1. OBJETIVO

Definir la metodología para atender los incidentes de seguridad de forma oportuna y eficaz, asegurando la seguridad de la información y la continuidad de los procesos de negocio.

2. ALCANCE

El procedimiento inicia con la creación del equipo de respuestas ante incidentes de seguridad de la Información y termina con la documentación y cierre del incidente.

3. RESPONSABLES

- Director de Seguridad de la Información
- Administrador de Infraestructura Tecnológica
- Grupo de Infraestructura Tecnológica
- Dirección Administrativa
- Funcionarios SysCafé

4. TÉRMINOS Y DEFINICIONES

- **Evento en la Seguridad de la información:** Un evento de seguridad de la información es un cambio en las operaciones diarias de una red o servicio de tecnología de la información que indica que una política de seguridad puede haber sido violada o una protección de seguridad puede haber fallado.
- **Incidente en la Seguridad de la información:** Una sola o una serie de eventos de seguridad de la información no deseados o inesperados que tienen una probabilidad significativa de comprometer las operaciones comerciales y amenazar seguridad de información. Por ejemplo, un comportamiento anómalo en un sistema es un evento, sin embargo, si se encuentra evidencia del virus en el sistema, se puede considerar un incidente de seguridad.
- **Vulnerabilidad en la Seguridad de la información:** Se refiere a una debilidad o defecto en un sistema o activo de información que puede dejarlo expuesto a una amenaza o ataque. Una vulnerabilidad también puede referirse a cualquier tipo de debilidad en un sistema de información en sí mismo, en un conjunto de procedimientos o en cualquier cosa que deje la seguridad de la información expuesta a una amenaza.

5. POLÍTICAS

- Todos los funcionarios SysCafé, clientes y proveedores deben reportar eventos, incidentes y violaciones de seguridad a su jefe inmediato o proveedor de servicio, para ser tratados de forma oportuna y eficaz.

- El tratamiento de eventos, incidentes y violaciones de seguridad deben ser tenidos en cuenta para el inicio de acciones de mejoramiento de la seguridad y para la aplicación de procesos disciplinarios cuando sea necesario.

- Este control se aplica para la atención de incidentes de seguridad en todos los procesos de la organización relacionados con:
  - ✓ Aplicación de actividades de monitoreo de la seguridad.
  - ✓ Reporte de empleados, contratistas y otras partes interesadas.

- Todos los funcionarios SysCafé permanecen vigilantes ante cualquier actividad fraudulenta o que pueda comprometer la seguridad de la información y en consecuencia deben reportar inmediatamente cualquier violación de la seguridad al director de seguridad de la información y grupo de apoyo.

- Los incidentes con implicaciones legales tienen un tratamiento especial.

6. DESCRIPCIÓN GENERAL

Se llevan a cabo las siguientes actividades:

- Reporte incidente de seguridad.
- Registro y diagnóstico.
- Contención del incidente.
- Recolección de Evidencia.
- Solución del incidente.
- Análisis e Investigación del Incidente.
- Reporte Autoridades / Sanciones Disciplinarias.
- Generación de problemas de seguridad.
- Acción correctiva, preventiva y de mejora.

6.1 Reporte incidente de seguridad

La persona que detecta el incidente lo reporta inmediatamente al **Grupo de Infraestructura** o al **Director de Seguridad de la Información**. Puede hacerse verbalmente, por correo electrónico o en el Aplicativo GLPI. Cualquier evidencia o soporte del incidente que se tenga debe anexarse.

6.2 Registro y diagnóstico

Los incidentes de seguridad de información reportados son clasificados por el director SI para determinar su gravedad según el impacto en la información y/o sistemas de información comprometidos y tomar la acción correspondiente de acuerdo con los criterios establecidos en el Instructivo Tratamiento de Incidentes de Seguridad.

El Administrador de Infraestructura Tecnológica hace el diagnóstico del incidente, para determinar las posibles causas y definir si se requiere una acción de contención inmediata antes de dar una solución definitiva. Para el diagnóstico se realizan las siguientes actividades:

- Identificación de la falla, error o incidente.
- Pruebas de la falla
- Identificación de causa (error humano, falla de equipos, error de software, causa ambiental, personas maliciosas, códigos maliciosos, ataque de seguridad etc.)
- Recolección de evidencia.
- Posibles soluciones.

6.3 Contención del Incidente

Para incidentes graves, *el* ***Grupo de Infraestructura Tecnológica*** debe tomar acción de contención de la amenaza inmediatamente y escalar al **Director de Seguridad de la Información**. La acción de contención puede implicar suspender el servicio afectado únicamente, suspender todo el servidor o toda la red, o incluso suspender la operación del área afectada y activar el Plan de Disponibilidad y Continuidad del Negocio.

6.4 Recolección de Evidencia

Los incidentes graves que deben ser reportados a las autoridades o que tienen sanciones disciplinarias asociadas, requieren recolección de evidencia antes de proceder. **El Director Seguridad de la Información** recolecta esta evidencia lo más pronto posible (incluso durante la ocurrencia del incidente mismo) para garantizar la cadena de custodia. Es importante que quien reporta no tome ninguna acción para permitir la investigación y documentación del incidente.
El material que constituye la evidencia debe registrarse en un repositorio de la configuración con control de acceso y estricto control de cambios para evitar que sea manipulada.

La evidencia recolectada debe cumplir con los siguientes principios:

- **Relevancia**: La evidencia debe vincular al sujeto con el incidente, probar alguna hipótesis de caso de estudio y validar un indicio clave que permita esclarecer los hechos en estudio.

- **Confiabilidad**: Los procedimientos efectuados sobre los dispositivos tecnológicos deben ser previamente probados, se conoce la tasa de error de las herramientas forenses informáticas utilizadas.

- **Suficiencia**: La evidencia recolectada debe estar basada y apoyada en la situación que se debe probar, además que se deben involucrar todos los elementos informáticos relacionados con los incidentes teniendo en cuenta aquellos que posiblemente fueron eliminados.

Para incidentes no graves, la recolección de evidencia no es obligatoria y puede manejarse como datos adjuntos en la herramienta donde se reportan los incidentes.

6.5 Solución del Incidente

El **Director de Seguridad de la Información y el Administrador de Infraestructura** se encargan de la solución del incidente. Consiste en implementar las acciones que restablecen el funcionamiento del servicio/aplicación que ha presentado fallas, corregir errores en la información y prevenir daños mayores, de acuerdo con los lineamientos del instructivo Tratamiento de Incidentes de Seguridad.
Una vez aplicada la solución se hacen pruebas de funcionamiento con el usuario (fallas de hardware /software) y/o monitoreo de seguridad para verificar que la causa ha sido eliminada de forma definitiva y que el usuario ha quedado satisfecho con la solución o el riesgo de seguridad de la información ha sido mitigado

Cuando la solución de un incidente cause cambios en la configuración de los sistemas de procesamiento de información, se aplica este proceso debe seguirse los lineamientos del Procedimiento de Administración de la Configuración IT.

Luego de atender el incidente y solucionarlo, se procederá a informar a la persona que reportó el incidente de seguridad.

6.6 Análisis e Investigación del Incidente

La solución puede ser de carácter temporal y requerir análisis adicionales para implementar soluciones definitivas, desarrollar acciones de mejora de la seguridad y/o ejecutar acciones legales contra los responsables.

El **Director de Seguridad de la Información** analiza los incidentes de seguridad teniendo en cuenta:

- Recurrencia de los casos / probabilidad
- Impacto en la información y aplicaciones / servicios.
- Costos de los incidentes
- Análisis forense de la evidencia recolectada.
- Salvaguardas y medidas de contingencia

Según el alcance y naturaleza del caso se puede requerir el uso de técnicas de análisis de causa o herramientas especiales de monitoreo o de seguridad. La evidencia forense recolectada inicialmente puede ser muy útil para realizar un análisis a fondo. Puede ser necesario recurrir a firmas consultoras especializadas para una investigación especializada si no se tiene el conocimiento suficiente al interior de la organización.

6.7 Reporte Autoridades / Sanciones Disciplinarias

El **Director de Seguridad de la Información** puede reportar el incidente a las autoridades legales porque incumple algunas de las leyes relacionadas con la seguridad de la información; o recibir sanciones disciplinarias dentro de la organización porque incumple gravemente alguna de las políticas de seguridad establecidas.

Antes de proceder debe garantizarse la validez de la evidencia recolectada y realizar un análisis e investigación del incidente para no incurrir en falsos positivos o en errores que puedan comprometer legalmente a la organización.
Las sanciones disciplinarias se manejan como anotaciones en la Historia Laboral del empleado y/o observaciones en la evaluación del desempeño.
Para incidentes muy graves, la sanción disciplinaria puede implicar la terminación unilateral de la relación laboral.

6.8 Generación de Problema de seguridad

Después de realizar el análisis e investigación del incidente, si se evidencia que este ha sido repetitivo, el **Director de Seguridad de la Información** debe generar Acciones Correctivas y de Mejora en el formato correspondiente.

6.9 Acción correctiva, preventiva y de mejora

Luego del análisis e investigación de un incidente de seguridad, el director SI puede requerir el inicio de acciones correctivas, preventivas o de mejora para eliminar la causa raíz del problema identificado. Esta solución puede implicar cambios en los sistemas, nuevos recursos, compras de repuestos, equipos, dispositivos y software. También puede implicar cambios a las políticas de seguridad de la información e implementación de nuevos controles de seguridad.

El **Director de Seguridad de la Información** periódicamente hace balances consolidados de los incidentes de seguridad presentados para evaluar el estado actual de la seguridad de la información y desarrollar acciones de mejoramiento. Este es el caso, por ejemplo, de los análisis realizados anualmente durante la revisión del sistema de gestión de seguridad de la información.

7. CONTROL DE CAMBIOS

CONTROL DE CAMBIOS

N° Versión	Fecha de cambio			Descripción de cambios	Numeral(es)	Responsable
	Mes	Dia	Año			
1	06	30	2020	Versión inicial del procedimiento	Todo el documento	José Omar Mayorga Pabón, Gerente General
2	12	12	2022	Ajuste del formato del procedimiento	Todo el documento	Jorge Armando Varela Rendón, Asesor en Gestión Documental
3	01	09	2024	Actualización Documento	Todo el documento	Diana Karime Cruz Celis
4	10	25	2024	Actualización Documento	Todo el documento	Diana Karime Cruz Celis