UNIVERSIDAD DISTRITAL
FRANCISCO JOSÉ DE CALDAS

GUIA DE LA GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

SIGUD

Oficina Asesora de Sistemas
Red de Investigaciones de Tecnología Avanzada RITA
Red de Datos UDNET

TABLA DE CONTENIDO

1. OBJETIVO

Presentar las directrices y lineamientos de manejo de los incidentes que afectan la disponibilidad, confidencialidad e integridad de la información en el marco del proceso de Gestión de los Sistemas de Información y Telecomunicaciones (GSIT) del Sistema de Gestión de Calidad (SIGUD) y del Subsistema de Gestión de la Seguridad de la Información (SGSI) de la Universidad Distrital Francisco José de Caldas.

2. ALCANCE

Esta guía se centra en los elementos de gestión y respuesta apropiada a los incidentes que, de cualquier origen atentan contra los factores clave de la seguridad de la información, describiendo los conceptos relacionados, responsabilidades y las políticas de operación para las diversas condiciones y fases de gestión del procedimiento relacionado.

3. RESPONSABLES

3.1 Informante

Es la persona que siendo parte de un área TIC o perteneciente a la comunidad universitaria bajo cualquier forma de vinculación, identifica y reporta información de un incidente de seguridad por ser afectado directamente o por conocerlo al encontrarse ante indicios suficientes que hacen necesaria su consideración y tratamiento como tal.

3.2 Encargado del soporte básico

Funcionario o contratista prestador de soporte básico en un área TIC, responsable de recolectar y registrar toda la información disponible y de efectuar la evaluación inicial de un caso para confirmar que se está ante un incidente de seguridad de la información dado a conocer por un Informante. El responsable del soporte básico recibe y registra la información del caso, determina sobre las primeras acciones de manejo, incluyendo escalar al responsable o líder de seguridad asignado a su área TIC. Durante la gestión del caso, y hasta el cierre informa a los usuarios e interesados respondiendo las consultas e informando de acuerdo con el desarrollo, las políticas de operación y la gestión realizada sobre el caso.

3.3 Jefe del área TIC

Responsable de la ejecución exitosa del plan de respuesta a incidentes en su área. Aprueba las acciones de control, define los recursos inmediatos a utilizar, presenta a la alta directiva un entendimiento claro sobre el impacto del negocio y procesos afectados y gestiona los recursos adicionales para la gestión del incidente.

3.4 Responsable de la seguridad de la información

Persona encargada perteneciente o no al área TIC, asignada como responsable de la gestión de seguridad de la información, miembro del equipo de respuesta a incidentes, quién lidera la gestión de un incidente de acuerdo con las políticas de operación, las técnicas, conocimientos y las buenas prácticas aplicables. Responsable de determinar y ejecutar las primeras acciones de control, de establecer la gravedad del incidente y de escalar a otros niveles la gestión según corresponda.

3.5 Encargado de la gestión de procesos

Responsable de la verificación del registro de información de calidad, obtención de los indicadores e informes del área gestora de servicios de TIC según se describe en los diversos procedimientos y guías del proceso GSIT.

4. BASE LEGAL

- **Decreto 943/2014. Presidencia de la República de Colombia,** "Por el cual se actualiza el Modelo Estándar de Control Interno MECI 1000: 2014".
- **Acuerdo 01/2013. Universidad Distrital Francisco José de Caldas** "Por el cual se adopta el Plan Maestro de Informática y Telecomunicaciones de la Universidad Distrital Francisco José de Caldas".
- **Norma Técnica Colombiana NTC - ISO 27001/2013. Organización Internacional para la Estandarización,** "Cambios en la Norma para gestionar la Seguridad de la Información".
- **Norma Técnica Colombiana NTC -ISO/IEC 20000-1/2011. Organización Internacional para la Estandarización, "** Gestión de Servicios de Tecnologías de la Información"
- **Resolución 678/2011, Universidad Distrital Francisco José de Caldas, "**Por la cual se adopta la Política para la Seguridad de la Información de la Universidad Distrital y se otorgan funciones en relación con ésta al Comité de Informática y Telecomunicaciones".
- **Resolución 632/2015, Universidad Distrital Francisco José de Caldas,** "Por la cual se crea el Subsistema de Gestión de Seguridad de la Información SGSI de la Universidad Distrital Francisco José de Caldas".

5. MARCOS DE REFERENCIA

ITIL v.3: Marco de referencia que describe un conjunto de mejores prácticas y recomendaciones para la administración de servicios de TI, con un enfoque de administración de procesos.
COBIT 5: Permite que las tecnologías de la información y relacionadas se gobiernen y administren de una manera holística a nivel de toda la Organización

6. POLÍTICAS DE OPERACIÓN

6.1 Objetivos de la Gestión de incidentes de seguridad de la información

La Gestión de incidentes de seguridad de la información comprende la identificación, valoración, el escalamiento y la aplicación de las acciones de control de un caso de incidente para el logro de los siguientes objetivos:

6.1.1. Prevenir incidentes y/o detectarlos y diagnosticarlos rápidamente.

6.1.2 Identificar las causas u origen del incidente y las vulnerabilidades que dieron paso a su ocurrencia.

6.1.3 Valorar el impacto y aplicar las primeras medidas de control que lo controlen o impidan su agravamiento.

6.1.4 Aplicar las acciones de control que permitan minimizar su impacto y eliminar su efecto en el menor tiempo posible, incluidas el escalamiento y obtención de apoyo a otros niveles de la Universidad o externos a ella.

6.1.5 Cerrar los casos de incidentes presentados con informe de su origen, impacto y solución, y las recomendaciones de prevención de casos similares.

6.2 Actividades preventivas en seguridad de la información

6.2.1 Es prioridad de las áreas TIC el fortalecer la capacidad de prevención y de respuesta a incidentes de seguridad de la información como factor de calidad de los servicios de TI ofrecidos.

6.2.2 Todo proyecto de servicios TIC debe prever en su gestión de riesgos las previsiones y controles relacionados con la seguridad de la información, e igualmente debe integrarse a los planes de respuesta a incidentes de su área TIC.

6.2.3 La Política de Seguridad de la Información vigente debe ser consultada y verificada su estricta aplicación en el área TIC.

6.3 Equipo de respuesta a incidentes

Las áreas TIC deben conformar un equipo de respuesta a incidentes o integrarse a uno existente en la Universidad.

6.4 Respuesta a incidentes

Cada área debe contar con un plan de respuesta a incidentes de seguridad de la información.

6.5 Otras

7. DEFINICIONES

Incidente: Un Incidente de Seguridad de la Información es la violación o amenaza inminente a la Política de Seguridad de la Información implícita o explícita. También se puede expresar como la materialización de uno o varios eventos no deseados o inesperados que comprometen o impactan la disponibilidad, integridad y confidencialidad de la información en los recursos informáticos.

8. PROCEDIMIENTOS RELACIONADOS

8.2 Gestión de cambios de TIC

La Gestión de Cambios provee la planeación apropiada teniendo en cuenta el riesgo, impacto y los niveles de autorización de los cambios que afectan a los servicios de TIC, e implica actividades de coordinación, seguimiento, comunicación y documentación en su implementación. Los cambios en los servicios y las incidencias que se generan durante la gestión de cambios deben ser de conocimiento de las áreas y responsables del soporte y de todos los interesados.

8.3 Gestión de Incidentes de TIC

Tiene por objetivo Implementar el registro, seguimiento y control centralizado de incidentes de TIC en el área funcional designada mediante la especificación de los pasos, instrumentos y controles necesarios en la gestión de los incidentes, de forma que se restaure la operación normal de los sistemas o servicios, minimizando el impacto sobre los procesos afectados, incluidos los procesos críticos que invocan el Plan de Continuidad.

9. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

Es la capacidad prevenir, anticipar, detectar, evaluar, controlar, reportar y documentar mediante estrategias, planes, herramientas y mecanismos los incidentes de seguridad de la información.

9.1 Causas

La determinación de la causa u origen de un incidente es fundamental para la aplicación de una respuesta eficaz que minimice su impacto. Entre las múltiples causas pueden encontrarse:

* Accidentes
* Errores
* Actos intencionalmente maliciosos
* Robo
* Extorsión
* Fraude
* Espionaje
* Causas naturales

9.2 Prevención de los incidentes

Algunas acciones preventivas a aplicar son:

- La formación de una cultura de prevención de incidentes.
- Administración de parches.
- Aseguramiento de servidores.
- Implementación de seguridad en redes.
- Prevención contra código malicioso.
- Entrenamiento en respuesta a incidentes.

9.3 Clasificación de incidentes

- **Acceso no autorizado**: Se clasifican los incidentes en donde un agente (interno, externo o sistema), gana acceso lógico o físico a un recurso de información y tecnología (equipo, servidor, dato, software, red, edificación, etc.) sobre el cual no tiene derechos.
- **Denegación de servicio:** Se clasifica en esta categoría incidentes en los cuales un atacante (interno o externo) impide el uso autorizado de servicios de información y tecnología, redes o sistemas de información mediante el consumo excesivo de recursos de la plataforma o sistema bajo ataque.
- **Código malicioso:** En esta categoría están los incidentes en dónde software como virus, troyanos, rat, gusanos y demás formas de malware infecta exitosamente un recurso de información y tecnología.
- **Uso inapropiado:** Se presenta cuando un agente incumple la política de seguridad de la información.

9.4 Respuesta a incidentes de seguridad de la información

Comprende desde la preparación adecuada para el manejo de los riesgos a los que se pueden ver expuestos los recursos de infraestructura, comunicaciones y soporte de la información, pasa por la detección temprana y diagnóstico de incidentes en curso, hasta la restauración o normalización de los factores disponibilidad, confidencialidad e integridad de la información. A mayor eficacia en la prevención y preparación en la respuesta a incidentes, menor el impacto negativo y la menor vulneración de los factores clave de la seguridad de la información.

9.4.1 Instrumentos claves

En la preparación se debe contar con al menos los siguientes instrumentos:

1. Política de gestión de incidentes de seguridad y compromiso de la dirección.
2. Establecimiento de un esquema de gestión de incidentes de seguridad tanto para el área como integrado con todas las áreas TIC de la Universidad.
3. Aseguramiento de redes, sistemas, análisis y gestión de riesgos, actualización de políticas.
4. Toma de conciencia, entrenamiento, aplicación de buenas prácticas, equipos de respuesta a incidentes
5. Selección y uso de herramientas para la detección y control de incidentes, la restauración de las características de seguridad de la información vulneradas, así como la recuperación o restauración de los activos de información.

9.4.2 Análisis del incidente

La detección y análisis de los incidentes se simplifica cuando el origen se identifica con precisión, sin embargo no siempre se puede identificar con precisión la fuente.

Si está en curso un incidente se debe determinar:

- Alcance del incidente (redes, sistemas o aplicaciones afectadas).
- Quién o cuál es la fuente del incidente.
- Como está ocurriendo el incidente (herramientas que se están usando para realizar el ataque, vulnerabilidad que están explotando).
- Perfiles de redes y sistemas: se debe mantener perfiles o registros actualizados del comportamiento de los diferentes dispositivos y sistemas.
- Comprensión del comportamiento normal: Se debe estudiar periódicamente las redes, sistemas y aplicaciones para obtener un conocimiento detallado de lo que se considera un comportamiento normal
- Mantener los relojes de los sistemas sincronizados con una fuente única: Esto con el fin que el proceso de correlación de eventos sea efectivo.
- Documentación: Es necesario documentar únicamente los hechos relacionados con el incidente, se deben evitar registros personales o subjetivos.

- Priorización de incidentes: Todos los incidentes deben ser priorizados para garantizar que son atendidos de acuerdo con su nivel de criticidad.
- Notificación del incidente: Una vez que el incidente ha sido analizado y priorizado se debe proceder a notificar a las áreas e individuos apropiados.

9.4.3 Contención, Recuperación, Erradicación

Es necesario contener la acción del incidente para evitar que su propagación impida su erradicación y afecte a otros sistemas de información e impacte de manera considerable la institución.
Cada incidente tiene su forma particular de contención que debe ser estudiada, definida y adoptada por el equipo de respuesta a incidentes.

9.4.4 Recolección y Manejo de Evidencias

9.4.4.1 Manejo de evidencias

Aunque la principal razón para el manejo de incidentes es la gestión de incidentes también es necesaria para procesos legales (La Ley 1273 de 2009 tipifica los delitos informáticos la protección de la información y de los datos). De esta manera, se deben seguir los procedimientos formales y legales de recolección y manejo de evidencias forenses.

Las actividades de recolección de evidencias deben ser realizadas por personal debidamente entrenado y que se emplee el mínimo de acciones para evitar modificar la evidencia y que ésta pierda valor probatorio frente a un proceso judicial. Es necesario tener en cuenta que cualquier acción que se ejecute sobre el equipo puede afectar considerablemente las evidencias. De igual forma, un atacante puede estar aún dentro del equipo y la recolección de la evidencia en esas circunstancias puede tener consecuencias técnicas irreparables para el equipo y la información.

9.4.4.2 Recolección de evidencias

* Aislar la escena.
* Fotografiar la escena (incluidas las pantallas de los equipos afectados).
* No encender los equipos si están apagados.
* No apagarlos si están encendidos.
* Recolectar información volátil.
* Si es factible recolectar el mayor número de archivos sin apagar el equipo.
* Quitar la potencia del equipo.
* Documentar todas las conexiones de red, cables y periféricos que tenga conectado el equipo.
* Desconectar los dispositivos.
* Generar una imagen forense del disco.
* Recolectar los medios de almacenamiento externo.
* Embalar en fundas protectoras.
* Documentar todo el proceso.

* Remitir al laboratorio forense

9.4.3 Erradicación y Recuperación

Luego que el incidente ha sido contenido es necesario realizar actividades de erradicación para eliminar los componentes que fueron empleados para el desarrollo del mismo. En algunos ataques la erradicación no es necesaria o se realiza durante las actividades de recuperación, allí los administradores restauran los sistemas a su operación normal.

9.4.4 Seguimiento Post Incidente

De cada incidente de seguridad se debe realizar un aprendizaje que permita identificar las amenazas, vulnerabilidades y oportunidades de mejora. De esta manera se debe saber lo siguiente:

* Exactamente ¿qué sucedió?
* ¿Fue bueno el desempeño del grupo de atención de incidentes y del grupo directivo?
* ¿Se siguieron los procedimientos documentados?
* ¿Fueron adecuados los procedimientos?
* ¿Se ejecutaron pasos o acciones que pudieron impedir la recuperación?
* ¿Qué acciones se deben ejecutar en forma diferente durante la atención de un futuro incidente?
* ¿Qué herramientas adicionales o recursos son necesarias para detectar, analizar y mitigar futuros accidentes?

9.5 Equipo de respuesta de incidentes en un área TIC

En la respuesta a un incidente de seguridad de la información participan todos los miembros del área TIC de acuerdo con la dimensión o impacto del mismo. A continuación se describe sucintamente esta participación, lo que aplica según esté conformada el área y los servicios TIC que implemente.

9.5.1 Centro de servicios o personal de soporte

* Recepción de los reportes de incidentes

9.5.2 Jefe

* Asume la responsabilidad en la ejecución exitosa del plan de respuesta a incidentes
* Presenta a la alta directiva un entendimiento claro sobre el impacto del negocio y procesos afectados

9.5.3 Equipo o personal de seguridad de la información

* Gestiona de manera efectiva los riesgos e incidentes.
* Toma medidas proactivas y reactivas para controlar el nivel de riesgo de información.
* Elaboración y ejecución de medidas de contención y mitigación.

* Supervisa las tareas de respuesta a incidentes.
* Realiza las tareas de investigación sobre el incidente.
* Ayuda a determinar el origen de la causa del incidente.
* Redacta informe sobre los hallazgos de la investigación.
* Documenta y cataloga los incidentes
* Coordina y ayuda en la elaboración de un plan de respuesta a incidentes.

9.5.4 Infraestructura

* Aísla o apaga servicios.
* Restaura servicios.
* Ayuda a determinar el origen del incidente.
* Elaboración y ejecución de medidas de contención y mitigación.
* Ayuda a identificar los sistemas expuestos.
* Actualización de parches para mitigar vulnerabilidades.
* Supervisa comportamientos de herramientas (Firewall, Web Applications Firewall, Intrusión Detection System, Intrusión Prevention System, Correlacionado de eventos)
* Ayuda en la elaboración de un plan de respuesta a incidentes.

9.5.5 Auditoria

* Realiza evaluación y plan de auditoría de seguridad de TI como medida proactiva y parte de la gestión de las vulnerabilidades.

9.5.6 Administradores de Bases de Datos

* Determina afectación en sus bases de datos.
* Apaga servicios.
* Restauración de backups
* Ayuda a determinar el origen del incidente.
* Elaboración y ejecución de medidas de contención y mitigación.
* Ayuda en la elaboración de un plan de respuesta a incidentes.

9.5.7 Líderes de proyecto

* Determina tipo de información afectada.
* Trabaja proporcionando información para el análisis de impacto al negocio y procesos afectados.

9.5.8 Equipos de desarrollo

* Realiza desarrollo de nuevas funcionalidades de ser el caso para mitigar el riesgo
* Realiza ajustes en código.

Elaboró	**Revisó**	**Aprobó**
Nombre: Equipo SIGUD **Cargo:** N/A **Fecha:** 15/08/2017	**Nombres:** Roberto Ferro Escobar, Martha Cecilia Valdés Cruz, Beatriz Elisa Jaramillo Moreno **Cargos:** Director RITA, Jefe Oficina Red de Datos, Jefe Oficina Asesora de Sistemas **Fecha:** 15/09/2017	**Nombre:** Carlos Javier Mosquera Suárez **Cargo:** Rector **Fecha:** 15/09/2017