1. COMPROMISO DE LA DIRECCIÓN

La alta dirección, a través del Director General y de los responsables de las áreas de la organización, se compromete a:

- Establecer, implementar y mantener un sistema de Gestión de Seguridad de la Información, que cumpla con los lineamientos de la norma ISO-IEC-27001:2022, proporcionando los recursos necesarios tanto humanos como financieros y considerando el costo-beneficio y los criterios de riesgo de la organización.
- Impulsar la mejora continua en materia de seguridad de la información en todas las operaciones relevantes de la organización.
- Asegurar el cumplimiento de los requerimientos de las autoridades, de los clientes y de las partes interesadas en materia de Seguridad de la Información.
- Supervisar el cumplimiento de las Políticas internas de Seguridad de la información y las Políticas o directrices relacionadas.

2. POLÍTICA DE LA SEGURIDAD DE LA INFORMACIÓN

2.1. Enunciado general

La organización implementará, mantendrá y mejorará de manera continua un Sistema de Gestión de Seguridad de la Información basado en la norma ISO-27001:2022. Este sistema procurará mantener controles adecuados para mitigar los riesgos de seguridad de la información y así proteger la confidencialidad, la integridad y la continuidad de la información en todas las áreas tanto de servicios internos como de las diferentes unidades de negocio.

2.2. Alcance

Los responsables de las áreas internas y unidades de negocio incluidas en el alcance del sistema de gestión de seguridad de la información deberán conocer, entender y cumplir con todos los requisitos y procesos del sistema de gestión de seguridad de la información en sus áreas de responsabilidad.

2.3. Vigencia.

Esta política entra en vigor el 6 de Julio del 2023 y se revisará al menos 1 vez cada 12 meses o cuando haya cambios relevantes en el contexto de la organización.

2.4. Difusión.

Todos los documentos, políticas, procedimientos, registros relevantes y actividades relacionadas con el SGSI, se difundirá a todos los colaboradores de la organización, así como al resto de las partes interesadas (Clientes clave, proveedores clave, consejo de administración), con base en su nivel de involucramiento en el sistema mismo.

2.5. **Gestión de riesgos**

Los órganos de alta dirección y supervisión deberán garantizar que la gestión de riesgos esté integrada en todas las actividades organizativas y demostrar liderazgo y compromiso

El proceso deberá ejecutarse por cada una de las áreas o unidades de negocio en el alcance del SGSI una o varias veces en el año, dependiendo de la criticidad del nivel de riesgo de la entidad o cuando se presenten cambios relevantes en los contextos internos y externos.

Los riesgos, procesos o actividades que serán catalogados con alta materialidad para su tratamiento deberán ser aprobados por el responsable de riesgo, control y cumplimiento.

La frecuencia de ejecución del proceso deberá ser establecida por el responsable del área o unidad de negocio con la aprobación del Oficial de Seguridad de la Información.

2.6. **Responsabilidades:**

a. **Comité de Seguridad de la Información**

   Es el responsable, sin reserva alguna de:

   - La seguridad de la información de la organización.
   - Definir los objetivos estratégicos de seguridad de la información.
   - El proceso y la administración de la Seguridad de la Información.
   - Políticas y directrices complementarias a la presente política.
   - Desarrollar estrategias y conceptos de la Seguridad de la Información

b. **Alta dirección**

   La dirección general y/o la comisión de seguridad de la información en el consejo de administración son los responsables de revisar y aprobar los objetivos, estrategias y políticas de Seguridad de la Información en la organización.

c. **Colaboradores**

   Todos los colaboradores son responsables de cumplir con los lineamientos de seguridad de la información y con cualquier reglamento relacionado; y son responsables de reportar cualquier riesgo o incidente de seguridad de la información detectado.

d. **Proveedores**

   Los proveedores deben cumplir con esta política y cualquier reglamento relacionado.

2.7. **Sistemas de Gestión de servicios.**

Todos los sistemas de gestión de servicios en las unidades de negocio o departamentos internos de la organización se alinearán a esta política.

2.8. Políticas (directrices) complementarias a esta política

Como parte del Sistema de Gestión de Seguridad de la Información se han publicado directrices específicas a los diferentes temas relevantes a la seguridad de la información. Estas directrices forman parte integral del sistema y deberán ser cumplidas por todos los colaboradores de la organización.

3. OBJETIVOS DE SEGURIDAD DE LA INFORMACIÓN

La organización planifica, establece y emite objetivos de seguridad de la información para las funciones y niveles pertinentes.

3.1. Normas y Leyes:

- Asegurar el cumplimiento de la Ley de Protección de Datos Personales mexicana
- Mantener la certificación de la norma ISO 27001-2022

3.2. Roles y Facultades:

- Gestionar de forma controlada la identidad, roles y facultades de los usuarios de las aplicaciones críticas y ambientes de desarrollo.
- Gestionar que la información confidencial tanto interna como de nuestros clientes, sea manejada de acuerdo a los requisitos establecidos.

3.3. Adopción

- Lograr que el SGSI sea adoptado de manera efectiva por cada una de las áreas incluidas en el alcance del sistema

3.4. Requisitos Contractuales

- Mantener el cumplimiento de los requisitos contractuales de nuestros clientes

3.5. Nivel de exposición al riesgo:

- Mantener un nivel de exposición al riesgo aceptable de acuerdo a los criterios de riesgo establecidos
- Mantener una alta eficacia en el tratamiento de los riesgos a través de la ejecución de controles

3.6. Incidentes de Seguridad de la Información

- Establecer y mantener un proceso de gestión de incidentes que permita prevenir la recurrencia y mitigar los riesgos.

Nota:

En el documento DOC-SSI-008 "Evaluación del desempeño", se mencionan los siguientes puntos relativos a los objetivos:

- Recursos requeridos
- Responsable de cada objetivo

- Lo que se hará para lograrlos
- Fecha esperada para lograrlos
- Forma de evaluar los resultados

4. ESTRUCTURA DE ORGANIZACIÓN DE SEGURIDAD DE LA INFORMACIÓN.

En el documento DOC-SSI-006 "Funciones, Responsabilidades y autoridades de la Organización en el Sistema de Gestión de Seguridad de la Información" se detalla cada uno de los roles que participan en el Sistema de Gestión de Seguridad de la Información.

1. PROCEDIMIENTO PARA LA GESTIÓN DE INCIDENTES DE SI

1.1. Funciones y responsabilidades

ACTIVIDADES	ROLES			
	Colaboradores, proveedores y partes interesadas	Comité de SI	Equipo de respuesta a incidentes	OSI
Detección y notificación	R	C	C	A
Evaluación y registro	I	I	C	R
Respuesta a los incidentes	I	I	R	A
Escalamiento	I	I	R	A
Lecciones aprendidas	I	C	R	A
Cierre del incidente	I	I	R	A

R = Responsable

A = Aprueba

C = Consulta

I = Informa

1.2. Detección y notificación

- Las personas que detecten o sospechen de algún evento en materia de seguridad de la información, deberán notificarlo de forma inmediata a través del proceso de bitrix "Kiosko de Seguridad de la Información", o a través del servicio 911. La notificación desde el proceso de bitrix, puede ser "anónima" o personalizada.
- Se entiende por evento de seguridad de la información: suceso que indica una posible violación de la seguridad de la información (confidencialidad, disponibilidad o integridad) o un fallo de los controles.
- Si la persona que detectó el evento, considera que requiere de un nivel mayor de confidencialidad puede contactar directamente con el OSI y reportarlo vía telefónica para recibir tratamiento como reporte anónimo.
- Todos los eventos adversos que sean registrados en las distintas plataformas deberán ser revisados por el Oficial de Seguridad de la Información para identificar si se trata de un incidente de seguridad de la información y actuar en consecuencia.

1.3. Evaluación y registro

- El Oficial de Seguridad de la Información revisará los registros de eventos reportados a través de los distintos canales y determinará:
    - Si es correcto clasificarlo como un incidente de seguridad de la información.
    - El nivel de impacto, con la posible consulta al Comité de Seguridad de la Información de acuerdo a los siguientes criterios:

Impacto 1	Pone en riesgo la totalidad de las operaciones de la empresa
Impacto 2	Pone en riesgo a uno o varios clientes importantes
Impacto 3	Pone en riesgo alguna actividad clave de la empresa
Impacto 4	Incumplimiento de alguna política de seguridad de la información que podría afectar alguna actividad de la empresa

- Deberá asegurarse que el incidente sea registrado en el proceso de bitrix "Kiosko de Seguridad de la Información".

1.4. Respuesta a los eventos de seguridad de la información.

- El Oficial de Seguridad de la Información se encargará de determinar la persona o grupo de personas que deberán ejecutar las acciones a llevar a cabo. Para ese efecto llenarán los campos correspondientes en bitrix y enviarán el flujo al responsable de la acción.
- El equipo de respuesta a incidentes será notificado formalmente de sus funciones y responsabilidades.
- La persona asignada recibirá la notificación de asignación y deberá registrar las acciones que llevará a cabo, incluyendo acciones de recuperación (correctivas) y un plan de prevención.
- El responsable asignado deberá realizar una consulta a las lecciones aprendidas de eventos anteriores que pueda utilizar como apoyo para determinar las acciones a tomar o evaluar el incidente.
- El líder del equipo de respuesta a incidentes deberá identificar la evidencia a ser recopilada para cada evento y deberá solicitar a las partes involucradas los documentos, registros de incidentes, información de bitácoras, pruebas ejecutadas u otras evidencias que demuestran que ocurrió el evento.
- El Oficial de Seguridad de la Información deberá aprobar las acciones a realizar y las evidencias recopiladas.

1.5. Escalamiento

- Se entiende por escalamiento funcional el notificar a los responsables, que por su función le corresponde atender un evento o incidente de seguridad de la información.
- Se tiende por escalamiento jerárquico el notificar al comité de seguridad de la información y a la Alta Dirección sobre la ocurrencia de eventos o incidentes de seguridad de la información.

1.5.1 Escalamiento de Eventos de seguridad de la información

  - Cuando un evento de seguridad de la información, en opinión del oficial de seguridad de la información, tiene alta probabilidad de convertirse en incidente, este será escalado jerárquicamente al comité de seguridad.

- Cuando el evento corresponde a otros con características similares que se han presentado de manera recurrente, también será escalado jerárquicamente al comité de seguridad.

1.5.2 Escalamiento de Incidentes de seguridad de la información

- Una vez que el evento es evaluado y clasificado como incidente de seguridad de la información se lleva a cabo el escalamiento funcional al líder del equipo de respuesta de incidentes para iniciar el tratamiento del incidente informado. A su vez, emitirá escalamientos funcionales a las personas que conformarán el equipo de respuesta a incidentes.

- El escalamiento jerárquico cuyo objetivo es mantener informados a los miembros del comité de seguridad de la información y en particular al líder del área al que corresponde el incidente por su naturaleza y área de responsabilidad. El escalamiento jerárquico a la Alta Dirección se realizará cuando se determine que el nivel de impacto se ha clasificado como nivel 1 o 2. Durante la atención del incidente se realizarán escalamientos jerárquicos en los momentos claves de la atención.

- Cuando se trate de un incidente con nivel de impacto 1 se llevará a cabo una reunión con el Comité de Seguridad de la Información y el equipo de respuesta a incidentes en la que se comunicarán los detalles del incidente, las funciones y responsabilidades del equipo de respuesta, los canales de comunicación y la frecuencia de revisión.

1.6. Lecciones aprendidas

- Una vez que completaron las acciones, el responsable llenará el campo de "Lecciones aprendidas" que contenga tanto los síntomas como el aprendizaje obtenido, tomando en cuenta alguno o algunos de los siguientes puntos:
  - Impacto económico o de prestigio incurrido debido al incidente
  - Impacto potencial que podría haber resultado en caso de no atenderse a tiempo
  - Identificar si se trata de un incidente recurrente
  - Controles adicionados o modificados o acciones realizadas para mitigar el riesgo de recurrencia.
  - Cambios generados en el proceso de sensibilización a los colaboradores

- Cuando se trate de un incidente con nivel de impacto 1 se registrarán lecciones aprendidas durante cada sesión de revisión y se convocará una sesión final para validar las lecciones aprendidas que deban detonar uno o varios hallazgos.

1.7. Cierre del incidente

- Cuando se ha concluido con el plan de trabajo y se han registrado las lecciones aprendidas y/o los hallazgos, el responsable deberá enviar a cierre el incidente.
- El OSI recibe la notificación y decide si las acciones mitigan suficientemente el riesgo y aprueba.
- El OSI debe determinar si se requiere hacer un comunicado oficial a una o varias de las partes interesadas (internas o externas) respecto de las acciones llevadas a cabo.

1.8. Recopilación de evidencias:

- Durante la respuesta al incidente se deberá recopilar la evidencia que demuestre que ocurrió el evento y las evidencias de su atención.
- Para el caso en el que una persona cometió o estuvo involucrada en la comisión de un incidente se deberá:
    - Determinar de acuerdo a las evidencias a las personas que deberán ser sancionadas
    - Comunicar y aplicar la sanción a los responsables.
    - Guardar físicamente en el expediente de las personas esta evidencia la cual se le dará un manejo confidencial.
- Todas las evidencias recopiladas se deberán mantener almacenadas por un periodo mínimo de 12 meses.

1.9 Informes a la Dirección

- Los responsables de áreas internas o unidades de negocio, como parte de su presentación trimestral a Dirección, deberán informar:
    - Eventos detectados en el área durante el periodo
    - Incidentes de alto impacto en el área (nivel 1 y 2)
    - Participación en la atención de incidentes de otras áreas
    - Estatus de los eventos de su área.
    - Actividades preventivas
    - Lecciones aprendidas y hallazgos
- El Oficial de Seguridad de la información, como parte del informe trimestral del SGSI deberá presentar:
    - Tiempo de detección
    - Tiempo de respuesta
    - Volumetría de eventos.
    - Incidentes confirmados.
    - Estatus de eventos
    - Incidentes de alto impacto (nivel 1 y 2)
    - Planes de acción más relevantes
    - Capacitación y concientización

INNOVACION Y ADMINISTRACION DE TI S DE RL DE CV

Querétaro - México | Programación informática, consultoría ...

Tamaño de la empresa **M** | Ámbito de evaluación: **Entidad**

Ficha de evaluación | Carbono | Métricas | Plan de acción correctiva | Documentos | Otros

Fecha de publicación: 7 de sep. de 2023 Válida hasta: 7 de sep. de 2024

Desempeño en sostenibilidad: Insuficiente | Parcial | Bueno | Avanzado | Destacado

PUNTUACIÓN GLOBAL

46 / 100

36.º percentil

MEDIO AMBIENTE

30 / 100

Peso

PRÁCTICAS LABORALES Y DERECHOS HUMANOS

50 / 100

Peso

ÉTICA

60 / 100

Peso

PROGRAMA DE AUDITORÍAS

CONTINUUM

Vigencia dle plan: 31/12/2021- 31/12/2024 [5]

Norma	Actividad	Mes	Año	Requisitos a evaluar: De la organización	Requisitos a evaluar: De la Norma	Requisitos de planificación e informes	Plan de auditoría	Alcance	Método de auditoría: Cumplimiento	Método de auditoría: Eficacia	Método de auditoría: Otro	Responsables	Responsabilidades de auditados	Selección de auditores Criterios	Informe (Link)	Revisión por Dirección (Link minuta - VoBo)	
ISO 27001	Auditoría organizacional interna SGSI	Septiembre	2021	☐	☑	1. Notificación con al menos 15 días de anticipación a los involucrados.	03_Listado de Verificación 2021 - Auditoría interna SGSI - Continuum.xlsx	Procesos relacionados a la norma ISO-27001 en las unidades de negocios y departamento.	☑	☐		AA | AGC	Mostrar evidencia y documentación	*Plan de capacitación orientado a proceso de auditoría *Evaluación de conocimientos teóricos	03_Informe de Auditoría Interna SGSI - Agosto 2021	-	
ISO 27001	Auditoría Externa ISO 27001	Diciembre	2021	☐	☑	-	FORCSG-PI 2.2.5 PLAN DE AUD ICORP.docx	Dirección General, Administrativo, Desarrollo Organizacional, Marketing, Venta.	☑	☐		AGC | AA	*Proporcionar los recursos necesarios para permitir al equipo auditor designado verificar el cumplimiento de los requisitos a evaluar. Esto se aplica a todas las instalaciones o sitios dentro del alcance. *Permitir el acceso a la información, los documentos y los registros que permitan la verificación del cumplimiento de los requisitos a evaluar. *Pagar las tarifas establecidas por el organismo.	N/A	E2 INFORME...	-	
ISO 20000	Auditoría qdoc	Febrero	2022	☑	☑	Se estima 1 semana con sesiones remotas para la evaluación. El nivel de implementación del SGS se considera medio.	Listado de Verificación 2022 - Auditoría interna SGS qdoc - Continuum	Catálogo de servicios vigente de qdoc Procesos de gestión organizacionales de qdoc	☑	☐		RT | AA	Mostrar evidencia y documentación	- Independencia - Imparcialidad - Alineado a objetivos	Informe de Auditoría Interna SGS qdoc - Marzo 2022	-	
ISO 20000	Auditoría TI	Febrero	2022	☑	☑	Se estima 1 semana con sesiones remotas para la evaluación. El nivel de implementación del SGS se considera alto. El nivel de madurez del SGS se considera medio.	**Plan de auditoria TI.pdf [1]**	Catálogo de servicios vigente de TI Procesos de gestión organizacionales de TI	☑	☐		JET | AA	Mostrar evidencia y documentación	- Independencia - Imparcialidad - Alineado a objetivos	Informe de Auditoría Interna SGS TI - Marzo 2022	-	
ISO 20000	1ra auditoría de vigilancia SGS TI [2]	Abril	2022	☐	☑	-	**icorp_v1_PLAN DE AUD.docx**	Los servicios de TI de Aplicaciones, Comunicaciones, Gestión e Infraestructura, Monitoreo, Seguridad, Soporte, Telecom y Virtualización de acuerdo al catálogo de servicios DOC-CNS-002, ofrecidos para los usuarios áreas y departamentos internos de ICORP.	☑	☑		JET | AA	Proporcionar los recursos necesarios para permitir al equipo auditor designado verificar el cumplimiento de los requisitos a evaluar. Esto se aplica a todas las instalaciones o sitios dentro del alcance. Permitir el acceso a la información, los documentos y los registros que permitan la verificación del cumplimiento de los requisitos a evaluar. Pagar las tarifas establecidas por el organismo.	na	ICORP_V1_ INFORME DE AUD_04042022.pdf		
ISO 27001	Auditoría interna SGSI	Diciembre	2022	☑	☑	1. Notificación con al menos 15 días de anticipación a los involucrados. 2. Realizar entrega formal del informe.	Listado de Verificación 2022 - Auditoria interna SGSI - Rev	*Cláusulas 8, 9 y 10 *Dominios 6-9, 11-3,14,16 y 18 *Informe de auditoría anterior	☑	☑		MMH | AGC	-Mostrar evidencia de la información solicitada por los auditores. -Dar seguimiento a la resolución de los hallazgos detectados en la auditoría	*Plan de capacitación orientado a eficacia de controles y entendimiento de la norma. *Evaluación práctica para identificar: - Independencia - Imparcialidad - Capacidad de análisis - Alineado a objetivos	03_Informe de Auditoría Interna SGSI - 2022_v1	Minuta - Auditoría interna - Reunión de cierre 2022	
ISO 27001	1ra auditoría de vigilancia SGSI	Febrero	2023	☐	☑	-	FORCSG-PI 2.2.5 PLAN DE AUD 27K 2D Completo.docx	La protección de la información de clientes y proveedores, almacenada en la infraestructura de la organización y procesos o servicios internos de las áreas de tecnología de la información, administración, recursos humanos, ventas, mercadotecnia y unidades de negocio de acuerdo a la declaración de aplicabilidad SGSI -Matriz de aplicabilidad de controles de SI, versión del 14 de diciembre del 2021.	☑	☑		MMH | AGC	*Proporcionar los recursos necesarios para permitir al equipo auditor designado verificar el cumplimiento de los requisitos a evaluar. Esto se aplica a todas las instalaciones o sitios dentro del alcance. *Permitir el acceso a la información, los documentos y los registros que permitan la verificación del cumplimiento de los requisitos a evaluar. *Pagar las tarifas establecidas por el organismo.	N/A	-	NA	
ISO 20000	Auditoria interna TI	Febrero	2023	☐	☑	Se estima 1 semana con sesiones remotas para la evaluación. El nivel de implementación del SGS se considera alto. El nivel de madurez del SGS se considera alto	**Carta de Auditoría SGS TI 2022 [3]**	4.0 Contexto de la organización 6.0 Planificación 7.5 Información documentada 9.0 Evaluación del desempeño 10.0 Mejora Continua 8.2 Relación con el Negocio 8.2.3 Control de las partes involucradas 8.2.4 Catálogo de Servicios 8.3.4 Gestión de Proveedores 8.5.1 Gestión de Cambios 8.6 Resolución y cumplimiento	☑	☐		JET | MMH	Mostrar evidencia y documentación	- Independencia - Imparcialidad - Alineado a objetivos	04_Informe de Auditoría Interna SGS TI - Marzo 2023	Aprobación en el informe de auditoría	
ISO 20000	2da auditoría de vigilancia SGS TI	Marzo	2023	☐	☑	--	**FORCSG-PI 2.2.7 PLAN DE AUD INNOVACIÓN V2.docx**	Servicios de TI de Aplicaciones, Comunicaciones, Gestión de Infraestructura, Monitoreo, Seguridad, Soporte, Telecom y Virtualización de acuerdo al Catálogo de Servicios TI., ofrecidos para usuarios de las áreas y departamentos internos de icorp.	☑	☐		JET | MMH	--	--	Complete_con_ DocuSign_ICORP_20000-1_TA_FORCS.pdf	Informe firmado a través de DocuSign por el responsable del SGS	
ISO 27001	Auditoría interna SGSI	Noviembre	2023	☑	☑	1. Notificación con al menos 15 días de anticipación a los involucrados. 2. Incluir evaluación de adopción	Listado de Verificación 2023 - Auditoría interna SGSI	*Cláusulas 5-10. *Dominios 4, 5, 6, 7, 8	☑	☑	Adopción	MMH | AGC | SQ	*Entregar toda la información solicitada por los auditores. *Dar seguimiento a los hallazgos detectados en la auditoría	-Capacidad -Alineado a objetivos -Imparcialidad -Análisis profundo -Independencia	03_Informe de Auditoría Interna SGSI - 2023	Aprobación en el informe de auditoría	
ISO 20000	Auditoria interna TI [4]	Enero	2024	☐	☑	1. Notificación con al menos 15 días de anticipación a los involucrados. 2. Auditar toda la Norma	2da Auditoría Interna TI DIC 2023 - Listado de verificación	Todas las cláusulas	☑	☐		JET | MMH	Mostrar evidencia y documentación	- Independencia - Imparcialidad - Alineado a objetivos - Capacidad	04_Informe de Auditoría Interna SGS TI Dic 2023	PO - Conitnuum - SGS TI: Entrega de informe de auditoría interna	
ISO 27001	2da auditoría de vigilancia SGSI	Febrero	2024	☐	☐				☐	☐							