PROCEDIMIENTO DE GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN
DOCUMENTO INSTITUCIONAL

MACROPROCESO: PLANEACIÓN ESTRATÉGICA
PROCESO: Sistemas de Información
DEPENDENCIA / PROGRAMA: Vicepresidencia
Versión: 1

1 OBJETO

Gestionar de forma oportuna los eventos e incidentes de Seguridad de la Información relacionados con la perdida de Confidencialidad, Integridad y Disponibilidad de la información de la Universidad Piloto de Colombia.

2 ALCANCE

Aplica para la gestión de todos los Eventos e Incidentes de Seguridad de la Información al interior de la Universidad Piloto de Colombia, iniciando desde el reporte hasta el cierre y finalización del incidente, comprendiendo las siguientes actividades:

- Reporte y registro del evento y/o incidente de seguridad de la información.
- Evaluación inicial del reporte.
- Análisis y evaluación del impacto.
- Aplicación de acciones de contención y acciones complementarias.
- Documentación de lecciones aprendidas.
- Notificación de cierre del evento y/o incidente.

Este procedimiento requiere del cumplimiento por parte de empleados, estudiantes y terceros

3 CONTENIDO

3.1 DESCRIPCIÓN DE ACTIVIDADES

3.1.1 Procedimiento de Gestión de Incidentes de Seguridad de la Información

Actividad	Descripción	Responsable
1. Reportar	Todos los funcionarios, estudiantes y terceros deben reportar cualquier evento y/o incidente de seguridad de la información, a través de los siguientes canales:	Funcionarios Estudiantes

PROCEDIMIENTO DE GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN
DOCUMENTO INSTITUCIONAL

MACROPROCESO: PLANEACIÓN ESTRATÉGICA
PROCESO: Sistemas de Información
DEPENDENCIA / PROGRAMA: Vicepresidencia
Versión: 1

Actividad	Descripción	Responsable
	- Correo institucional de centro de servicio de tecnología Citius - Línea de Atención telefónica: 571-3322900 Extensión 10000 Sin excepción, sea cual sea el medio por el cual se reportó el evento y/o incidente de Seguridad de la Información, deben quedar registradas en la herramienta de gestión.	Terceros
2. Categorizar y Registrar	El Centro de Servicios de Tecnología recibe el reporte del evento y/o incidente de seguridad de Seguridad de la Información, lo identifica, registra, clasifica y escala inmediatamente al Especialista de Seguridad Informática y al Oficial de Seguridad.	Centro de Servicio de Tecnología
3. Recolectar Información	El Oficial de Seguridad debe realizar la evaluación inicial que involucra el análisis de la información descrita en el reporte e información adjuntada, si existe. Además, de ser necesario, el Oficial de Seguridad debe establecer comunicación con el personal involucrado para así recolectar la información necesaria que permita precisar la clasificación del reporte. El reporte puede ser clasificado en: ✓ Evento de seguridad de la información. ✓ Incidente de seguridad de la información. ✓ Falsa alarma. Son catalogados incidentes de seguridad de la información los que coincidan con las siguientes causas: • Ejecución de Denegación de Servicio. • Hacking. • Ejecución de Pruebas Maliciosas o Escaneos de Red. • Contraseñas comprometidas. • Llaves de cifrado comprometidas. • Suplantación de sitios Web Phishing. • Suplantación de identidad de funcionarios.	Oficial de Seguridad

Actividad	Descripción	Responsable
	• Eavesdropping: Escuchar Secretamente y sin autorización llamadas o comunicaciones. • Introducción de código malicioso (Virus, gusanos, troyanos) • Ingeniería social. • Distribución de spam. • Acceso no autorizado a sistemas de información o redes. • Cambio de privilegios sobre sistemas de información sin autorización. • Modificación o inserción de transacciones, archivos o bases de datos sin autorización. • Descarga o envió de contenido inapropiado. • Divulgación no autorizada de información del negocio. • Piratería de software. • Robo de información de negocio. • Robo de información personal de clientes y/o funcionarios (ej.: Phishing). • Pérdida o hurto de equipo de cómputo. • Robo de software. • Robo de información de autenticación. • Daño o pérdida de los servicios o enlaces de comunicaciones. • Pérdida de energía. • Daño o pérdida de los equipos del Centro Alterno de Datos. Si el reporte corresponde a una *falsa alarma*, se debe documentar en el sistema la justificación de la decisión y posteriormente se debe cerrar y notificar a los interesados. Si el evento o incidente de seguridad de la información, atenta contra los sistemas de información o bases de datos que contienen datos personales y es catalogado como crítico entrañando un alto riesgo para los derechos y libertades de los titulares de la información se procederá sin dilación a realizar la actividad # 8 y # 9.	

PROCEDIMIENTO DE GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN
DOCUMENTO INSTITUCIONAL

MACROPROCESO: PLANEACIÓN ESTRATÉGICA
PROCESO: Sistemas de Información
DEPENDENCIA / PROGRAMA: Vicepresidencia
Versión: 1

Actividad	Descripción	Responsable
4. Análisis y Evaluación del Impacto	El oficial de Seguridad de la Información debe determinar: ➢ Valorar el Impacto (Confidencialidad e Integridad). ➢ Valorar la Urgencia (Disponibilidad). ➢ Determinar de la Prioridad (Impacto * Urgencia). ➢ Afectación. ➢ Causas o Tipo de Ataque. Adicionalmente, el Oficial de Seguridad debe informar al Especialista de Seguridad Informática para planear las actividades enfocadas a contener, controlar y restaurar a la normalidad las operaciones afectadas por el incidente, esto mediante las siguientes tareas, las cuales deben ser documentadas en el sistema, las acciones pueden ser: La criticidad para clasificarla en función de su impacto, y establecer el nivel de prioridad en la resolución de cada incidente de Seguridad de la Información. Se categorizan las incidencias en los siguientes términos: Critica Grave Moderada Leve ➢ Acciones de contención (Si se requieren). ➢ Acciones complementarias (Si se requieren).	Oficial de Seguridad
5. Aplicar acciones de contención	El Especialista de Seguridad Informática si aplica, debe identificar las acciones de respuesta inmediata (*Contención*) con el equipo especialista del sistema de información para tratar el incidente, esto puede dar como resultado controles de Emergencia y/o controles permanentes adicionales. • El plan de acción puede contener acciones como: ➢ Activar Contingencias ➢ Desconectar ➢ Copiar/Clonar ➢ Registrar posible evidencias	Especialista de Seguridad Informática

PROCEDIMIENTO DE GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN
DOCUMENTO INSTITUCIONAL

MACROPROCESO: PLANEACIÓN ESTRATÉGICA
PROCESO: Sistemas de Información
DEPENDENCIA / PROGRAMA: Vicepresidencia
Versión: 1

Actividad	Descripción	Responsable
	➢ Establecer posibles causas ➢ Notificar a los interesados Si la acción de Contención requiere un cambio de Emergencia, se debe activar el proceso de Gestión de Cambios de Emergencia. El Especialista de Seguridad Informática gestiona la ejecución de las actividades del plan de acción enfocadas en la recuperación de la operación. Dentro de estas actividades pueden estar: ➢ Ejecución de las acciones de restauración ➢ Implantación de medidas de remediación ➢ Pruebas ➢ Ejecución de plan de retorno Cualquiera que sea el resultado de las acciones realizadas, se debe hacer seguimiento a las acciones por parte del Oficial de Seguridad de la información verificando la documentación y evidencias registradas. Una vez finalizada las acciones de contención, el oficial de Seguridad determina si el incidente de Seguridad de la Información está bajo control.	
6. Aplicar acciones Complementarias	El Especialista de Seguridad Informática con el equipo especialista del sistema de información debe identificar si se requieren actividades complementarias para tratar los incidentes de seguridad de la información, esto puede incluir la restauración del Sistema(s), Servicio(s) y/o redes de información a su estado normal. Si las acciones complementarias requieren de un cambio normal, se debe activar el proceso de Gestión de Cambios de TI.	Especialista de Seguridad Informática

PROCEDIMIENTO DE GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN
DOCUMENTO INSTITUCIONAL

MACROPROCESO: PLANEACIÓN ESTRATÉGICA
PROCESO: Sistemas de Información
DEPENDENCIA / PROGRAMA: Vicepresidencia
Versión: 1

Actividad	Descripción	Responsable
7. Notificar	El Especialista de Seguridad Informática, almacena copia de las evidencias recopiladas, y documenta el incidente por medio del sistema que corresponda. La información que debe contener como mínimo es: Fecha de solicitud - Persona que lo diligencia - Ubicación - Descripción del incidente (descripción cronológica de los acontecimientos) - Clasificación del incidente de acuerdo al procedimiento (en caso que el evento sí sea incidente) - Posibles Impactos - Partes involucradas (especificar especialmente si hay terceros involucrados) - Acciones realizadas (Medidas de contención y de recuperación)	Especialista de Seguridad Informática
8. Reporte en el Registro Nacional de Base de Datos RNBD	En la Plataforma tecnológica de la Superintendencia de Industria y Comercio reportar el incidente de seguridad dentro los (15) días hábiles siguientes al registro del incidente o evento de seguridad	Coordinador de Protección de Datos
9. Comunicación a los afectados	Una vez identificado el incidente de seguridad y cumplidas con las actividades descritas en el presente procedimiento, la Oficina de Seguridad de la Información comunicara al interesado en un lenguaje claro y sencillo la violación de seguridad, las medidas correctivas adoptadas por la organización y las recomendaciones de seguridad que deberán seguir los interesados.	Coordinador de Protección de Datos
10. Documentar Lecciones Aprendidas	El Oficial de Seguridad con el equipo que atendiendo el incidente es responsable de identificar las lecciones aprendidas con el objeto de evitar la reincidencia de los hechos y la eliminación de las debilidades aprovechadas por la amenaza que causó el incidente de seguridad. Así mismo, el oficial de Seguridad de la Información es responsable de identificar si aplica, controles nuevos o modificaciones a los existentes en la Universidad, esto en Pro	Oficial de Seguridad

Actividad	Descripción	Responsable
	de mejorar el proceso y la Seguridad de la Información de la Universidad Piloto de Colombia.	
11. Cerrar el Incidente	Oficial de Seguridad informa al Centro de Servicios de Tecnología para el cierre del incidente en la herramienta de gestión e informa a las personas interesadas.	Oficial de Seguridad

Tabla 1. Descripción Proceso de Gestión de Incidentes de Seguridad de la Información.

3.1.2 Roles y Responsabilidades

- **Oficial de Seguridad**

El Oficial de Seguridad de la Información es el responsable de planificar, desarrollar, controlar, gestionar y/o coordinar las estrategias de seguridad de la información, con el fin de mantener la confidencialidad, integridad y disponibilidad; y de promover el diseño, establecimiento, implementación, operación, revisión, mantenimiento y mejora continua de la gestión en seguridad de la información.

- **Especialista de Seguridad Informática**

El Especialista de Seguridad Informática es responsable de gestión y administración de la infraestructura de seguridad informática, gestionar la remediación de vulnerabilidades técnicas y monitorear los eventos de seguridad de la plataforma tecnológica, así como coordinar las acciones de respuesta y recuperación al incidente se seguridad de la información.

- **Coordinador de Protección de Datos**

El Coordinador de Protección de Datos es responsable de velar por la implementación efectiva de las políticas y procedimientos del programa de protección de datos personales para dar cumplimiento a las normas sobre protección de datos personales, así como la implementación de buenas prácticas de gestión de datos personales dentro la Universidad.

4 GLOSARIO DE TÉRMINOS

- **Evento:** La ocurrencia detectada en un estado de un sistema de información, servicio o red que indica una posible violación de la política de seguridad de la información, un fallo de las salvaguardas (controles) o una situación desconocida hasta el momento y que puede ser relevante para la seguridad de la información.

- **Incidente:** Un incidente de seguridad de la información se define como un acceso, intento de acceso, uso, divulgación, modificación o destrucción no autorizada de información; un impedimento en la operación normal de las redes, sistemas o recursos informáticos; o una violación a una política de seguridad o de tratamiento de la información personal de la Universidad Piloto de Colombia.

- **Falsa Alarma**: Reporte de evento que no cumple con la característica de afectación de la Confidencialidad, Integridad y Disponibilidad de la Información.

- **Niveles de clasificación de la información**: Nivel asignado (Confidencial, Privada, Interna o Pública) a la información en función de los requisitos legales, valor de la información, criticidad y susceptibilidad a la divulgación o modificación no autorizada.

- **Integridad:** Propiedad de la información relativa a su exactitud y completitud.

- **Confidencialidad:** Propiedad de la información restringe su disposición o revelación a individuos, entidades o procesos no autorizados.

- **Disponibilidad:** Propiedad de la información de estar accesible y utilizable cuando lo requiera un individuo, entidad o procesos autorizados.

5 ANEXOS

Formato Reporte de Incidente