GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN DEL SGI

Proceso del Sistema de Gestión Integral de GBInfragroup S.A. de C.V. que define la forma en que se identifican, registran, analizan, contienen, resuelven y documentan los incidentes de seguridad de la información, asegurando la protección de los activos, la continuidad de los servicios y la mejora continua del sistema.

Contenido

1. DATOS DE IDENTIFICACIÓN

Elemento	Definición
Código del documento	SGI-PRC-SEG-01
Nombre	Gestión de Incidentes de Seguridad de la Información del SGI
Tipo documental	Proceso
Responsable del documento	Responsable del SGI
Responsable de elaboración	Responsable del SGI
Revisor	Project Manager
Aprobador	Director General
Clasificación	Interno
Versión	1.0
Estado	Vigente
Vigencia / revisión	Revisión anual o cuando existan incidentes relevantes o cambios en el entorno
Ruta maestra editable	docs/01_Procesos_SGI/SGI-PRC-SEG-01_Gestion_de_Incidentes_Seguridad_Informacion_SGI_v1.0.docx
Ruta PDF publicada	SGI_pdf/01_Procesos_SGI/SGI-PRC-SEG-01_Gestion_de_Incidentes_Seguridad_Informacion_SGI_v1.0.pdf
Documentos relacionados	SGI-PRC-CAL-07; SGI-PRC-AUD-01; SGI-PRC-RSI-01; SGI-PRC-REV-01; SGI-CRT-MED-01; SGI-FOR-SEG-01 Registro de Incidentes de Seguridad de la Información del SGI.

2. OBJETIVO

Establecer la forma en que se gestionan los incidentes de seguridad de la información para asegurar su identificación, control, análisis, resolución y prevención de recurrencia.

3. ALCANCE

Aplica a todos los incidentes que afecten o puedan afectar la confidencialidad, integridad o disponibilidad de la información dentro del alcance del SGI.

Incluye:

1. Identificación y registro
2. Clasificación y priorización
3. Contención
4. Análisis
5. Recuperación
6. Cierre
7. Mejora

4. DEFINICIONES

1. **Incidente de seguridad de la información:** Evento o conjunto de eventos que comprometen o pueden comprometer la confidencialidad, integridad o disponibilidad de la información dentro del alcance del SGI.
2. **Evento de seguridad:** Suceso observado que puede tener relevancia para la seguridad de la información y que debe evaluarse para determinar si constituye un incidente.
3. **Contención:** Acción inmediata orientada a limitar el impacto, propagación o consecuencias de un incidente de seguridad de la información.
4. **Recuperación:** Restablecimiento controlado de las condiciones de operación, integridad de la información y disponibilidad de los servicios afectados.
5. **Severidad:** Nivel de impacto del incidente determinado conforme a sus efectos sobre la confidencialidad, integridad, disponibilidad, cumplimiento o continuidad del servicio.

5. ROLES Y RESPONSABILIDADES

1. **Director General:** Tomar decisiones en incidentes críticos, autorizar recursos extraordinarios y aprobar acciones que impliquen impacto relevante para la operación, el cumplimiento o la continuidad del servicio.

2. **Responsable del SGI:** Coordinar el proceso, asegurar su integración al SGI, validar la trazabilidad de la gestión del incidente y escalar decisiones cuando el impacto del caso lo requiera.
3. **Responsable de Seguridad:** Dirigir la gestión del incidente, coordinar el análisis, contención, recuperación y cierre, y asegurar que la respuesta sea consistente con los criterios definidos por la organización.
4. **Equipo técnico:** Ejecutar las acciones técnicas de análisis, contención, recuperación y validación conforme a las actividades asignadas.
5. **Mesa de ayuda:** Registrar incidentes o eventos reportados, canalizarlos oportunamente y mantener trazabilidad inicial de la atención cuando corresponda.
6. **Áreas involucradas:** Apoyar la resolución del incidente, ejecutar acciones asignadas y aportar información o evidencias necesarias para su tratamiento.

6. ENTRADAS Y SALIDAS DEL PROCESO

6.1 Entradas

1. Eventos de seguridad
2. Reportes de usuarios
3. Alertas de monitoreo
4. Resultados de auditoría
5. Riesgos identificados
6. No conformidades
7. Reportes o evidencias de pérdida, daño, uso indebido, acceso no autorizado, alteración, indisponibilidad o condición de no aptitud de activos, información, medios o recursos pertenecientes a clientes o proveedores externos.

6.2 Salidas

1. Incidentes gestionados
2. Registros completos
3. Acciones de contención y recuperación
4. Información para no conformidades
5. Actualización de riesgos
6. Información para revisión por la dirección

7. LINEAMIENTOS DEL PROCESO

7.1 Identificación y registro de eventos e incidentes

1. Todo evento de seguridad reportado, detectado o identificado dentro del alcance del SGI deberá registrarse de manera controlada desde su conocimiento inicial, asegurando trazabilidad suficiente para su análisis posterior.
2. Todo evento registrado deberá evaluarse para determinar si constituye un incidente de seguridad de la información.
3. Un evento se considerará incidente cuando afecte o tenga el potencial de afectar la confidencialidad, integridad o disponibilidad de la información, el cumplimiento de requisitos aplicables, la continuidad del servicio o la eficacia de controles relevantes del SGI.
4. Los eventos que no cumplan criterios de incidente podrán registrarse y analizarse sin activar el proceso completo de gestión de incidentes, siempre que se conserve evidencia del criterio aplicado.

Cuando el evento o incidente involucre activos, información, medios, credenciales, accesos o recursos pertenecientes a clientes o proveedores externos, dicha condición deberá registrarse expresamente desde el conocimiento inicial del caso.

7.2 Clasificación, priorización y escalamiento

1. Todo incidente de seguridad de la información deberá clasificarse conforme a su severidad, naturaleza e impacto potencial o real sobre la confidencialidad, integridad y disponibilidad de la información.
2. La priorización del incidente deberá considerar, como mínimo, el impacto sobre los activos afectados, la criticidad del servicio, la posible afectación a requisitos contractuales o regulatorios, la recurrencia y la urgencia de atención.
3. Los incidentes clasificados como críticos o de alto impacto deberán escalarse de forma inmediata al nivel de autoridad correspondiente.
4. El criterio de clasificación, priorización y escalamiento deberá quedar documentado como parte del expediente del incidente.

7.3 Contención y control del incidente

1. Una vez identificado un incidente, deberán adoptarse medidas de contención oportunas y proporcionales para limitar su impacto, propagación o consecuencias.
2. Las acciones de contención deberán ejecutarse sin demora injustificada, pero procurando preservar evidencia útil para el análisis posterior.
3. Cuando las acciones de contención impliquen afectación relevante al servicio, a recursos críticos o a obligaciones con terceros, deberá mantenerse trazabilidad de la decisión adoptada y de su justificación.

7.4 Análisis del incidente

1. Todo incidente deberá analizarse para determinar su naturaleza, alcance, activos afectados, condiciones de ocurrencia, impacto real o potencial y causa raíz cuando corresponda.
2. El análisis deberá sustentarse en evidencia verificable suficiente y no en apreciaciones informales o no documentadas.
3. Cuando el incidente revele fallas de control, debilidades recurrentes o condiciones de riesgo no tratadas, dicha información deberá integrarse a la gestión del SGI conforme a los procesos relacionados.

Cuando el incidente afecte propiedad perteneciente a clientes o proveedores externos, el análisis deberá considerar, además de la afectación a la confidencialidad, integridad o disponibilidad, las obligaciones de custodia, notificación, restitución, comunicación o tratamiento derivadas de dicha condición.

7.5 Recuperación y restablecimiento

1. La recuperación deberá orientarse al restablecimiento controlado de la operación, validando la integridad de la información, la disponibilidad de los servicios y la efectividad de las medidas aplicadas.
2. No se considerará resuelto un incidente únicamente por la contención inicial; deberá existir evidencia suficiente de recuperación y validación del restablecimiento cuando aplique.
3. Cuando la recuperación requiera acciones extraordinarias, uso de respaldos, intervención de terceros o medidas de continuidad, dichas acciones deberán documentarse y mantenerse bajo control.

7.6 Cierre del incidente y lecciones aprendidas

1. Todo incidente deberá cerrarse formalmente una vez que se haya confirmado la contención, la recuperación, la documentación suficiente del caso y, cuando aplique, la definición de acciones de mejora.
2. El cierre deberá incluir la determinación de si el incidente genera lecciones aprendidas, necesidades de ajuste de controles, actualización de riesgos o vinculación con otros procesos del SGI.
3. Los incidentes relevantes o recurrentes deberán dar lugar a análisis de tendencias y acciones orientadas a prevenir su repetición.

7.7 Integración con otros procesos del SGI

1. Los incidentes que impliquen incumplimientos, desviaciones o debilidades de control deberán vincularse al proceso **SGI-PRC-CAL-07 Control de No Conformidades del SGI**, cuando corresponda.
2. Los incidentes que modifiquen el perfil de riesgo, revelen riesgos no identificados o afecten la eficacia de tratamientos existentes deberán reflejarse en la actualización del registro de riesgos y en los mecanismos de evaluación y seguimiento aplicables del SGI.
3. Los incidentes relevantes deberán integrarse como información de entrada para la **Revisión por la Dirección**, cuando su impacto, recurrencia o criticidad lo justifique.

Los incidentes que involucren propiedad de clientes o proveedores externos deberán vincularse, cuando corresponda, con el registro de activos, con el tratamiento de riesgos, con la gestión de no conformidades y con cualquier acción de comunicación o seguimiento requerida por las condiciones aplicables del caso.

7.8 Control de evidencia

1. Toda evidencia generada en la gestión del incidente deberá mantenerse como información documentada controlada conforme al proceso documental vigente del SGI.
2. La evidencia deberá ser suficiente, trazable, verificable y disponible para fines de auditoría, seguimiento, mejora y toma de decisiones.

3. No deberá cerrarse un incidente sin evidencia mínima suficiente de registro, clasificación, análisis, acciones aplicadas, recuperación y decisión de cierre.

8. REGISTROS ASOCIADOS

Los registros y documentos asociados a este proceso deberán mantenerse bajo control conforme a lo establecido en SGI-PRC-DOC-01 Control de la Información Documentada del SGI.

Como evidencia de la operación del proceso deberán existir, según corresponda:

1. SGI-FOR-SEG-01 Registro de Incidentes de Seguridad de la Información del SGI, como registro primario de reporte, clasificación, atención, seguimiento y cierre del incidente.
2. Evidencia de análisis, severidad, priorización y criterio aplicado para determinar si un evento constituye incidente.
3. Evidencia de acciones de contención implementadas.
4. Evidencia técnica de análisis, erradicación, recuperación y validación de restablecimiento.
5. Evidencia de escalamiento, comunicación y coordinación con las áreas involucradas, cuando aplique.
6. SGI-REG-ASI-01 Registro de Activos de Información, Clasificación y Manejo del SGI, cuando el incidente se relacione con activos o recursos previamente identificados bajo custodia, uso o administración de la organización.

9. REFERENCIAS NORMATIVAS Y DOCUMENTALES

1. ISO/IEC 27001:2022
2. ISO/IEC 27002:2022
3. ISO/IEC 27035
4. SGI-PRC-CAL-07
5. SGI-PRC-AUD-01
6. SGI-PRC-DOC-01
7. SGI-PRC-RSI-01
8. SGI-PRC-REV-01
9. SGI-CRT-MED-01

SGI-FOR-SEG-01 Registro de Incidentes de Seguridad de la Información del SGI.

10. INDICADORES DE EFICACIA

La eficacia del proceso deberá evaluarse mediante indicadores vinculados de forma directa con las salidas del proceso y con la capacidad de la organización para identificar, contener, resolver y cerrar incidentes de seguridad de la información de manera controlada y oportuna.

1. **Tiempo promedio de detección de incidentes de seguridad de la información.**
   Mide el tiempo requerido para identificar y registrar un incidente desde su ocurrencia o reporte.
   Salidas relacionadas: Incidentes gestionados; registros completos.
2. **Tiempo promedio de resolución de incidentes de seguridad de la información.**
   Mide el tiempo requerido para resolver un incidente y restablecer condiciones aceptables de operación.
   Salidas relacionadas: Incidentes gestionados; acciones de contención y recuperación.
3. **Porcentaje de incidentes atendidos dentro del tiempo objetivo definido.**
   Mide la proporción de incidentes gestionados dentro de los tiempos comprometidos o criterios de atención establecidos.

Salidas relacionadas: Incidentes gestionados; acciones de contención y recuperación.

4. **Porcentaje de incidentes cerrados con expediente completo y evidencia suficiente.**
   Mide la proporción de incidentes que cuentan con trazabilidad documental suficiente desde su registro hasta su cierre.
   Salidas relacionadas: Registros completos; información para revisión por la dirección.
5. **Porcentaje de incidentes que actualizan el registro de riesgos o generan vinculación con no conformidades, cuando aplique.**
   Mide la proporción de incidentes que, por su impacto o recurrencia, se integran formalmente a la gestión de riesgos o al proceso de no conformidades.
   Salidas relacionadas: Información para no conformidades; actualización de riesgos.
6. **Porcentaje de recurrencia de incidentes de seguridad de la información.**
   Mide la proporción de incidentes que vuelven a presentarse después de haber sido gestionados y cerrados.
   Salidas relacionadas: Incidentes gestionados; información para revisión por la dirección.

11. APROBACIÓN DEL DOCUMENTO

Rol	Nombre / cargo	Fecha
Elaboró	Responsable del SGI	14/04/26
Revisó	Project Manager	14/04/26
Aprobó	Director General	14/04/26

Nota: Las firmas de aprobación se incorporan en la versión PDF final controlada del documento, conforme al mecanismo de autorización vigente de GBInfragroup S.A. de C.V.

12. CONTROL DE CAMBIOS

Versión	Fecha	Descripción del cambio
1.0	14/04/26	Emisión inicial del proceso

Página final de firmas y certificación digital

Referencia visible de firmas digitales y certificación documental

Certificación expresa del documento

Yo, Raúl Rodríguez Macías, en mi carácter de Responsable del Sistema de Gestión Integral, certifico de manera expresa la integridad documental del presente PDF. Este documento incorpora las firmas digitales válidas de aprobación correspondientes y la presente constancia visible de cierre documental.

Aprobación del Project Manager

Firmante Bruno Ivan Reynoso Trejo
Cargo Project Manager
Alcance Aprobación ejecutiva de la emisión documental y conformidad con el contenido del documento.

Certificado digital
Titular: Bruno Ivan Reynoso Trejo | Emisor: PDF CA Interna Intermediate CA
Serie: 2CED87417FAEA06901F739758B92197C | Vigencia: 2026-04-15 a 2029-04-14

Aprobación de Dirección General

Firmante Juan Carlos Reyes Oropeza
Cargo Director General
Alcance Aprobación final institucional del documento dentro del marco de gobierno y dirección del SGI.

Certificado digital
Titular: Juan Carlos Reyes Oropeza | Emisor: PDF CA Interna Intermediate CA
Serie: A44658F437D7B4C68381429D1D3E6ABD | Vigencia: 2026-04-15 a 2029-04-14

Certificación documental del Responsable del SGI

Firmante Raul Rodriguez Macias
Cargo Responsable del Sistema de Gestión Integral
Alcance Constancia visible de cierre documental del PDF final y de incorporación de las firmas digitales previas.

Certificado digital
Titular: Raul Rodriguez Macias | Emisor: PDF CA Interna Intermediate CA
Serie: 1006D5244EA0DF0BBA77F08906A48975 | Vigencia: 2026-04-15 a 2029-04-14