Gestión de Incidentes de Seguridad

Elaboró:	Líder del Sistema de Gestión Integral		
Revisó:	Control de Documentos		
Aprobó:	Director General		
Responsable del documento:	Líder del Sistema de Gestión Integral	Tiempo de retención:	1 año posterior a su vigencia
		Disposición final:	Eliminación del repositorio documental

Versión	Fecha	Descripción del cambio
1	27/02/19	Emisión inicial

Contenido

1. Objetivo

Establecer las actividades a seguir para detectar, reportar y restaurar las debilidades (vulnerabilidades) y los incidentes que impacten al Sistema de Gestión integral, lo cual permita tomar acciones pertinentes en tiempo y forma minimizando el impacto al negocio.

2. Alcance

Todos los documentos del Sistema de Gestión Integral de la Organización, tales como el Manual de Políticas, Procedimientos de Gestión y Procedimientos Operativos, así como los documentos de trabajo que apoyan la realización de las actividades

3. Políticas

1. El personal debe notificar de manera oportuna las debilidades e incidentes de seguridad de la información que detecte.
2. El personal en ninguna circunstancia debe intentar probar o corregir la debilidad que dio origen al incidente de seguridad de información detectado.
3. El personal debe evitar el uso de activos o mecanismos comprometidos por el incidente de seguridad de información
4. Líder del SGI debe atender los reportes de incidentes de seguridad de una manera rápida y eficaz.
5. Líder del SGI debe evitar, en la medida de lo posible, acciones reactivas del atacante/ intruso.
6. En el caso de que a consecuencia del incidente se vean comprometidos documentos en papel, el documento original se mantiene bajo custodia y se genera un registro de la persona que encontró el documento y dónde y cuándo fue encontrado, así como también, quién fue testigo del descubrimiento.

4. Definiciones

AAV: Acrónimo de Activo-Amenaza-Vulnerabilidad. Al conjunto Activo-Amenaza-Vulnerabilidad también se le conoce como escenario de riesgo.

Aceptación del Riesgo: Es la decisión de aceptar un nivel de riesgo de tal forma que se opere conviviendo con éste.

Activo: Cualquier elemento que tenga valor tangible o intangible para la organización.

Administración de riesgos: Actividades coordinadas para dirigir y controlar una organización con respecto a los riesgos que afrontan. La administración de riesgos incluye la evaluación de riesgos, su tratamiento, aceptación y comunicación.

Alta Dirección: Rol cubierto por el Director de Seguridad y Redes.

Amenaza: Causa potencial de un incidente no deseado que puede provocar daños a uno o más activos, procesos, servicios de la organización.

Análisis de riegos: Método analítico de la administración de riesgos que permite la identificación de vulnerabilidades y amenazas de seguridad, así como la evaluación de la magnitud o impacto de los daños a efecto de determinar dónde sería necesaria la implementación de controles y la cantidad máxima razonable de recursos que sería necesario invertir.

CID: Acrónimo de Confidencialidad, Integridad y Disponibilidad.

Confidencialidad: Principio de seguridad de la información que consiste en asegurar que el acceso al activo únicamente se realiza por los autorizados y a través de los procedimientos establecidos para ello.

Control: Recurso aplicado para mitigar el riesgo.

Disponibilidad: Principio de seguridad de la información que estipula que el activo puede ser utilizado por los autorizados cuando éstos lo requieran.

Incidente de Seguridad: Es un evento o serie de eventos no deseados o inesperados que atentan contra una o más de las características de la Seguridad de la Información (Confidencialidad, Integridad y/o Disponibilidad).

Integridad: Principio de seguridad de la información que consiste en que el activo sólo puede ser modificado por los autorizados.

Riesgo: Resultado de multiplicar la probabilidad de un evento por su impacto o consecuencia.

Riesgo Residual: Es el riesgo que permanece después de que la organización realiza el tratamiento de los riesgos identificados como parte de la administración de riesgos, es decir, es el riesgo que permanece después de implementar los controles seleccionados.

SGI: Sistema de Gestión Integral

SoA: Declaración de Aplicabilidad (Statement of Applicability, SoA por sus siglas en inglés).

Tratamiento del Riesgo: Proceso de selección e implementación de controles para modificar el riesgo.

Vulnerabilidad: Debilidad de un activo o grupo de activos que puede ser aprovechada por una o más amenazas comprometiendo en consecuencia la confidencialidad, disponibilidad e integridad de la información o de los activos.

5. Responsabilidades

Personal de Silent4business

- Detecta un incidente o debilidad que comprometa la seguridad de la información.
- Contacta vía telefónica o correo electrónico al Líder del SGI para reportarle el incidente o debilidad de seguridad de información detectada.

Líder del SGI

- Recibe el reporte de incidente o debilidad de seguridad de información y lo registra en el formato del Reporte del Incidente de Seguridad de la Información (F-SGI-006)
- Convoca al equipo de respuesta de incidentes de seguridad.
- Clasifica el incidente de seguridad y asigna prioridad si procede el manejo del incidente.
- Notifica a la persona que realiza la llamada para reportar el incidente.
- Registra en el formato el lugar donde sucedió el incidente y la naturaleza del mismo.
- Documenta en la base de conocimiento de incidentes de seguridad.
- Canaliza a otra área.

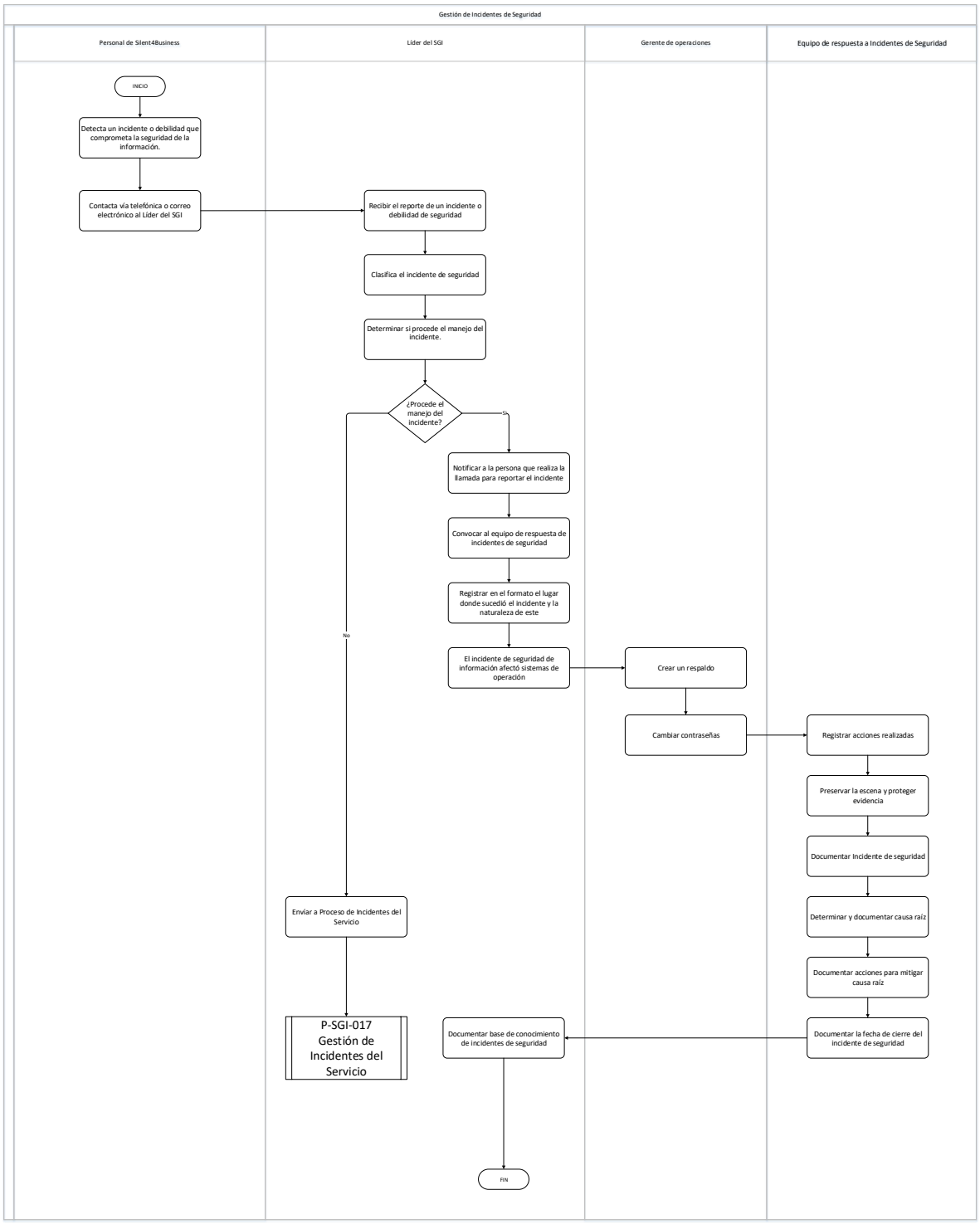
Gerente de operaciones

- Crea un respaldo de estos, con el objetivo de analizar el respaldo y dejar intacto el sistema
- Cambia contraseñas o mecanismos de acceso a los sistemas afectados.

Equipo de respuesta a Incidentes de Seguridad

- Registra las acciones realizadas en el formato del Reporte del Incidente de Seguridad de la Información.
- Preserva la escena (asegura el área afectada por el incidente) y protege la evidencia.
- Documentar Incidente de seguridad, acciones para mitigar causa raíz y la fecha de cierre del incidente de seguridad.
- Determina la causa raíz de este, documentándola en el formato del Reporte del Incidente de Seguridad de la Información.

6. Diagrama de Flujo



7. Descripción del Proceso

No.	RESPONSABLE	ACTIVIDAD	DESCRIPCIÓN	REGISTROS
qs 1	Personal de silent4business	Detecta un incidente o debilidad que comprometa la seguridad de la información.	Detecta un incidente o debilidad que comprometa la seguridad de la información. A continuación, se listan algunos ejemplos de incidentes de seguridad de información, los cuales son enunciativos, más no limitativos: • Pérdida de documentación del negocio • Detectar que alguna persona esté dentro de las instalaciones de la Organización sin autorización. • Extravío o robo del gafete de identificación • Error humano. • Violación al control de acceso físico. • Incumplimiento con políticas y/o procedimientos • Pérdida de servicios, equipos o instalaciones • Malfuncionamiento de los sistemas • Cambios al sistema no controlados • Malfuncionamiento del hardware y/o software • Violaciones al control de acceso lógico. • Ejecución intencionada de código malicioso que ponga en riesgo la información. • Ejecución intencionada de herramientas y escáneres detectores y atacantes de vulnerabilidades de	

			seguridad en los sistemas informáticos.	
2	Personal de silent4business	Contacta vía telefónica o correo electrónico al Líder del SGI	Contacta vía telefónica o correo electrónico al Líder del SGI para reportarle el incidente o debilidad de seguridad de información detectada. **NOTAS:** - En ninguna circunstancia intenta probar o corregir la debilidad que dio origen al incidente de seguridad de información detectada. - Evitar el uso de activos o mecanismos comprometidos por el incidente de seguridad de información	
3	Líder del SGI	Recibir el reporte de un incidente o debilidad de seguridad	Recibe el reporte de incidente o debilidad de seguridad de información y lo registra en el formato del Reporte del Incidente de Seguridad de la Información (F-SGI-006) los siguientes datos: ▪ No. de Reporte. ▪ Fecha de reporte. ▪ Hora de reporte. ▪ Nombre de la persona que llamó para reportar el incidente o debilidad de seguridad de información. ▪ Área que se ve directamente afectada a causa del incidente o debilidad de seguridad de información. ▪ Descripción del incidente o debilidad de la seguridad de información, proporcionada por la persona que realiza el reporte. ▪ Breve descripción del incidente.	F-SGI-006 Reporte del Incidente de Seguridad de la Información
4	Líder del SGI	Clasifica el incidente	De acuerdo con la descripción dada sobre el incidente o debilidad de la	

		de seguridad	seguridad de información; clasifica y asigna prioridad.	
5	Líder del SGI	Determinar si procede el manejo del incidente.	Determina si procede el manejo del incidente. **Si:** Continúa actividad 6 **No:** Continúa actividad 19	
6	Líder del SGI	Notificar a la persona que realiza la llamada para reportar el incidente	Notifica a la persona que realiza la llamada para reportar el incidente, las acciones que deben seguirse ya sean para contener el incidente o para atender el evento documentándolo en Acciones inmediatas del formato del Reporte del Incidente de Seguridad de la Información (F-SGI-006).	F-SGI-006 Reporte del Incidente de Seguridad de la Información
7	Líder del SGI	Convocar al equipo de respuesta de incidentes de seguridad	De acuerdo con la extensión y el impacto del incidente o debilidad de seguridad de información reportado determina el apropiado curso de acción, convoca al Equipo de Respuesta de incidentes, según el tipo de reporte para que lo asista y ayude en la resolución del incidente documentándolo en Personas que manejan el incidente del formato del Reporte del Incidente de Seguridad de la Información (F-SGI-006).	F-SGI-006 Reporte del Incidente de Seguridad de la Información
8	Líder del SGI	Registrar en el formato el lugar donde sucedió el incidente y la naturaleza de este	Registra en el formato el lugar donde sucedió el incidente y la naturaleza del mismo (robo, pérdida de información, incendio, etc.) en el campo 10 del formato del Reporte del Incidente de Seguridad de la Información (F-SGI-006). **Nota:** De ser posible acude al sitio donde ocurrió el incidente reportado en compañía del personal de apoyo involucrado en el manejo del incidente de seguridad.	F-SGI-006 Reporte del Incidente de Seguridad de la Información
9	Líder del SGI	El incidente de seguridad de	¿El incidente de seguridad de información afectó sistemas de operación?	

		información afectó sistemas de operación	**Si:** Continúa actividad 10 **No:** Continúa actividad 12	
10	Gerente de operaciones	Crear un respaldo	Crea un respaldo de los mismos, con el objetivo de analizar el respaldo y dejar intacto el sistema comprometido para que pueda servir como evidencia en caso necesario.	
11	Gerente de operaciones	Cambiar contraseñas	Cambia contraseñas o mecanismos de acceso a los sistemas afectados. **Nota:** En caso de que el equipo haya sido comprometido, se evita utilizarlo para intercambio de información (Chat, correo electrónico, etc.), incluso el equipo deberá desconectarse de la red.	
12	Equipo de respuesta a Incidentes de Seguridad	Registrar acciones realizadas	Registra las acciones realizadas en el campo Acciones subsecuentes del formato del Reporte del Incidente de Seguridad de la Información (F-SGI-006).	F-SGI-006 Reporte del Incidente de Seguridad de la Información
13	Equipo de respuesta a Incidentes de Seguridad	Preservar la escena y proteger evidencia	Preserva la escena (asegura el área afectada por el incidente) y protege la evidencia con el objetivo de preservar su admisibilidad y valor en caso de que sea necesario entablar una acción legal, para lo cual se deben tener en consideración las siguientes acciones: ▪ Tomar fotografías, asegurar las bitácoras, tomar notas el estado del sistema, etc. ▪ Identificar cada parte de la evidencia por medio de etiquetas, fechas firmas, etc., cuando aplique. ▪ Usar acuses de recibo cuando la evidencia sea transferida a otra persona para su manejo ▪ Controlar el acceso a la evidencia ▪ Definir quien tiene acceso a la evidencia	

			▪ Recolecta toda la información posible a cerca del incidente. Las cuales se agregarán de forma impresa para historial de la Base de Datos de Conocimientos que se estará generando	
14	Equipo de respuesta a Incidentes de Seguridad	Documentar Incidente de seguridad	Registra en Evidencia del incidente del formato del Reporte del Incidente de Seguridad de la Información (F-SGI-006).	F-SGI-006 Reporte del Incidente de Seguridad de la Información
15	Equipo de respuesta a Incidentes de Seguridad	Determinar y documentar causa raíz	Con base en la información obtenida acerca del incidente de seguridad de la información, determina la causa raíz de este, documentándola en campo Causa raíz del incidente del formato del Reporte del Incidente de Seguridad de la Información (F-SGI-006).	F-SGI-006 Reporte del Incidente de Seguridad de la Información
16	Equipo de respuesta a Incidentes de Seguridad	Documentar acciones para mitigar causa raíz	Documenta en el campo Acciones posteriores del formato del Reporte del Incidente de Seguridad de la Información (F-SGI-006), las acciones necesarias que deben llevarse a cabo para mitigar la causa raíz del incidente y evitar futuras ocurrencias de este e identifica áreas de mejora.	F-SGI-006 Reporte del Incidente de Seguridad de la Información
17	Equipo de respuesta a Incidentes de Seguridad	Documentar la fecha de cierre del incidente de seguridad	Una vez que el incidente fue atendido y solucionado, anota la fecha y hora en que el incidente se da por cerrado en el campo Fecha y hora de cierre del incidente del formato del Reporte del Incidente de Seguridad de la Información (F-SGI-006). **Nota:** Cuando aplique, levantan una acción correctiva de acuerdo con el Procedimiento de Acciones Correctivas, con el objetivo de eliminar la causa raíz del incidente y así evitar su recurrencia.	F-SGI-006 Reporte del Incidente de Seguridad de la Información
18	Líder del SGI		Crea una base de conocimiento de los incidentes de seguridad ocurridos y la	

		Documentar base de conocimiento de incidentes de seguridad	forma en que se resolvieron, con la recopilación de los Reportes de Incidentes que se han tenido resguardándolos en una carpeta, con el objetivo de aprender de los incidentes, minimizar los tiempos de recuperación y evitar en lo posible su recurrencia. **Nota:** En caso de que el incidente de seguridad de información haya sido provocado por personal de la Organización, determina las acciones disciplinarias apropiadas.	
19	Líder del SGI	Enviar a Proceso de Incidentes de Servicio	Lo canaliza a el Proceso de Incidentes de Servicio	Proceso de Incidentes de Servicio

8. Documentos relacionados

- F-SGI-006 Reporte de Incidente de Seguridad