GESTIÓN DE INCIDENTES

TIPO DE DOCUMENTO: Procedimiento

CÓDIGO: PRO GSI 020

I. AUTORIZACIONES

Elaboró:	*Revisó:*	*Autorizó:*
Ing. Rafael Fernando 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

Definir los lineamientos y metodología para la adecuada gestión de eventos e incidentes de seguridad de la información, responsabilidades y seguimiento.

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	Adecuación en diversos puntos por uso de la Bitácora de registro de sistemas REG SIS 001	MBS	Mayo 2015
3	Cambio de formato	LBR	Octubre 2016
4	Actualización de A. 16.1.2 incluyendo la Ley Federal de Protección de Datos Personales para sujetos obligados.	LBR	Marzo 2017
5	Se menciona el horario de respuesta ante incidentes en el punto 1	LBR	Febrero 2019
6	Actualización de referencias, modificación en notificación de incidentes, notificación de puntos débiles, evaluación y seguimiento de los incidentes de seguridad con asignación de responsabilidades.	LBR	Junio 2019

7	En esta versión publicamos la nueva hoja de autorizaciones, así como la actualización del portal de soporte técnico antes freshdesk ahora CIA-Desk, así como la actualización del punto 4.1 siendo más específicos en lo que aplicaría en caso de alguna incidencia que detenga la operación de la organización.	RFML	Octubre 2020

V. REFERENCIAS

- MAN GSI 001 Manual de gestión de seguridad de la información
- POL GSI 001 Políticas generales de seguridad de la información
- FOR GSI 024 Formato de incidentes de SI
- FOR GSI 008 Matriz de riesgos de seguridad de la información.

VI. ABREVIACIONES Y DEFINICIONES

Abreviaciones:

DGE	Director General / Director General Adjunto
GAD	Gerente Administrativo
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.

Incidente de Seguridad: Un incidente de seguridad es un evento adverso en un sistema de computadoras, o red de computadoras, que puede comprometer o compromete la confidencialidad, integridad y/o disponibilidad de la información. Puede ser causado mediante la explotación de alguna vulnerabilidad o un intento o amenaza de romper los mecanismos de seguridad existentes.

VII. DESARROLLO DE ACTIVIDADES

No.	Descripción	Responsable(s)
1	Notificación de los eventos de seguridad de la información	
1.1	En caso de algún evento de seguridad de la información, que sea de conocimiento de los empleados de la organización, proveedores o contratistas, deberá de notificarlo de inmediato al área de sistemas a través de los siguientes canales de comunicación: 1. Portal de soporte (CIA-DESK) a. Liga del portal https://ciadesk.ciasc.mx:8080/helpdesk/ b. Enviar correo electrónico a soporte@ciasc.mx 2. Llamada telefónica a las extensiones 169, 170 y 179. Los canales se encuentran disponibles en medio electrónico para todos los usuarios y en donde se debe de registrar el evento o incidente para llevar a cabo las acciones necesarias para su mitigación o eliminación. Se puede reportar un evento de seguridad de la información en cualquier momento, sin embargo, el horario de respuesta es de lunes a viernes de 7:00 a 22:00 horas y sábados de 07:00 a 14:00 horas.	Proveedor o Contratista / Dueños de Proceso / Coordinador de Sistemas TI
2	Notificación de los puntos débiles de la seguridad	
2.1	Se define como punto débil en materia de seguridad de la información: ➢ Los hallazgos que derivado de la realización y/o desarrollo de sus actividades y uso de activos (equipos, redes, aplicaciones, servidores, bases de datos, entre otros) haga el empleado de la organización 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. ➢ Los hallazgos que derivado de la realización y/o 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. **Queda estrictamente prohibido que empleados de la Organización, proveedores o contratistas intenten comprobar puntos débiles que sospechen que exista.**	Proveedor o Contratista / Dueños de Proceso / Coordinador de Sistemas TI
2.2	Para efectos de notificación de los puntos débiles de la seguridad de la información se tiene la siguiente matriz de notificación:	

	➢ **Empleado:** Notificar a través del portal de soporte (CIA-Desk), enviar un correo electrónico a soporte@ciasc.mx o llamando a las extensiones, los cuales se encuentran disponibles en medio electrónico para todos los usuarios y en donde debe de registrar el incidente. ➢ **Proveedor o Contratista:** Notificar al Gerente Administrativo a través del portal de soporte (CIA-Desk) o enviando un correo electrónico a g.sistemas@ciasc.mx, la cual se encuentra disponible en medio electrónico para todos los usuarios y en donde debe de registrar el incidente. ➢ **Responsable de Sistemas:** Dar seguimiento al portal de soporte (CIA-Desk), clasificarlo de acuerdo con su nivel de urgencia y dar seguimiento hasta la resolución del punto débil detectado.	Proveedor o Contratista / Dueños de Proceso / Coordinador de Sistemas TI
3	Evaluación y decisión sobre los eventos de seguridad de la información. Respuesta a incidentes de seguridad de la información. Aprendizaje de los incidentes de seguridad de la información. Recopilación de evidencias.	
3.1	Independientemente del incidente, evento o punto débil de seguridad de la información detectado, deberá de levantarse un ticket en el portal de soporte (CIA-Desk) para su registro y tratamiento, en donde personal del área de Sistemas con base en los datos evaluará y establecerá la categoría y prioridad para la atención.	Responsable del área donde se produjo o detecto el incidente / Sistemas
3.2	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 un 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 considerables a los procesos. ➢ **Integridad:** Ante cualquier evento que afecte a este aspecto de la seguridad de la información. ➢ **Confidencialidad:** Ante cualquier evento que afecte a este aspecto de la seguridad de la información.	Sistemas / Gerente Administrativo

	Gerente Administrativo: Notificará a la dirección, con base en la evaluación de nivel de impacto del incidente a la Organización (daño potencial a activos, tiempo de resolución, recursos necesarios para las medidas a tomar, criticidad de los sistemas afectados, entre otros).	
3.3	Para el caso de incidentes o eventos clasificados como relevantes, personal del área de sistemas notificará al personal de calidad, quienes en conjunto deberán llenar el **Formato de incidentes de SI FOR GSI 024,** de acuerdo con los requisitos establecidos en el mismo formato.	Sistemas / Seguridad de la Información
3.4	Del resultado de las acciones emprendidas para el tratamiento de incidentes y puntos débiles, se deberá de llevar a cabo un análisis detallado, aprendizaje obtenido y proponer acciones globales de mejora. Este análisis se presentará periódicamente en las revisiones por la dirección para el SGSI: ➢ Definir esquemas de respuesta más efectivos ante situaciones que afecten la seguridad de la Información. ➢ Mantener la documentación de los incidentes de seguridad de la Información. ➢ Integrar los incidentes de seguridad al **Plan de Tratamiento de Riesgos y Oportunidades del SGC y SGSI FOR CAL 017**. ➢ Realizar capacitaciones relacionadas con eventos e incidentes de Seguridad de la Información.	Sistemas
3.5	De acuerdo con la naturaleza del incidente, puede ser necesario la recopilación de evidencias (capturas de pantalla, logs del sistema, grabaciones, fotografías, entre otros) para futuras investigaciones, siendo estrictamente necesarias aquellas en las que requieran de una acción disciplinaria y legal. Estas serán adjuntas al **Formato de incidentes de SI FOR GSI 024** físicamente y resguardados por el personal de Seguridad de la Información.	Responsable del área donde se produjo o detecto el incidente / Sistemas
3.6	Todos los servidores de la organización cuentan con un monitor de actividades, el cual emite registros sobre las actividades en el sistema operativo, estos registros se deben de revisar y analizar por el área de sistemas cada 15 días, únicamente se buscan registros de actividades que ponga en riesgo la confidencialidad, disponibilidad e integridad de la información, esta revisión se debe de documentar en la lista de **revisión de LOGS LIS GSI 002**.	Sistemas / Gerente Administrativo

	En el caso de detectar una anomalía se registra en el **Formato de incidentes de SI FOR GSI 024** y se notifica a la gerencia administrativa para que en conjunto con recursos humanos se apliquen las sanciones correspondientes en caso de aplicar.	
4	Declaración de Desastre	
4.1	La organización cuenta con distintos BCP para escenarios que impliquen detener nuestra operación, en caso de que ocurran este tipo de incidentes que paralicen nuestras actividades principales, aplicaremos el BCP indicado. **Ver. PRO GSI 100 - PLAN DE RECUPERACIÓN DE DESASTRES**	Dirección / Gerente Administrativo / Sistemas