORES EN ADMINISTRACIÓN S.C. AEQUITAS ADMINISTRADORA DE ACTIVOS S.R.L. DE C.V.CIA INTEGRACIÓN EN ADMON S.R.L. DE C.V.** evaluado bajo las norma **ISO/IEC 27001:2022**
Modificaciones realizadas	N/A

PERSONAL QUE REALIZÓ LA EVALUACIÓN

Karina Alonso Sánchez Auditor Líder	David Abraham Nieto López Auditor

ACEPTACIÓN DEL INFORME

Irais Dafne Mendoza Sánchez.

Director: General Adjunta

Notas

1. A la firma del presente informe se da por entendido que el contenido de éste ha sido aclarado y entendido por el solicitante y sus representantes.
2. La auditoría fue realizada mediante un muestreo, lo que implica que no se garantiza el no encontrar no conformidades en futuras auditorías.
3. Teniendo en cuenta las no conformidades que se hayan presentado en este informe, el solicitante se compromete a presentar a NYCE la documentación y evidencia del cierre de cada una en el plazo indicado en el informe de no conformidades registradas.
4. Para los temas de preocupación, si debido a los resultados de la etapa 1 en la recomendación y conclusiones generales del equipo auditor se indica se deba enviar un plan de acción de los temas de preocupación, se debe proceder así para continuar con la programación de la etapa 2. En caso de que el equipo auditor no indique lo anterior, solo bastará con informar a NYCE por correo electrónico que los temas de preocupación se han atendido conforme a su sistema de gestión sin necesidad de ingresar el plan. En caso de que los temas de preocupación detectados en la etapa 1, no se hayan atendido debidamente existe la posibilidad de que se detecten nuevamente y se escalen a no conformidad en la etapa 2.
5. Para las observaciones y temas de preocupación no es necesario se ingrese información de su atención a NYCE, pero sí de atenderlas conforme a su sistema de gestión debido a que si en una próxima auditoría se detectan nuevamente se escalarán estos hallazgos a no conformidad.
6. El solicitante deberá considerar recibir su auditoría de renovación 90 días naturales antes del término de la vigencia de su certificado de registro de empresa con la finalidad de que, en caso de que se detecten hallazgos clasificados como no conformidades se dé oportunidad de este tiempo para atender dichos hallazgos.
7. Para las organizaciones que tengan un alcance con multisitio, la relación de todos los sitios que se incluyen en la totalidad del alcance se puede presentar en formato libre (Word o Excel) pero con los datos completos de cada domicilio del sitio y se anexará a este informe como parte integral del mismo. En caso de tener sitios temporales es importante señalarlos como tal en esta relación.
8. Para el alcance en idioma inglés, será necesario que la organización lo envíe por correo electrónico al contacto de logística, con el fin de liberar los certificados que lleguen a emitirse.
9. Este informe debe rubricarse en todas sus páginas, o mediante firma electrónica en la totalidad del documento, por el representante auditado y por el grupo auditor.
10. La información que se obtenga durante el proceso de auditoría será tratada de forma confidencial.

11. Para cualquier queja, apelación o aclaración comunicarse con: Gerente Corporativo de la Calidad Tel. +52(55) 12045190 ext. 423, correo: ncanuto@nyce.org.mx, Directora Técnica y de Certificación, Tel. +52(55) 1204 5190 ext. 402, correo: lcampos@nyce.org.mx