GESTIÓN DE INCIDENTES SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Elaboró:	Revisó:	Aprobó:
Contratista Seguridad de la Información	Director Gestión de Recursos Tecnológicos	Rector(a)

1. OBJETIVO

Establecer las actividades y condiciones necesarias para la prevención, detección, identificación, manejo y control de incidentes de seguridad de la información en la Institución Universitaria Colegio Mayor del Cauca (IUCMC) con el fin de buscar soluciones oportunas y eficaces.

2. ALCANCE

El presente documento y sus actividades aplican para todos los incidentes de seguridad de la información que se presenten en la institución. Este documento debe ser conocido y aplicado por todos los funcionarios y contratistas de la institución.

Este procedimiento inicia con la prevención de los incidentes, cubre la detección e identificación, y finaliza con el control y registro del incidente con la finalidad de que sirva de base para el aprendizaje y la mejora continua, evitando futuras materializaciones de los mismos en el futuro.

3. DEFINICIONES

Consecuencia: Resultado de un evento que afecta a los objetivos.
Contención: Acciones necesarias para garantizar el control del incidente mientras se realiza un análisis más detallado y se definen las acciones necesarias para remediar el incidente.
Criterios de decisión: Umbrales, objetivos o patrones utilizados para determinar la necesidad de una acción o de una mayor investigación, o para describir el nivel de confianza en un resultado determinado.
Evento: Aparición o cambio de un conjunto particular de circunstancias.
Eventos en seguridad de la información: Ocurrencia identificada de un sistema, servicio o estado de la red que indica una posible violación de la política de seguridad de la información o el fracaso de los controles, o una situación previamente desconocida que puede ser la pertinente a seguridad.
Gusano: Programa que se reproduce por sí mismo, puede viajar a través de redes y difundirse a través de estas generando intenso tráfico para volverlas lentas.
Gestión de Incidentes de Seguridad de la Información: Procesos para detectar, informar, evaluar, responder, tratar, y aprender de los incidentes de seguridad de la información.
Incidente en seguridad de la información: Un evento o una serie de eventos de seguridad de la información no deseados o inesperados, que tienen una probabilidad significativa de comprometer las operaciones de la organización y amenaza la seguridad de la información.
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.
Log's: Registro de los sistemas de información que permite verificar las tareas o actividades realizadas por un determinado usuario o sistema.

Malware: Malicious software, Código malicioso. Programa informático diseñado para realizar acciones no deseadas o perjudiciales para el usuario legítimo de una computadora.
Parches de Seguridad: Conjunto de archivos adicionales al software original de una herramienta o programa informático, que sirven para solucionar sus posibles carencias, vulnerabilidades, o defectos de funcionamiento.
Phishing: Suplantación de identidad, clonación de una página o abuso informático para adquirir información.
Snnifer: Es un analizador de paquetes. Un programa que captura las tramas o mensajes que viajan a través de una red de computadoras.
Virus Troyano: Virus informático que ingresa al sistema a través de otro archivo.

4. DOCUMENTOS Y REGISTROS

DOCUMENTOS Y REGISTROS	CÓDIGO
Formato Incidentes de seguridad de la información	104.01.02.R.23

5. DESARROLLO

5.1 PREPARACIÓN, CONTEXTO, CONTROL Y APRENDIZAJE

La preparación y contexto de la gestión de incidentes contiene las actividades previas requeridas para enfrentar o dar un adecuado manejo a los incidentes. Estas actividades se describen a continuación:

5.1.1 Prevención de Incidentes

La gestión de incidentes tiene como objetivo principal la atención, tratamiento y respuesta eficaz a cualquier incidente que afecte la disponibilidad en la prestación del servicio de la institución.

El proceso de prevención de incidentes incluye todas aquellas actividades de tipo proactivo que puedan llevarse a cabo con el fin de estar preparado para responder y enfrentar incidentes de seguridad. Entre las actividades principales para prevenir incidentes de seguridad se encuentran las capacitaciones a los funcionarios y contratistas de la institución, la identificación de riesgos y la aplicación de controles de seguridad de la información en la institución.
Para la prevención de incidentes es necesario realizar una serie de actividades por parte de los funcionarios y contratistas responsables de los activos de información de la institución, tales como:

a. Análisis anual de riesgos en seguridad de la información o cada vez que se produzca un cambio significativo en la institución o en la infraestructura, tomando como referencia el plan de tratamiento de riesgos de seguridad y privacidad de la información
b. Auditorías anuales de seguridad de la información.
c. Pruebas técnicas de seguridad, mínimo una vez al año.
d. Administración de actualizaciones de software.
e. Aseguramiento de los equipos de cómputo, activos críticos y ciberactivos.
f. Aseguramiento de la red de comunicaciones.
g. Prevención de código malicioso.
h. entrenamientos y sensibilizaciones a los funcionarios y contratistas en seguridad de la información. Mínimo una vez al año.

5.1.2 Identificación, detección y reporte

En la medida que un funcionario, contratista o personal con acceso a los activos de información sensible de la institución note que se está presentando un ataque, sea conocedor de que alguna persona está violando las políticas de seguridad de la información o en general, conozca de riesgos asociados a los activos de información sensible, debe proceder a reportar esta situación como un evento o incidente de seguridad a través del envió de un correo electrónico o llamada telefónica al responsable de atender el incidente, para el caso del correo electrónico se debe adjuntar el formato de incidentes de seguridad, diligenciado del numeral 1 al 4. El responsable de atender el incidente escalará el ticket al líder de seguridad de la información.

5.1.3 Registro de Incidentes de Seguridad de la Información

El líder o responsable de seguridad de la información toma los datos necesarios y realiza el registro correspondiente, categorizando si se trata de incidente o evento, fecha y hora, breve descripción de lo ocurrido, identificación o validación de la vulnerabilidad y la solución aplicada, para tal fin, se diligencian los numeral 5 a 14, del formato de incidentes de seguridad de la información.
El líder de seguridad de la información llevará un control del número consecutivo de cada evento y/o incidente.

5.1.4 Priorización del Incidente

El líder de seguridad de la información evaluará que tipo de incidente es el que se presenta, a que activos está afectando, cual es alcance del mismo y que pronóstico de expansión tiene, así como los daños potenciales o reales que se generen.
La priorización de los incidentes estará ligada al nivel de impacto y de urgencia del incidente de seguridad de la información, teniendo en cuenta la afectación sobre uno o varios activos de información.

- Impacto: Determina la importancia del incidente dependiendo de cómo éste afecta la prestación del servicio de energía eléctrica, número de usuarios, activos críticos, ciberactivos o información sensible afectada, y la importancia de los mismos para la institución.

- Urgencia: Depende del tiempo máximo de demora que acepte el usuario para la resolución del incidente y/o el nivel de servicio.

La siguiente figura, corresponde al diagrama de prioridades en función de la urgencia y el impacto del incidente de seguridad de la información:

PRIORIDAD		IMPACTO			
		Menor	Moderado	Mayor	Bloqueante
URGENCIA		1	2	3	4
Urgente	4	4	8	12	16
Alta	3	3	6	9	12
Normal	2	2	4	6	8
Baja	1	1	2	3	4

Figura 1. Diagrama de prioridades

URGENCIA	
Urgente	El incidente requiere atención inmediata y recuperación de los procesos afectados o la prestación del servicio de energía eléctrica de forma inmediata.
Alta	El incidente requiere especial atención ya que ha afectado en forma parcial la prestación del servicio de energía eléctrica por parte de la institución.
Normal	El incidente requiere atención media debido a que afecta la continuidad de un proceso en forma parcial.
Baja	El incidente no requiere atención urgente, no afecta la continuidad de ningún proceso en la institución.

Tabla 1. Criterios Urgencia

IMPACTO	
Bloqueante	El incidente afecta de manera total la continuidad en la prestación del servicio de energía eléctrica por parte de la institución.

IMPACTO	
Mayor	El incidente afecta la continuidad del 70% de los procesos críticos de la institución.
Moderado	El incidente afecta de manera parcial los procesos críticos.
Menor	El incidente afecta de manera mínima los procesos de la institución.

Tabla 2. Criterios Impacto

Además, se debe tener en cuenta el tiempo de respuesta del incidente de seguridad de la información de acuerdo con el nivel de prioridad, así:

- **Crítico: 0 - 8 horas**; Se debe restablecer en el menor tiempo posible para no generar problemas legales, económicos o de imagen a la institución.
- **Alto: 8 - 16 horas**; En caso de no restablecer las actividades en un tiempo menor a 12 horas, la institución empieza a tener problemas de imagen, financieros o legales.
- **Medio: 16 - 48 horas**; El incidente tiene una prioridad Media debido a que afecta en forma parcial la continuidad en la prestación del servicio de energía eléctrica por parte de la institución en caso de llegar a las 36 horas sin solución.
- **Bajo: >=48 horas**; El nivel de prioridad es bajo debido a que el incidente no afecta la continuidad de la prestación del servicio por parte de la institución.

5.1.5 Respuesta: Contención, erradicación y recuperación

Las opciones o estrategias para la solución de los eventos o incidentes de seguridad de la información son:

5.1.5.1 Aspectos en las estrategias de contención

- Daño potencial de recursos a causa del incidente de seguridad de la información.
- Necesidad de preservación de la evidencia.
- Tiempo y recursos necesarios para poner en práctica la estrategia.
- Efectividad de la estrategia.
- Duración de las medidas a tomar.
- Criticidad de los sistemas afectados.
- Características de los posibles atacantes.
- Si el incidente es de conocimiento público.
- Pérdida económica.
- Posibles implicaciones legales.

El líder de seguridad de la información junto con el responsable de los activos de información define la estrategia de contención.

5.1.5.2 Recolección de evidencia

Para la recolección de evidencia es necesario tener en cuenta los siguientes criterios:

• Información basada en la red: Log´s de IDSs o IPSs, logs de monitoreo, información recolectada mediante Sniffers, logs de routers, logs de firewalls, información de servidores de autenticación.

- Información Basada en el Equipo:
  - Live data collection: Fecha y hora del sistema, aplicaciones corriendo en el sistema, conexiones de red establecidas, puertos abiertos, aplicaciones escuchando en dichos puertos, estado de la tarjeta de red.

  - Otra información: Testimonio de funcionario o contratista que reporta el evento o incidente.

5.1.5.3 Manejo de evidencias

Para el manejo de la evidencia se deben aplicar las políticas de seguridad y privacidad de la información.

5.1.5.4 Identificación de fuentes de ataque

Entre las posibles fuentes que se deben tener identificadas se encuentran:
- Funcionarios o contratistas descontentos.
- Baja concientización.
- Crecimiento de redes.
- Falta de previsión de contingencias.
- Falta de políticas.
- Desastres naturales.

Entre los posibles ataques que pueden ser identificados se encuentran:
- Malware (Virus, Caballos de Troya, ransomware, etc.)
- Explotación de Vulnerabilidades, tanto a nivel de host, como de arquitectura de red (vulnerabilidades de seguridad perimetral).
- Falsificación de identificadores (biométricas, de autenticación o de encabezado de paquetes).
- Robo de Información confidencial.
- Violación a la privacidad.
- Ingeniería social.
- Denegación de servicios.

5.1.5.5 Indicadores

Los indicadores son señales que advierten que un incidente ocurrió o está ocurriendo en este momento.

- Aviso de IDS sobre Buffer overflow.
- Antivirus detecta a troyano en equipo de cómputo.
- Acceso lento a internet.
- Bloqueo de cuenta por intentos fallidos de login.
- Aviso de un usuario por robo de datos.
- Acceso físico o lógico no autorizado.

5.1.5.6 Estrategias de erradicación

Para decidir/definir las estrategias de erradicación es necesario tener en cuenta:

- Tiempo y recursos necesarios para poner en práctica la estrategia.
- Efectividad de la estrategia.
- Pérdida económica.
- Posibles implicaciones legales.
- Relación costo-beneficio de la estrategia.
- Experiencias anteriores.
- Identificación de los procedimientos de cada sistema operativo comprometido.
- Identificación de usuarios o servicios comprometidos para proceder a eliminarlos.

5.1.5.7 Estrategias de recuperación

Para decidir y/o definir las estrategias de erradicación es necesario tener en cuenta:

- Cargar la copia de respaldo actualizada del sistema de información, configuración y/o base de datos.
- Creación nuevamente de la información digital o física, configuración de sistemas operativos, sistemas de información y carga manual de la información.
- Actualización o instalación de parches de seguridad a los sistemas que se vieron comprometidos.

- En el formato de registro de incidentes de seguridad de la información, se debe diligenciar en el numeral 12, la solución del incidente y la actividad que se realizó de forma inmediata.

5.1.5.8 Plan de comunicación

Para el plan de comunicación es necesario tener en cuenta los niveles de escalamiento y los requisitos de seguridad y privacidad de la información sugeridos por el Ministerio TIC (diagnostico MSPI), debe reportar en primera instancia al líder de Gestión de Recursos

Tecnológicos y de acuerdo al impacto se dará parte al proceso Gestión y Desarrollo del Talento Humano y Gestión jurídica y esta última autoriza se deberá realizar reporte a las siguientes direcciones de correo: ponal.csirt@policia.gov.co (Centro de respuesta a incidentes de seguridad informática de la Policía Nacional), igualmente a incidentesseginf@mintic.gov.co (equipo de coordinación de incidentes de seguridad de la información del Ministerio de Tecnologías de la Información y las Comunicaciones) o comunicarse con el siguiente número telefónico en Bogotá 3159090 (CSIRT de la Policía Nacional).

Aquellos incidentes de seguridad de la información que estén relacionado con afectación de datos personales en la institución deben ser evaluados por el proceso Gestión Jurídica y si se requiere se debe realizar comunicación detallada mediante la construcción de informes internos que deben ser reportados a la Superintendencia de Industria y Comercio y los titulares afectados en el incidente mencionando como mínimo:

- Descripción del incidente
- Hora y fecha de inicio del incidente y de finalización
- Cantidad de titulares afectados en el incidente
- Posibles consecuencias al titular
- Tipo de información comprometida en el incidente
- Medidas tomadas por parte de la institución para mitigar cualquier impacto.

Si el incidente es considerado un delito informático y requiere de una denuncia penal según lo establecido en la ley 1273 de 2009 debe comunicarse a:

- POLICÍA NACIONAL, Unidad de Delitos Informáticos: Dirección de Investigación Criminal "DIJIN", Grupo de Investigaciones Tecnológicas - Avenida Calle 26 No. 75 - 25 Barrio Modelia – Bogotá. Teléfonos: 57(1)4266301 - 57(1)4266302

- CAI VIRTUAL (información unidades en delitos informáticos a nivel nacional)
  Web: http://www.ccp.gov.co Email: caivirtual@delitosinformaticos.gov.co

De ser necesario, se debe informar al proceso de Gestión y Desarrollo del Talento Humana o quien realice sus funciones para aplicar las acciones disciplinarias correspondientes, en caso de identificarse que el responsable sea interno.

5.1.6 Actividades post-incidentes

5.1.6.1 a. Lecciones Aprendidas

Cada vez que se convoque el Comité de Seguridad, el líder o responsable de seguridad de la información llevará el listado y análisis de los eventos e incidentes de seguridad de la información presentados durante el periodo.

Se buscará definir esquemas más efectivos para responder ante situaciones que afecten la seguridad de la información en la institución. Entre las actividades que se realizan están:

- Mantener la documentación de los eventos e incidentes de seguridad de la Información.
- Crear bases de datos de conocimientos.
- Integrar los eventos e incidentes a la matriz de riesgos de los activos.
- Realizar entrenamientos y sensibilizaciones a los funcionarios y contratistas de la institución en lo relacionado a eventos e incidentes de seguridad de la información.
- Analizar los hechos y tomar decisiones.
- Implementar controles preventivos.

5.1.6.2 Uso de los datos y evidencias recolectadas

Los datos y evidencias recolectadas de eventos e incidentes deben ser almacenados para futuras investigaciones e implementación de controles preventivos o de mejoramiento. La información que debe ser almacenada y custodiada por el líder o responsable de seguridad de la información incluye:

- Cantidad de incidentes presentados y tratados.
- Tiempo asignado a los incidentes.
- Daños ocasionados y pérdidas.
- Vulnerabilidades explotadas.
- Cantidad de activos de información involucrados.
- Frecuencia de ataques.

5.1.6.3 Retención de las evidencias

Las evidencias retenidas deben cumplir con un control de seguridad que garantice la confidencialidad, integridad y disponibilidad de la información. El almacenamiento físico seguro de las evidencias estará bajo custodia del líder o responsable de seguridad de la información.

5.2 RESPONSABILIDADES

5.2.1 Líder de seguridad de la información:

- Mantener actualizada la política y los procedimientos para su implementación
- Velar por la divulgación y mantenimiento de las políticas y procedimientos
- Diligenciar el formato de incidentes de seguridad de la Información
- Verificar el cumplimiento del presente procedimiento al interior de la institución

5.2.2 Líder de gestión de Recursos Tecnológicos:

- Adelantar las gestiones operativas necesarias para dar cumplimiento al presente procedimiento.
- Escalar al líder de seguridad de la información cualquier circunstancia que se salga del presente lineamiento.

5.2.3 Líder de Gestión y Desarrollo del Talento Humano:

- Incluir en el plan de capacitación anual de la institución la aplicación del procedimiento de incidentes de seguridad de la información.
- Velar por que se haga la ejecución completa del plan de capacitación
- Garantizar que todos los funcionarios, contratistas y terceros vinculados reciban la capacitación en gestión de incidentes de seguridad de la información.

5.2.4 Funcionario y contratistas:

Reportar cualquier evento o incidente de seguridad de la información que se presenten en la institución.

5.3 GESTIÓN DE ACTIVIDADES

ACTIVIDADES	RESPONSABLE	REGISTRO
Contiene las actividades de tipo proactivo que puedan llevarse a cabo con el fin de estar preparado para responder y enfrentar incidentes de seguridad. Ver numeral 5.1.1 del presente documento.	Líder de Seguridad de la Información	No aplica
La detección y reporte de los incidentes se menciona en el numeral 5.1.2 del presente documento.	Funcionarios y contratistas de la Institución	Ticket mesa de ayuda, correo electrónico
Debe llevarse a cabo el registro de incidentes según lo estipulado en el numeral 5.1.3 del presente documento.	Líder de Seguridad de la Información	Formato evento o incidente de seguridad de la información.
Se realiza la priorización del incidente de acuerdo con lo referido en el numeral 5.1.4 del presente documento.	Líder de Seguridad de la Información	Formato de Incidentes de Seguridad de la Información.
Las actividades de contención, erradicación y recuperación deben estar alineadas con lo descrito en el	Líder de Seguridad de la Información / Líderes de proceso afectado	

numeral 5.1.5 del presente documento.		
La comunicación debe ser de acuerdo con lo descrito en el numeral 5.1.5.8	Líder de Seguridad de la Información	
Las lecciones aprendidas, uso de datos, evidencia recolectada y su retención se describen en el numeral 5.1.6 del presente documento.	Líder de Seguridad de la Información / funcionarios	Indicadores de seguridad

6. DOCUMENTOS DE REFERENCIA

No aplica.

7. DISPOSICIONES FINALES

7.1 DIFUSIÓN

El personal autorizado por el proceso Gestión de Recursos Tecnológicos realizará la socialización y/o difusión de esta política a la comunidad universitaria y grupos de interés, de acuerdo a las directrices del documento 104.01.02.D.13 Plan de sensibilización de seguridad de la información.

7.2 ACTUALIZACIÓN

Para garantizar la vigencia, mejora continua y actualización de este procedimiento, deberá ser revisada por lo menos una vez por año por personal competente y autorizado del proceso Gestión de Recursos Tecnológicos y será el comité integral de planeación y gestión quien avale las mejoras a implementar.

Durante la actualización se deberá tener en cuenta la normatividad vigente, lineamientos institucionales y resultado de auditorías de seguridad y privacidad de la información.

7.3 SANCIONES

El incumplimiento de esta política se aplicará la normativa vigente en la Institución Universitaria Colegio Mayor del Cauca, además de las normas emitidas a nivel nacional y regional.

8. ANEXOS

No aplica

9. CONTROL DE CAMBIOS

FECHA DE CAMBIO	CAMBIO REALIZADO
2 de diciembre de 2019	Actualización del procedimiento, corrección de procesos involucrados, se normalizó la nomenclatura y se hizo revisión general.
16 de junio de 2021	Se actualiza código del documento, según nueva TRD. Se actualiza documentos de referencia y sus códigos.
14 de junio del 2022	Se realizó revisión de la política en todos sus aspectos con el equipo de seguridad de la información donde se considera que actualmente no requiere modificación relevante a la fecha evaluada a excepción de una actualización en el apartado sanciones. Se realizó actualización de cargo de Asesor TIC a Director de Gestión de Recursos Tecnológicos.
6 de septiembre de 2022	Se actualizó código del procedimiento, según TRD. Se actualiza denominación del proceso, según nuevo mapa de procesos. Se actualiza código de documentos de referencia.
13 de octubre de 2022	Se actualiza el procedimiento según revisión realizada por el proceso de Gestión de Recursos Tecnológicos.