CONTINUIDAD DE LA SEGURIDAD DE LA INFORMACIÓN

TIPO DE DOCUMENTO: Procedimiento

CÓDIGO: PRO GSI 019

I. AUTORIZACIONES

Elaboró:	*Revisó:*	*Autorizó:*
Ing. Rafael Mendoza Loza *Coordinador de Sistemas TI*	*Ing. Salvador Santiago Araujo* *Gerente Administrativo*	*C.P. Jerónimo Javier Mendoza Lara / Lic. Irais Dafne Mendoza Sánchez* *Director General / Director General Adjunto*

Última revisión: octubre 2025

No. de versión: 7

Fecha de emisión: Agosto 2015

Revisó: GAD

Aprobó: DGE

INDICE

CONTENIDO **PÁGINA**

II. OBJETIVO

Asegurar la continuidad de la seguridad de la información de acuerdo al alcance del SGSI.

III. ALCANCE

Aplica a todas las áreas, procesos y activos de la Organización, involucradas en el Sistema de Gestión de Seguridad de la Información.

IV. HISTORIAL DE CAMBIOS

Versión	Descripción de cambios	Autor(es)	Fecha de cambio
1	Versión inicial.	MBS	Agosto 2015
2	Adecuaciones en 3.2 indicando las acciones que aseguran la continuidad de la seguridad de la información	MBS	Noviembre 2015
3	Cambio de Formato	LBR	Octubre 2016
4	Adecuaciones generales y se agregan las referencias pertinentes.	LBR	Mayo 2017
5	Actualización de referencias, actualización de concientización del personal.	LBR	Junio 2019
6	Actualización del rubro de “Referencias” y de “Autorizaciones” con el nombre del nuevo Gerente Administrativo.	RML	Octubre 2020
7	Se actualizan la sección 6 y el puesto de “Coordinador de TI por Coordinador de Sistemas TI	CST	Septiembre 2023

V. REFERENCIAS

- MAN GSI 001 Manual de gestión de seguridad de la información
- POL GSI 001 Políticas generales de seguridad de la información
- FOR CAL 001 Minuta
- FOR CAL 016 Matriz de riesgos y oportunidades de SGC y SGSI
- FOR CAL 017 Plan de tratamiento de riesgos y oportunidades de SGC y SGSI
- PRO GSI 016 Control de accesos
- PRO GSI 020 Gestión de incidentes
- PRO GSI 032 Respaldos y eliminación de información
- PRO CAL 009 Procedimiento para el Tratamiento de Riesgos y Oportunidades del SGC y SGSI

VI. ABREVIACIONES Y DEFINICIONES

Abreviaciones:

DGE	Director General / Director General Adjunto
GAD	Gerente Administrativo
CSG	Coordinador de Sistemas de Gestión
CST	Coordinador de Sistemas TI
N/A	No Aplica
SGC	Sistema de Gestión de Calidad
SGSI	Sistema de Gestión de Seguridad de la Información

Definiciones:

Integridad: Propiedad de la información relativa a su exactitud y completitud.

Confidencialidad: Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados.

Disponibilidad: Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada.

VII. DESARROLLO DE ACTIVIDADES

No.	Descripción	Responsable(s)
1	Planificación de la continuidad de la seguridad de la información	
1.1	Generalidades: ➢ La Organización determina sus necesidades de seguridad de la información de acuerdo al contexto interno y externo, así como a los requisitos de los clientes, los legales y los de la propia Organización, planteado en el apartado 4.1 del **Manual de gestión de seguridad de la información MAN GSI 001**. ➢ De acuerdo al alcance establecido para el SGSI de la Organización, la parte crítica se circunscribe a asegurar en todo momento la confidencialidad, integridad y disponibilidad de las bases de datos y que residen de forma primordial en servidores. ➢ Bajo esta premisa, la Organización debe de garantizar que dichas bases de datos mantienen su confidencialidad, integridad y disponibilidad a través de acciones indicadas en este documento. ➢ Es responsabilidad de todos los empleados de la Organización, así como de proveedores, contratistas y terceros, el respetar los lineamientos descritos en este documento y acatar las disposiciones que le sean indicadas en caso de un desastre o crisis. ➢ El Área de Sistemas está facultada para emprender las acciones necesarias que conduzcan a la restauración de los sistemas críticos de "información" de la Organización, con el objeto de mantener y asegurar la continuidad de la seguridad de la información y su confidencialidad.	Dirección / Sistemas
1.2	El proceso de administración en la continuidad de la seguridad de la información incluye los siguientes puntos: ➢ Concientización del personal de los riesgos potenciales que implican en la operación, la interrupción de los servicios por eventos impredecibles, y la necesidad de tomar planes de recuperación para esos casos. ➢ Identificación de los bienes y servicios más importantes a proteger en caso de una contingencia (bases de datos y servidores), así como los procesos específicos de recuperación indicados en este documento y de fácil acceso a toda la Organización a través de la página de Sistemas de Gestión. ➢ **FOR GSI 050 Simulacro**	Sistemas

	➢ Matriz de responsabilidades en funciones de situaciones adversas (como se indica más adelante), como parte crítica de las actividades de la Organización.	
2	Concientización del personal	
2.1	Todo el personal al momento de ingresar como empleado a la empresa firma **una Carta de Confidencialidad** de la Información que se integra a su expediente, recibe un curso de Inducción al SGSI, así como una capacitación formal en materia de Seguridad de la Información y participa activamente (de acuerdo al perfil) en los planes y simulacros en materia de continuidad de la seguridad de la información.	Sistemas / Recursos Humanos
3	Identificación de los bienes y servicios más importantes a proteger en caso de una contingencia (bases de datos y servidores)	
3.1	Los servidores que se encuentran ubicados dentro del site, corresponden a la parte crítica del Sistema de Gestión de Seguridad de la Información, ya que contienen las bases de datos, software y aplicaciones para su explotación. El área del site, como hemos indicado en el procedimiento de **Control de accesos PRO GSI 016**, está altamente protegida y restringida en su acceso de forma física y/o remota y solo el personal autorizado puede acceder a ella.	Sistemas
3.2	En caso de crisis, desastres o contingencia, el personal del Área de Sistemas se asegura de que se pueda mantener la continuidad de la seguridad de la información, mediante las siguientes acciones: ➢ Haber realizado los respaldos de la información de acuerdo a la periodicidad y en los sitios físicos alternos (Centro Espejo) de acuerdo a lo que indica el procedimiento de **Respaldos y eliminación de la información PRO GSI 032**. ➢ Contar con el software y aplicaciones (identificadas como necesarias para seguir operando las bases de datos y la información complementaria) en el Centro Espejo y de que se pueda seguir operando. ➢ Asegurarse de que exista la infraestructura mínima necesaria para seguir trabajando (redes, PC, posiciones de trabajo, entre otros) y de que los activos estén en condiciones de operatividad. ➢ Tener informado y capacitado al personal mínimo necesario para seguir trabajando en el sitio alterno (de acuerdo a la capacidad del sitio). ➢ Asegurarse de que, en el Centro Espejo, se mantienen las condiciones de seguridad de la información igual que en la Oficina Matriz.	Sistemas / Dirección

	➢ Llevar a cabo los planes de simulacros de continuidad de la operación y documentar esta actividad en el **Simulacro FOR GSI 050.** ➢ Contar con medios de comunicación o sistema de localización las 24 horas del día, los 365 días del año, con el personal de sistemas. ➢ Contar con las herramientas, recursos y permisos necesarios para la resolución de los problemas para los cuales sean requeridos. ➢ Contar con los directorios del personal necesario, interno y externo, que puedan ofrecer el soporte técnico especializado que pueda ser requerido. ➢ Asegurar en coordinación con la dirección y la gerencia administrativa, el traslado del personal al centro espejo, el traslado se deberá realizar con la flotilla automotriz de la empresa.	
4	Planes de prueba (simulacros)	
4.1	De forma anual, el área de sistemas lleva a cabo simulacros en materia de continuidad de la seguridad de la información, asegurando la confidencialidad, integridad y disponibilidad de las bases de datos, se mantiene evidencia de su realización en el **Simulacro FOR GSI 050**, así como de los hallazgos y su tratamiento para mitigar o eliminar los riesgos asociados.	Sistemas
5	Matriz de responsabilidades	
5.1	➢ Se cuenta con un sistema organizacional para hacer frente a eventos de riesgo o casos de incidentes o fenómenos. ➢ El equipo de respuesta ha sido diseñado de manera funcional que permita coordinar la movilización de los recursos humanos, logísticos y tecnológicos necesarios para hacer frente al evento. ➢ Se cuenta también con una matriz de escalamiento de los puestos claves para delegar funciones.	Dirección
6	Tipos de eventos que ponen en riesgo la confidencialidad, integridad y disponibilidad de las bases de datos.	
6.1	De acuerdo al alcance establecido para el SGSI y la criticidad de las bases de datos, los eventos o incidentes que podrían impedir la continuidad de la seguridad de la información de la Organización, están indicados en la **Matriz de riesgos y Oportunidades de SGC y SGSI FOR CAL 016, Plan de tratamiento de riesgos y oportunidades del SGC y SGSI**	Sistemas

	FOR CAL 017, de acuerdo a lo establecido en el **Procedimiento para el Tratamiento de Riesgos y Oportunidades del SGC y SGSI PRO CAL 009.**	
7	Implementación de la continuidad de la seguridad de la información	
7.1	A efecto de dar continuidad a la seguridad de la información, se cuenta con la siguiente estructura de responsabilidades en caso de Contingencia, tanto en materia de seguridad de la información como en Continuidad de la Operación: Es responsabilidad de las diferentes brigadas de protección civil CIA (Coordinación, Comunicación, Primeros Auxilios, Contra Incendios y Evacuación, búsqueda y rescate) en conjunto con el Gerente Administrativo, elaborar calendarios de realización de ejercicios de evacuación, o ejercicios de emergencia y estén en condiciones de aplicar las acciones de respuesta al presentarse situaciones de riegos de seguridad de la información.	Sistemas / Gerente Administrativo / Brigadas
8	Centro Espejo	
8.1	Cuando por factores naturales como sismos, inundación, incendios, etc., la Organización está preparada para continuar operando con un mínimo de afectaciones, ya que las oficinas de Nezahualcóyotl, Toluca e Insurgentes cuentan con las características informáticas para trasladar la operación entre ellos en caso de que así será requerido. Estos cambios únicamente los puede detonar la autorización de la dirección general.	Dirección / Gerente Administrativo
8.2	El director general, el director general adjunto y el gerente administrativo son los puestos autorizados para el cambio de domicilio a efecto de dar continuidad a la operación y a la seguridad de la información, considerando los siguientes aspectos: a) Debe asegurarse de mantener orden absoluto durante la migración y traslado de personal al Centro Espejo. b) Mantener comunicación con la dirección o el gerente administrativo. c) Dando inicio a las operaciones de traslado. d) La operación concluye cuando la dirección o el gerente administrativo, dan aviso y autorización para regresar y reiniciar operaciones en las instalaciones oficiales de la Organización.	Dirección / Gerente Administrativo
9	Vuelta a la normalidad	
9.1	Cuando la Dirección General o el Gerente Administrativo, determinan que se puede volver a la normalidad, se emprenden las siguientes acciones: a) Dan aviso y autorización para reiniciar operaciones en las instalaciones oficiales de la Organización.	Gerente Administrativo / Sistemas

	b) En la Oficina Matriz con apoyo del personal, restablecen los servidores y se aseguran de que las bases de datos mantienen su confidencialidad, integridad y disponibilidad para que los equipos y personal puedan dar inicio a las operaciones. c) Generar un reporte o minuta general, efectuando una evaluación de daños y pérdidas de información mencionando la situación de perdida, así como un cálculo de las pérdidas económicas, recomendaciones para la mejora e identificación de necesidades para atender y mejorar los procedimientos de atención a contingencias, mediante el formato de **Minuta FOR CAL 001**.	
10	Verificación, revisión y evaluación de la seguridad de la información	
10.1	Derivado de la realización de los simulacros programados y de los riesgos detectados para la continuidad de la seguridad de la información, deberán de emprenderse acciones que mitiguen y/o eliminen dichos riesgos o que mejoren los mecanismos de seguridad de la información. Estas actividades (verificación, revisión y evaluación de la seguridad de la información) deberán de hacerse de acuerdo a lo que indica el procedimiento de **Gestión de Incidentes PRO GSI 020**.	Calidad / Gerente Administrativo / Sistemas
11	Disponibilidad de los recursos de tratamiento de la información	
11.1	La Dirección General se asegura de asignar los recursos necesarios y suficientes para el tratamiento de la información y de hacer las inversiones pertinentes que garanticen la seguridad de la información y su tratamiento, así como de su disponibilidad. Los recursos identificados para el tratamiento de la información son: ➢ Servidores ➢ Redes ➢ Equipos de cómputo ➢ Software y aplicaciones ➢ Instalaciones ➢ Entre otros.	Dirección