CONTENIDO

Elaborado por:	Revisado y Aprobado por:	Aprobación Metodológica por:
Nombre: Oscar Fabián Ramírez Torres Cargo: Coordinador Grupo de Trabajo de Informática Forense y Seguridad Digital.	Nombre: Jaroslav Marlen López Chávez Cargo: Jefe Oficina de Tecnología e Informática (E).	Nombre: Giselle Johanna Castelblanco Muñoz Cargo: Representante de la Dirección para el Sistema de Gestión de Calidad Fecha: 2022-12-05

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, recuperación, recolección de evidencia e inicio de procesos legales relacionado 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.

BCP (plan de continuidad del negocio): es un plan logístico para la práctica de cómo una organización debe recuperar y restaurar sus funciones críticas parcial o totalmente interrumpidas dentro de un tiempo predeterminado después de una interrupción no deseada o desastre.

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.

DRP (plan de recuperación ante desastres): es un proceso de recuperación que cubre los datos, el hardware y el software crítico, para que un negocio pueda comenzar de nuevo sus operaciones en caso de un desastre natural o causado por humanos.

EVENTO DE SEGURIDAD DE LA INFORMACIÓN: Presencia identificada de un estado del sistema, servicio o de red de datos, 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.

MSPI: Modelo de Seguridad y Privacidad 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.

PLAYBOOK: Los playbook complementan al Plan de Respuesta a Incidentes, ya que definen las líneas de acción específicas para cada tipología de incidente.

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.

SOC: Centro de operaciones de seguridad, responsable de supervisar, administrar y garantizar la seguridad de la información a través de distintas herramientas y procedimientos técnicos.

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 la generación, 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 NORMATIVAS

Jerarquía de la norma	Numero/ Fecha	Título	Artículo	Aplicación Específica
NTC-ISO-IEC	27035:2011	Tecnología de la información. Técnicas de seguridad. Gestión de incidentes de seguridad de la información.	Aplicación total	Aplicación total
Guía	1.2/2016	Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información	Aplicación parcial	Aplicación parcial

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 con el 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 ETAPA	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. Mesa de servicios.	Correo electrónico con el resultado de la aplicación de medidas preventivas.
2	DETECTAR, REPORTAR Y ANALIZAR UN EVENTO DE SEGURIDAD DE LA INFORMACIÓN	Evento de seguridad de la información.	Se deben detectar, 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. Mesa de servicios Oficial de Seguridad de la Información o quien él delegue.	Reporte del incidente a interesados (correo, mensajes, video conferencia). Documentos del análisis del evento y determinación de incidente.
3	SOLUCIONAR EL INCIDENTE DE SEGURIDAD DE LA INFORMACIÓN	Documentación inicial del incidente. Reporte a interesados.	Definir las acciones para contener el incidente e implementar la solución definitiva, a través de las siguientes actividades: - Definir la solución del incidente de seguridad de la información. - Implementar la solución al incidente de seguridad de la información. - Notificar la solución del incidente. - Establecer contacto con las autoridades.	Oficial de Seguridad de la Información o quien él delegue. Responsable de la atención de incidentes de seguridad de la información.	Resultado del análisis del incidente. Evidencias de la solución del incidente.

No.	ETAPAS	ENTRADAS	DESCRIPCIÓN DE LA ETAPA	RESPONSABLE	SALIDAS
4	DOCUMENTAR EL INCIDENTE DE SEGURIDAD DE LA INFORMACIÓN	Resultado del análisis del incidente reportado. Evidencias de la solución del incidente.	El responsable de la atención de incidentes de seguridad de la información en primer nivel es el encargado de hacer el registro del incidente en la herramienta de registro oficial para lo cual debe documentar el impacto del incidente, ingresar la descripción del incidente e indicar los requisitos de la norma ISO 27001 afectados, 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 oficial de registro del SGSI.
5	RECUPERAR Y ANALIZAR LECCIONES APRENDIDAS	Resultado del análisis de la documentación. DRP y/o BCP.	Realizar las labores de recuperación y registro de lecciones aprendidas: - Recuperar los sistemas de información y/o procesos afectados. - Definir y analizar las lecciones aprendidas.	Oficial de Seguridad de la Información o quien él delegue.	Registro en documento maestro de casos. Lecciones aprendidas documentadas y adición a playbook de ser necesario. Evidencias forenses si aplica un proceso legal.
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

En esta etapa, se establecen acciones para prevenir los incidentes de 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, mantienen 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 y 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. https://www.ccoci.mil.co/
- Centro Cibernético Policial, https://caivirtual.policia.gov.co
- 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 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: DETECTAR, REPORTAR Y ANALIZAR UN EVENTO DE SEGURIDAD DE LA INFORMACIÓN

En esta etapa, se deben detectar, reportar y analizar los eventos para determinar si corresponden a incidentes de seguridad de la información que pueden afectar la seguridad de la información de la Entidad.

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: https://aranda.sic.gov.co/usdkv8/,
- Correo electrónico: mesadeservicios@sic.gov.co,
- Llamada telefónica: Extensión 10502, que serán gestionados por el proveedor de la mesa de servicios de la SIC.

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, integridad y privacidad 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 de datos, 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 los eventos de seguridad a tomar como referencia está incluido en la Matriz de Categorización, también incluida en la herramienta de registro de casos de la SIC.

7.2.2 Validar el evento de seguridad de la información

Luego de ser recibido un reporte del evento de seguridad de la información, la mesa de servicios debe validar que el evento de seguridad reportado esté relacionado con una afectación a nivel de confidencialidad, integridad, disponibilidad y privacidad de algún activo de información de la SIC, de acuerdo con el 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 evento reportado no se trate de un incidente o de un evento de seguridad de la información, por ejemplo, si se trata de un evento o actividad de soporte técnico, la mesa de servicios de la SIC procederá a tratar el evento 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 a quien lo notifico directamente, las razones para no procesarlo como un incidente de seguridad de la información. Desde la primera línea de comunicación se informará 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 de la información 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 efectivamente se trata de un incidente de seguridad de la información, 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.
- Privacidad.

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

Niveles de impacto del incidente	Confidencialidad o privacidad	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) es de 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.

Niveles de impacto del incidente	Confidencialidad o privacidad	Integridad	Disponibilidad
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 DE SEGURIDAD DE LA INFORMACION

En esta etapa se definen las acciones para contener el incidente e implementar la solución definitiva.

7.3.1 Definir la solución del incidente de seguridad de la información

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 el playbook, en la sección que corresponda según la naturaleza del incidente, existencia de incidencias similares que hayan ocurrido en el pasado y que aporten en la solución del incidente actual.

7.3.2 Implementar la solución al incidente de seguridad de la información

El responsable de la atención de incidentes de seguridad de la información 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 DE04-P04 Procedimiento Control De Cambios, el tipo de cambio será

definido por el Oficial de seguridad de la información, junto con el líder o responsable del área al cual pertenece el sistema/dispositivo y/o proceso que requiere cambio.

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

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://servicios web.sic.gov.co/servilinea/ServiLinea/Portada.php?cod_form=4 Coordinación Del Grupo De Trabajo De Investigaciones Administrativas. 5870000 ext. 70027
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	COLCERT – Grupo de Respuesta a	www.colcert.gov.co/ Línea de atención:

Descripción	Organización	Contacto
web, aplicaciones, servicios en línea, sistemas de información, entre otros).	Emergencias Cibernéticas en Colombia.	(+ 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: - Robo. - Acceso no autorizado. - Emergencia por incendio. - Emergencia con sustancias peligrosas (ejemplo: Gases tóxicos). - Antisecuestro y antiextorsión. - Siniestros ambientales.	Línea de emergencia única.	123

7.4 ETAPA 4: DOCUMENTAR EL INCIDENTE DE SEGURIDAD DE LA INFORMACIÓN

El responsable de la atención de incidentes de seguridad de la información es el encargado de hacer el registro del incidente en la herramienta oficial de registro.

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

El responsable de la atención de incidentes de seguridad de la información 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 de la información.
- 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 de la información debe definir y diligenciar los requisitos o aspectos del SGSI que son afectados por la incidencia en la herramienta de apoyo al SGSI de la SIC. Entre estos aspectos se encuentran los numerales y controles de la norma ISO 27001.

7.5 ETAPA 5: RECUPERAR Y ANALIZAR LECCIONES APRENDIDAS

En esta etapa se realizan las labores de recuperación de sistemas de información y registro del caso como lección aprendida.

7.5.1 Recuperar los sistemas de información y/o procesos afectados

El Oficial de Seguridad de la Información o quien él delegue, junto con el administrador o dueño del proceso afectado proceden a la recuperación y restauración de estos. Después del restablecimiento será necesario verificar que el sistema y/o proceso ha sido endurecido con el propósito de prevenir incidentes similares.

Este proceso puede o no incluir la utilización del BCP o el DRP en caso de que aplique, su uso depende de la determinación de criticidad y de la decisión tomada por el oficial de seguridad y responsables.

7.5.2 Definir y analizar las lecciones aprendidas

El Oficial de Seguridad de la Información o el designado para la solución del incidente, junto con el equipo o personal interesado deben identificar las lecciones aprendidas después de presentarse un incidente, lo cual es sumamente útil en la mejora de las medidas de seguridad y el proceso de gestión de incidentes, así como para robustecer el procedimiento.

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.
- Cuáles herramientas o recursos adicionales son necesarios para detectar, analizar y mitigar los incidentes en el futuro.
- En caso de ser necesario se deben realizar adiciones al playbook.

7.6 ETAPA 6: INICIAR PROCESO LEGAL

En esta etapa, cuando se requiera puede iniciarse un 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, para iniciar los trámites respectivos a través de la Oficina Asesora Jurídica de la SIC.

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

8 DOCUMENTOS RELACIONADOS

SC05-I01 Revisión De Las Políticas Del Sistema De Gestión De Seguridad De La Información - SGSI

DE04-P04 Procedimiento control de cambios.
SC05-POL01 Políticas Del Sistema De Gestión De Seguridad De La Información - SGSI

8.1 DOCUMENTOS EXTERNOS

No aplica.

9 RESUMEN CAMBIOS RESPECTO A LA ANTERIOR VERSIÓN

1. Se ajustó la norma de referencia.
2. Cambio en la etapa 5 para ajustarse a las normas y documentos de referencia.
3. Creación de documento adicional playbook.

_____
Fin documento