CONTENIDO

Elaborado por:	Revisado y Aprobado por:	Aprobación Metodológica por:
Nombre: Eduar Enrique Navarro Morales Cargo: Coordinador Grupo de Trabajo de Informática Forense y Seguridad Digital.	Nombre: Oscar Javier Asprilla Cruz Cargo: Jefe Oficina de Tecnología e Informática.	Nombre: Giselle Johanna Castelblanco Muñoz Cargo: Representante de la Dirección para el Sistema de Gestión de Calidad. Fecha: 2018-10-11

1 OBJETIVO

Gestionar las alertas, eventos e incidentes de seguridad de la información para tomar los correctivos necesarios y prevenir que no vuelvan a ocurrir, a través de la descripción de las etapas de prevención, reporte, análisis, solución, documentación, recolección de evidencia e inicio de procesos legales con los incidentes presentados en el ámbito de la Superintendencia de Industria y Comercio.

2 DESTINATARIOS

Este procedimiento aplica para todos los servidores públicos, contratistas o terceros de la Superintendencia de Industria y Comercio.

3 GLOSARIO

AGENTE DEL PRIMER PUNTO DE CONTACTO: Profesional de la mesa de servicios, encargado de recibir, registrar escalar los posibles incidentes de seguridad de la información reportados por los usuarios.

CIO (Chief Information Officer): es el líder de la gestión estratégica de tecnologías de información, encargado de planificar, organizar, coordinar, gestionar y controlar la estrategia de uso y apropiación de TI y el Modelo de Seguridad y Privacidad de la Información, y todo lo que conlleva esta tarea.

CONFIDENCIALIDAD: Propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados.

DISPONIBILIDAD: propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada.

EVENTO DE SEGURIDAD DE LA INFORMACIÓN: Presencia identificada de un estado del sistema, servicio o de red, que indica un posible incumplimiento de la política de seguridad de la información, una falla de controles, o una situación previamente desconocida que puede ser pertinente para la seguridad.

GESTIÓN DE INCIDENTES DE LA SEGURIDAD DE LA INFORMACIÓN: Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información.

GRUPOS DE INTERÉS ESPECIAL: Grupos u otros foros y asociaciones profesionales especializadas en seguridad de la información.

INCIDENTE DE SEGURIDAD DE LA INFORMACIÓN: Un solo evento o una serie de eventos inesperados o no deseados de seguridad de la información que tienen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

INTEGRIDAD**:** Propiedad de salvaguardar la exactitud y estado completo de los activos.

INVESTIGACIÓN FORENSE DE SEGURIDAD DE LA INFORMACIÓN: Aplicación de técnicas de investigación y análisis para recolectar registrar y analizar información de incidentes de seguridad de la información.

OFICIAL DE SEGURIDAD DE LA INFORMACIÓN: Es el profesional responsable de alinear las iniciativas de seguridad con los objetivos misionales, garantizando que los bienes y las tecnologías de la información están adecuadamente protegidos.

PROFESIONAL DEL LABORATORIO DE INFORMÁTICA FORENSE: Es el profesional responsable de aplicar técnicas científicas y analíticas especializadas a infraestructura tecnológica que permiten identificar, preservar, analizar y presentar datos que sean válidos dentro de un proceso legal o no legal.

RESPONSABLE DE LA ATENCIÓN DE INCIDENTES DE SEGURIDAD: Es el profesional responsable de llevar a cabo la implementación, notificación y registro de la solución al incidente que se haya identificado.

SALVAGUARDA: Prácticas, procedimientos o mecanismos que pueden proteger contra una amenaza y reducir la probabilidad de explotación de una vulnerabilidad.

SGSI (Sistema de Gestión de la Seguridad de la Información): Parte del sistema de gestión global, basada en un enfoque hacia los riesgos globales de un negocio, cuyo fin es establecer, implementar, operar, hacer seguimiento, revisar, mantener y mejorar la seguridad de la información.

SOLICITUD DEL SERVICIO**:** Petición realizada por un usuario sobre información o asesoramiento, solicitud de un cambio estándar, o solicitud de acceso a un servicio de TI.

TI (Tecnología de la Información): Se refiere a los elementos de hardware, software, servicios, procesos y en general cualquier otro elemento usado en el procesamiento, almacenamiento y transmisión de la información.

VULNERABILIDAD: Corresponde a una debilidad o fragilidad de un sistema (físico, técnico, organizacional, cultural, etc.) que puede ser explotada por una amenaza, causando daños o perjuicios.

4 REFERENCIAS

Jerarquía de la norma	Numero/fecha	Título	Artículo	Aplicación específica
NTC-ISO-IEC	27002:2013	Tecnología de la Información. Técnicas de Seguridad. Código de Práctica para la Gestión de la Seguridad de la Información.	Aplicación total	Aplicación total

5 GENERALIDADES

Se debe llevar a cabo una rápida, efectiva y ordenada gestión de incidentes para asegurar que los usuarios obtengan respuesta a sus reportes, que los incidentes son tratados de acuerdo al nivel de criticidad, que se establezca una metodología para las lecciones aprendidas basado en experiencias previas y que se opta por una resolución acertada de acuerdo con la situación particular del incidente.

6 REPRESENTACIÓN ESQUEMÁTICA DEL PROCEDIMIENTO

No.	ETAPAS	ENTRADAS	DESCRIPCIÓN DE LA ACTIVIDAD	RESPONSABLE	SALIDAS
1	PREVENIR INCIDENTES SEGURIDAD DE LA INFORMACIÓN	Comunicados y alertas emitidos por grupos de interés especial.	Establecer acciones para prevenir los incidentes de seguridad de la información, a través de las siguientes actividades: - Establecer contacto con grupos de interés especial. - Analizar los comunicados emitidos por los grupos de interés especial. - Implementar las medidas preventivas necesarias.	Oficial de Seguridad de la Información o a quien él delegue. Agente del primer punto de contacto.	Correo electrónico con el resultado de la aplicación de medidas preventivas.
2	REPORTAR Y ANALIZAR UN EVENTO DE SEGURIDAD DE LA INFORMACIÓN	Evento de seguridad de la información.	Se deben reportar y analizar los eventos para determinar si este corresponde a un incidente de seguridad de la información que pueden afectar la seguridad de la información, a través de la siguiente actividad: - Reportar eventos de seguridad de la información. - Validar el evento de seguridad de la información. - Valorar el impacto del incidente.	Todos los servidores públicos, contratistas y terceros de la SIC. Agente del primer punto de contacto. Oficial de Seguridad de la Información o quien él delegue.	Registro del incidente en la Mesa de Servicios.
3	SOLUCIONAR EL INCIDENTE.	Registro del incidente en la Mesa de Servicios.	Definir las acciones para contener el incidente e implementar la solución definitiva, a través de las siguientes actividades: - Definir la solución del incidente. - Implementar la solución al incidente. - Notificar la solución del incidente. - Establecer contacto con las autoridades. - Identificar las lecciones aprendidas.	Oficial de Seguridad de la Información o quien él delegue. Responsable de la atención de incidentes de seguridad.	Resultado del análisis del incidente reportado. Evidencias de la solución del incidente.
4	DOCUMENTAR EL INCIDENTE.	Resultado del análisis del incidente reportado. Evidencias de la solución del incidente.	Realizar el registro del incidente en la herramienta de apoyo al SGSI, a través de las siguientes actividades: - Diligenciar los campos de registro en la herramienta de apoyo al SGSI. - Identificar los requisitos de la norma ISO 27001 afectados por el incidente.	Responsable de la atención de incidentes de seguridad.	Registro del incidente en la herramienta de apoyo al SGSI.

5	RECOLECTAR LA EVIDENCIA.	Resultado del análisis del incidente reportado. Evidencias de la solución del incidente.	Realizar las labores de recolección de evidencia digital, a través de la siguiente actividad: - Recolectar y conservar la evidencia del incidente.	Profesional del laboratorio de Informática Forense de la SIC designado.	Evidencias forenses recolectadas.
6	INICIAR PROCESO LEGAL.	Evidencias forenses recolectadas.	Cuando se requiera puede iniciarse un proceso legal, a través de la siguiente actividad: - Iniciar el proceso legal.	Oficial de Seguridad de la Información o quien él delegue. CIO.	Memorando de solicitud de un proceso legal.

7 DESCRIPCION DE ETAPAS Y ACTIVIDADES

7.1 ETAPA 1: PREVENIR INCIDENTES SEGURIDAD DE LA INFORMACIÓN

7.1.1 Establecer contacto con grupos de interés especial

El Oficial de Seguridad de la Información y los profesionales de apoyo a la gestión operativa del SGSI, mantendrán contactos apropiados con grupos de interés especial, foros y asociaciones profesionales especializadas en seguridad, con el fin de prevenir los incidentes de seguridad de la información con el propósito de:

- Mejorar el conocimiento acerca de las mejores prácticas y permanecer al día con la información de seguridad pertinente.
- Asegurar que la comprensión del entorno de la seguridad de la información sea actual y esté completa.
- Recibir advertencias tempranas de las alertas, avisos y parches acerca de ataques y vulnerabilidades.
- Obtener acceso a asesoría especializada en seguridad de la información.
- Compartir e intercambiar información acerca de nuevas tecnologías, productos, amenazas o vulnerabilidades.
- Brindar puntos de enlace adecuados cuando se trata con incidentes de seguridad de la información.

A continuación, se presenta un listado base de organizaciones con las cuales el Oficial de Seguridad de la Información o a quien él delegue, debe inscribirse a sus boletines, comunicados, alertas y participar de las reuniones que algunas de ellas organicen, según aplique.

- CSIRT, https://cc-csirt.policia.gov.co/.

- COLCERT, http://www.colcert.gov.co/?q=tags/alertas-de-seguridad
- INCIBE, https://www.incibe.es/.
- CCOC, Comando Conjunto Cibernético.
- Centro Cibernético Policial, https://caivirtual.policia.gov.co
- Hispasec, https://hispasec.com/es/contact
- Ministerio de Tecnologías de la Información y las Comunicaciones, Modelo de Seguridad y Privacidad de la Información.

7.1.2 Analizar los comunicados emitidos por los grupos de interés especial

Cuando los grupos de interés especial emitan comunicados y alertas, es deber del Oficial de Seguridad de la Información o a quien él delegue, analizar su aplicabilidad en la entidad, y en caso de ser necesario debe tomar las acciones pertinentes dependiendo de la situación. Para el caso de alertas de correos maliciosos y vulnerabilidades que pongan en riesgo la plataforma tecnológica de la SIC, estos deben ser remitidos, vía correo electrónico, a la Mesa de Servicios.

7.1.3 Implementar las medidas preventivas necesarias

Una vez la Mesa de Servicios o el profesional asignado reciba el reporte, debe proceder a tomar las medidas preventivas necesarias para que no se vea afectada la plataforma tecnológica de la SIC y sus usuarios. El resultado de la implementación de las medidas preventivas debe ser notificado a los interesados a través del correo electrónico.

7.2 ETAPA 2: REPORTAR Y ANALIZAR UN EVENTO DE SEGURIDAD DE LA INFORMACIÓN

7.2.1 Reportar eventos de seguridad de la información.

Todos los servidores públicos y contratistas de la SIC deben reportar presuntos incidentes de seguridad de la información cuando aplique. Los canales de comunicación definidos para este reporte, son los siguientes:

- Portal web: http://mesadeservicios.sic.gov.co/,
- Correo electrónico: mesadeservicios@sic.gov.co,
- Llamada telefónica: Extensión 10502, que serán gestionados por el proveedor de la Mesa de Servicios de la SIC. Por medio de este canal se recibirán los incidentes de seguridad y se redirigirán hacia la persona encargada de su resolución.

Los eventos y/o debilidades que se pueden reportar para su respectiva investigación, análisis y gestión deben ser los que atenten contra la confidencialidad, disponibilidad e integridad de la información, entre los cuales se pueden mencionar:

- Accesos no autorizados a los sistemas de información.
- Uso indebido de los recursos informáticos de la Entidad.
- Divulgación de información a quien no tiene derecho a conocerla.
- Uso de la información con el fin de obtener beneficio propio o de terceros.
- Hacer pública la información sin la debida autorización.
- Realización de copias no autorizadas de software.
- Descargar software a través de Internet sin la debida autorización.
- Intentar modificar, reubicar o sustraer equipos de cómputo, software, información o periféricos sin la debida autorización.
- Transgredir o burlar los mecanismos de autenticación u otros sistemas de seguridad.
- Enviar cualquier comunicación electrónica fraudulenta.
- Violación de cualquier ley o regulación nacional respecto al uso de sistemas de información.
- Robo de información sensible.
- Robo y pérdida de equipos de cómputo con información sensible.
- Denegación de servicio sobre equipos de la red, afectando la operación diaria de la Entidad.
- Denegación de servicio por el ingreso y propagación de virus que explotan vulnerabilidades.
- Amenazas a través de diferentes medios de comunicación (por ejemplo, correo electrónico) que generen un impacto directo sobre la seguridad de la información.
- Cambios o modificaciones en registros de bases de datos sin previa autorización.
- Generación o distribución de código malicioso.
- Fallas en los sistemas de información y pérdidas de servicio.
- Otros eventos y/o vulnerabilidades relacionadas con la seguridad de la información.

El catálogo de incidentes a tomar como referencia está incluido en la sección Tipos de Incidencias de Seguridad de la herramienta de apoyo al SGSI de la SIC.

7.2.2 Validar el evento de seguridad de la información

Luego de ser recibido un reporte de incidente de seguridad de la información, la Mesa de Servicios debe validar que el incidente de seguridad reportado esté relacionado con una afectación a nivel de confidencialidad, integridad o disponibilidad de algún activo de información de la SIC, de acuerdo al listado de eventos y/o debilidades relacionado en el numeral 7.2.1 de este documento. Si esta validación es positiva, la Mesa de Servicios debe comunicar el incidente vía email o por medio de un flujo programado dentro del aplicativo de gestión de incidencias al Oficial de Seguridad de la Información, o quien él delegue.

En el caso de que el incidente reportado no se trate de un incidente o de un evento de seguridad, por ejemplo, si se trata de un incidente de soporte técnico, la Mesa de Servicio procederá a tratar el incidente siguiendo los procedimientos establecidos para tal fin.

7.2.3 Valorar el impacto del incidente

El Oficial de Seguridad de la Información, o quien él delegue, determina el tipo de incidente de seguridad de la información que ha sido reportado.
Si el Oficial de Seguridad de la Información o quien él delegue, determina que no se trata de un incidente de seguridad de la información, procede a informar vía email a la persona que notificó el hecho, de las razones para no procesarlo como un incidente de seguridad. Igualmente se debe informar e instruir al usuario acerca de qué son los incidentes de seguridad de la información y cómo reportarlos. Las comunicaciones de concientización y educación dirigidas a los usuarios al respecto de incidentes de seguridad pueden realizarse utilizando los siguientes medios:

- De forma verbal con los colaboradores o áreas involucradas.
- Mediante correo electrónico.
- Capacitaciones.

Si el Oficial de Seguridad de la Información, o quien él delegue, determina que se efectivamente se trata de un incidente, éste se debe valorar en función del tipo de impacto que puede causar para la SIC. Los tipos de impactos a considerar son los siguientes:

- Confidencialidad.
- Integridad.
- Disponibilidad.

Los valores posibles para la valoración se describen en la siguiente tabla:

Niveles de impacto del incidente	Confidencialidad	Integridad	Disponibilidad
Alta	La Información es sensible para la operación de la entidad.	La información ha sido modificada en gran parte o en su totalidad de forma accidental o intencionada.	El daño estimado para la entidad en términos de tiempo (horas hombre involucradas) más de una semana laboral.
Media	La Información es medianamente sensible para la operación de la entidad.	La información ha sufrido algunas modificaciones accidentales o intencionadas.	El daño estimado para la entidad en términos de tiempo (horas hombre involucradas) está entre un día y una semana laboral.

Baja	La Información no es sensible para la operación de la entidad.	La información está libre de modificaciones no autorizadas.	El daño estimado para la entidad en términos de tiempo (horas hombre involucradas) está entre horas y un día laboral.
Desconocida	No existe un criterio para determinar la sensibilidad de la información.	No se puede determinar si la información ha sido modificada.	No se puede determinar el daño para la entidad en términos de tiempo.

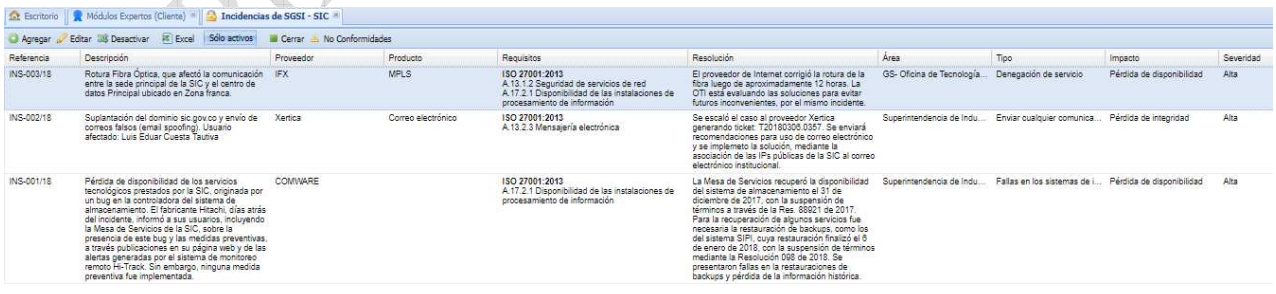
7.3 ETAPA 3: SOLUCIONAR EL INCIDENTE

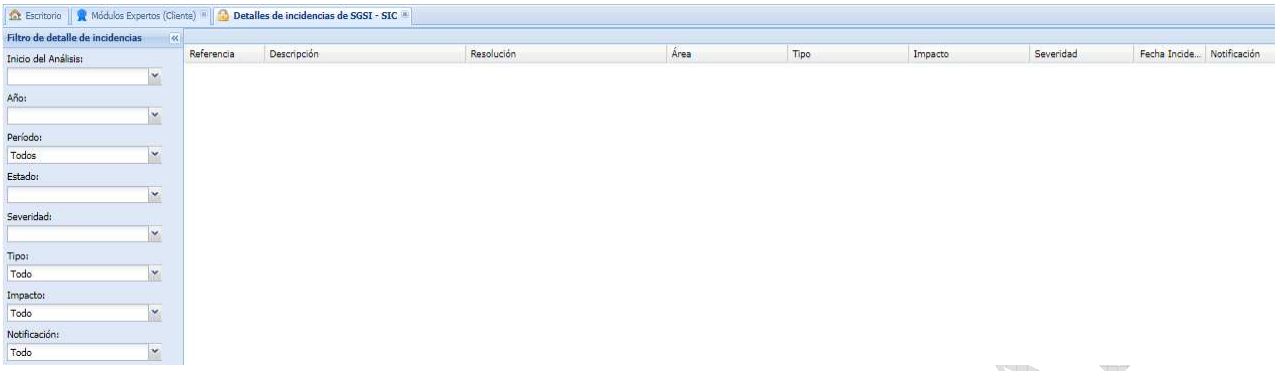
7.3.1 Definir la solución del incidente

Es importante aclarar que previo a una solución definitiva del incidente y cuando aplique, se debe implementar una respuesta inmediata con el fin de evitar mayores afectaciones a los activos de información de la SIC.

El Oficial de Seguridad de la Información, o quien él delegue, es el encargado de definir la solución al incidente reportado. En caso de ser necesario, se puede convocar a otros servidores públicos o contratistas de la SIC para aportar en la solución del incidente. En el caso de que no se encuentre una solución que dé respuesta al incidente se puede contactar grupos de apoyo como autoridades, grupos de interés externos que manejen asuntos relacionados a incidentes de seguridad de información para dar solución al mismo.

Para la definición de la solución definitiva del incidente se puede consultar en la herramienta de apoyo al SGSI de la SIC, en el módulo "ISO 27001:2013", en la sección "Incidencias", por la existencia de incidencias similares que hayan ocurrido en el pasado y que aporten en la solución del incidente actual. Igualmente se debe consultar dentro de este mismo software en la sección "Cuadro de Mandos", en la pestaña "Incidencias", por el "Detalle de Incidencias" y "Resumen de incidencias" para tener una perspectiva amplia de la frecuencia con que ocurre la incidencia, el impacto que genera y la severidad de la misma, que aporte información para la definición de la mejor solución para la incidencia.





7.3.2 Implementar la solución al incidente

El responsable de la atención de incidentes de seguridad debe llevar a cabo la implementación de la solución al incidente que se haya definido previamente. Las soluciones de incidentes que impliquen cambios sobre los activos de información que la OTI tiene a cargo, se deben llevar a cabo siguiendo el procedimiento GS01-P08 Procedimiento de Gestión del Cambio Tecnológico.
Si después de aplicar la solución al incidente, aún no se ha controlado el incidente, se retorna a la actividad anterior para redefinir la solución al incidente.

7.3.3 Notificar la solución del incidente

El responsable de la atención de incidentes de seguridad debe informar vía correo electrónico a los interesados, incluyendo al usuario que reportó el incidente, la conclusión y forma en que se resolvió y mitigó el incidente.

7.3.4 Establecer contacto con las autoridades

- Notificar la solución del incidente.
- Establecer contacto con las autoridades.

Identificar las lecciones aprendidas.

En la siguiente tabla se presentan las entidades competentes en caso de presentarse un incidente de seguridad que requiera ser notificado. En caso de requerirse a las autoridades mencionadas, sólo podrán ser contactadas por el Oficial de Seguridad de la Información, o quien él delegue:

Descripción	Organización	Contacto
Denuncias de Habeas Data y Protección de datos personales.	Superintendencia de Industria y Comercio.	http://www.sic.gov.co/ http://serviciosweb.sic.gov.co/servilinea/Servi

Descripción	Organización	Contacto
		Linea/Portada.php?cod_form=4
Cuando se tenga evidencia de un incidente informático y se requiera recibir asesoría para posterior judicialización de acuerdo con la Ley 1273 de 2009. Ejemplos: - Acceso abusivo a sistemas informáticos - Ingeniería Social - Uso de Software malicioso - Suplantación de Sitios Web - Transferencia no consentida de activos - Hurto por medios informáticos - Phishing	Centro Cibernético Policial (CCP).	https://caivirtual.policia.gov.co/ Correo electrónico: caivirtual@correo.policia.gov.co E-mail: lineadirecta@policia.gov.co
Incidentes con afectación a componentes de la infraestructura tecnológica (sitios Web, aplicaciones, servicios en línea, sistemas de información, entre otros).	COLCERT Grupo de Respuesta a Emergencias Cibernéticas en Colombia.	www.colcert.gov.co/ Línea de atención: (+ 57 1) 295 98 97 E-mail: contacto@colcert.gov.co
Incidentes con afectación a infraestructuras Criticas Cibernéticas.	Comando Conjunto Cibernético de Colombia CCOC.	(57 1) 3150111 ext. 3085 3087 2660247 Email: servicio@ccoc.mil.co ccoc@ccoc.mil.co
Requerimientos de apoyo en los siguientes temas: - Atención efectiva de eventos e incidentes, con el fin de restablecer la operación y mitigar el impacto causado. - Asistencia y atención con el fin de ayudar a tomar medidas para proteger y asegurar las plataformas tecnológicas, prever futuros ataques, dificultades o eventos que afecten la confidencialidad e integridad de la información. - Establecimiento de estándares y buenas prácticas para mejorar la seguridad de la información, generando recomendaciones, comentarios y sensibilizaciones con base en las lecciones aprendidas. - Análisis de Malware.	CSIRT-CCIT Centro de Coordinación Seguridad Informática Colombia.	https://cc-csirt.policia.gov.co Análisis de malware: https://cc-csirt.policia.gov.co/Sandbox
Incidentes relacionados con los siguientes temas:	Línea de emergencia única.	123

Descripción	Organización	Contacto
- Robo. - Acceso no autorizado. - Emergencia por incendio. - Emergencia con sustancias peligrosas (ejemplo: Gas). - Antisecuestro y Antiextorsión. - Siniestros ambientales.		

7.3.5 Identificar las lecciones aprendidas

El Oficial de Seguridad de la Información o él designado para la solución del incidente, debe identificar las lecciones aprendidas después de presentarse un incidente grave, y periódicamente después de los incidentes menores, lo cual es sumamente útil en la mejora de las medidas de seguridad y el proceso de gestión de incidentes.
Para mantener un adecuado registro de lecciones aprendidas la documentación de la lección aprendida debe permitir conocer:

- Exactamente lo que sucedió, en qué momento y cómo el personal gestionó el incidente.
- Si se tomaron las medidas o acciones que facilitaron la recuperación eficiente.
- Cuál sería la gestión de personal y que debería hacerse la próxima vez que ocurra un incidente similar.
- Las acciones correctivas que pueden prevenir incidentes similares en el futuro.
- Cuales herramientas o recursos adicionales son necesarios para detectar, analizar y mitigar los incidentes en el futuro.

Identificar los requisitos de la norma ISO 27001 afectados por el incidente. - Diligenciar los campos de registro en la herramienta de apoyo al SGSI.

7.4 ETAPA 4: DOCUMENTAR EL INCIDENTE

El responsable de la atención de incidentes de seguridad es el encargado de hacer el registro del incidente en la herramienta de apoyo al SGSI, para lo cual debe documentar el impacto del incidente, ingresar la información de descripción del incidente e indicar los requisitos de la norma ISO 27001 afectados.

7.4.1 Diligenciar los campos de registro en la herramienta de apoyo al SGSI

El responsable de la atención de incidentes de seguridad debe ingresar cada incidente en la herramienta de apoyo al SGSI de la SIC. El proceso de registro debe incluir los siguientes datos:

- Descripción: Detalle del suceso considerado incidencia de seguridad.

- Proveedor: Datos de proveedor si la incidencia tuviese relación con uno.
- Producto: Selección del producto/servicio relacionado con la incidencia.
- Tipo: Tipo de la incidencia detectada.
- Impacto: Tipo de impacto causado por la incidencia (Confidencialidad, integridad, disponibilidad).
- Severidad: Grado del impacto.
- Área: Área de la organización afectada por la incidencia.
- Fecha: Fecha en la que se sucede/descubre la incidencia.
- Notifica: Personal que notifica la incidencia.
- Notificación: Fecha en la que se notifica la incidencia.
- Registra: Personal que registra la incidencia.
- Registro: Fecha en la que se registra la incidencia.
- Resolución: Descripción de la solución o acción correctiva aplicada para dar solución a la incidencia y lecciones aprendidas.

7.4.2 Identificar los requisitos de la norma ISO 27001 afectados por el incidente

El responsable de la atención de incidentes de seguridad debe definir y diligenciar los requisitos o aspectos del SGSI que son afectados por la incidencia de seguridad de la información en la herramienta de apoyo al SGSI de la SIC. Entre estos aspectos se encuentran:

- Definición de la política de seguridad.
- Metodología de Análisis de Riesgos.
- Tratamiento de Riesgos.
- Selección de controles de seguridad, etc.

7.5 ETAPA 5: RECOLECTAR EVIDENCIA

7.5.1 Recolectar y conservar evidencia del incidente

El Oficial de Seguridad de la Información o quien él delegue, determina si el incidente amerita la recolección de evidencia digital, en cuyo caso, se procede a contactar inmediatamente al Laboratorio de Informática Forense de la SIC, con el propósito de que éste realice la recolección de la evidencia.

En general se tienen que considerar los lineamientos de las buenas prácticas de la cadena de custodia de evidencias digitales, tomando como marco general la legislación colombiana; en tal sentido, se deberán desarrollar las siguientes actividades como parte de la recolección y conservación de evidencias:

a) El primer paso comprende la captura de la evidencia, que será realizada por el Oficial de Seguridad de la Información, o quien él delegue, junto con el apoyo del Coordinador del grupo de Servicios Tecnológicos y Seguridad Digital, o quien él delegue, y las personas a cargo del proceso. La evidencia será la prueba de la infracción, la que delatará al intruso. A la hora de recaudar la evidencia, se debe proceder con cautela para no modificar pista alguna. Para recopilar estas evidencias se aplicarán las buenas prácticas de computación forense según el tipo de evidencia.

b) Se debe proceder a realizar la captura de la evidencia con herramientas que no modifiquen ni el entorno ni la prueba en sí, salvaguardando su integridad.

c) Se debe actuar con precaución a la hora de recolectar la evidencia; dado que se debe procurar la no alteración de la misma para garantizar su validez en un proceso legal. Para ello se pueden utilizar los siguientes elementos:

- Bolsas antiestáticas, que permitan la correcta manipulación de medios de almacenamiento.

- Bolsas de seguridad, para almacenar los elementos físicos, que permitan garantizar que una vez depositados, se tenga la certeza que la bolsa no ha sido abierta.

- Embalaje, para almacenar los discos duros y evitar que una eventual caída o maltrato al elemento ocasione una afectación a la integridad de la información, que en este caso sería perdida de la evidencia.

- Etiquetas o rótulos, para marcar los elementos físicos, con el fin de identificarlos. Esta etiqueta debe tener la información necesaria que identifique al elemento. Por ejemplo, si se habla de un disco duro, se debería incluir por lo menos la siguiente información:

  - Un consecutivo
  - Número del incidente.
  - Descripción del elemento (marca, modelo, serial, capacidad, tipo de conector (IDE, SCSI, SATA), configuración física, particiones, sistema operativo).
  - Fecha y hora.
  - Lugar.
  - Nombre y firma de quién recolecta el elemento. Si es posible nombre y firma de un testigo.

d) Dependiendo del tipo de incidente de seguridad y la criticidad del mismo, se determinan las actividades a seguir para la recolección y conservación de la evidencia, siguiendo los lineamientos de la cadena de custodia para cada caso específico.

e) La Superintendencia de Industria y Comercio, cuenta con un circuito cerrado de televisión, el cual tiene un monitoreo de veinticuatro (24) horas en cada una de las áreas de la Entidad. Este monitoreo queda registrado y también puede ser utilizado como evidencia en incidentes donde esté involucrado el robo de elementos, manipulación de información, ingresos indebidos de cualquier carácter, daño de activos, etc., aplicando las técnicas adecuadas de recolección y conservación de la evidencia.

f) Las tareas de recolección, así como las de análisis posteriores se realizan en conjunto entre la OTI y el Laboratorio de Informática Forense. En el caso de que haya un servidor público involucrado como sospechoso de la causa del incidente, el Grupo de trabajo de Control Disciplinario Interno también podrá participar en las actividades de análisis de la evidencia. Para la recolección y retención de las evidencias que puedan ser presentadas ante las autoridades competentes, se deberán seguir los procedimientos e instructivos indicados por el Laboratorio de Informática Forense de la Superintendencia de Industria y Comercio y los lineamientos de las buenas prácticas de la cadena de custodia de evidencias digitales, tomando como marco general la legislación colombiana.

Los incidentes de seguridad de la información sobre los cuales se va a requerir la toma de evidencia digital, serán aquellos cuya valoración de severidad sea alta y que adicionalmente deberá corresponder a algún incidente de los incluidos en la siguiente lista:

a) Cuando el equipo originador del incidente o afectado por el incidente sea un servidor que cumple una labor misional o un elemento de red:

- Modificación no autorizada de sitios web (Website Defacement).
- Ataques de denegación de servicio (Denial of Service Attacks).
- Ataques de código malicioso (Malicious Code virus/worm).
- Hackeo o intrusión (Intrusion/Hack).
- Notificaciones de IDS (IDS alert notifications).
- Espionage (Unauthorized Electronic Monitoring).
- Acceso no autorizado a sistemas de información.
- Robo de propiedad intelectual.

b) Cuando el equipo originador del incidente o afectado por el incidente es una estación de trabajo:

- Sospecha de incumplimiento al Código Único Disciplinario o la legislación aplicable según el caso, apoyándose en concepto del Grupo de trabajo de Control Disciplinario Interno.

7.6 ETAPA 7: INICIAR PROCESO LEGAL

7.6.1 Iniciar el proceso legal

En caso de que el análisis de la evidencia digital recopilada determine que se ameritan el inicio de acciones legales (civiles o penales), el Oficial de Seguridad de la Información o quien él delegue, procederá a comunicar el hecho al CIO, vía correo electrónico.

La solicitud de inicio de un proceso legal está a cargo del CIO, o de quien él delegue.

8 DOCUMENTOS RELACIONADOS

SC05-I01	Políticas del Sistema de Gestión de Seguridad de la Información SGSI.
GS01-P08	Procedimiento de Gestión del Cambio Tecnológico.

9 RESUMEN CAMBIOS RESPECTO A LA ANTERIOR VERSIÓN

1. Se ajustaron las actividades al formato procedimiento vigente en el SIGI; se ajustó el método de reporte de incidentes de seguridad; se incluyó información sobre contacto con las autoridades y grupos de interés especial.
2. Se realizó cambio de código documental debido al cambio de proceso, siendo el código anterior GS02-P03.

Fin documento