Pontificia Universidad Católica del Ecuador

Seréis mis testigos

Lineamientos para la gestión de incidentes de seguridad de la información

marzo | 2025

Versión 02.01

CONTENIDO

1. INTRODUCCIÓN

La notificación oportuna de los incidentes de seguridad de la información, permite responder a estos en forma sistemática, minimizar su ocurrencia, facilitar una recuperación rápida y eficiente de las actividades, de este modo se minimiza la pérdida de la confidencialidad, integridad y disponibilidad de la información, la interrupción de los servicios, el deterioro de la imagen institucional a su vez que permite la identificación de las brechas de seguridad y a través de esto brinda la oportunidad de fortalecer los controles.

2. MARCO LEGAL

Con base lo definido en la Política General de Seguridad de la Información en el numeral 5.26 Respuesta a incidentes de seguridad de la información.

3. OBJETIVOS

General:

- Definir la forma adecuada de gestionar los incidentes de seguridad de la información en la institución.

Específicos:

- Establecer los responsables y las funciones de estos para dar atención a los incidentes de seguridad de la información.
- Definir las fases, instrumentos y acciones a considerar para atender y dar seguimiento a los incidentes de seguridad de la información.

4. ALCANCE

La presente normativa es de aplicación nacional para dar atención a los incidentes de seguridad de la información.

5. RESPONSABLES

Comité nacional de seguridad de la información

- Conocer las lecciones aprendidas a nivel nacional.
- Priorizar el establecimiento o mejora de controles con base en las lecciones aprendidas.
- Definir proyectos de índole nacional con base en las lecciones aprendidas.
- Participar de ser requerido, en dar atención a los incidentes de seguridad de la información, que hayan sobrepasado el impacto local.

- Ejecutar las actividades post incidentes, sobre aquellos incidentes de SI en los cuales se hay requerido su participación para dar atención a los mismos.

Comité local de seguridad de la información

Los responsables de dar atención a los incidentes de seguridad de la información son los miembros del Comité Local de Seguridad de la Información (CSI), sin embargo, su participación corresponderá al ámbito de afectación del incidente de seguridad y la severidad de este, para lo cual, se define:

- Si la afectación del incidente de seguridad es sobre la información digital asociada a servidores, servicios, bases de datos, aplicaciones, equipos de seguridad perimetral y equipos tecnológicos institucionales de usuario final, el responsable local de Seguridad de la Información convocará al responsable local de tecnología.
- Si la afectación del incidente de seguridad de la información es sobre activos de información físicos, el responsable local de Seguridad de la Información convocará al responsable local de la gestión administrativa.
- Si la afectación del incidente de seguridad de la información causa daño sobre la imagen institucional o su reputación, el responsable local de Seguridad de la Información convocará al responsable local de comunicación.
- Si en la ocurrencia del incidente de seguridad de la información se identifica la participación de estudiantes, colaboradores, profesores, el responsable local de Seguridad de la Información convocará a los responsables locales de la gestión académica, de estudiantes, de talento humano y asesoría jurídica según corresponda para la definición y aplicación de las sanciones o análisis de implicaciones legales.

Adicionalmente, de ser necesario la participación de cualquiera de los miembros locales del CSI para la evaluación, esclarecimiento, abordaje en la atención del incidente de seguridad de la información, este deberá participar de forma obligatoria.

- Conocer las lecciones aprendidas a nivel local.
- Priorizar el establecimiento o mejora de controles con base en las lecciones aprendidas.
- Recomendar la ejecución de proyectos con base en las lecciones aprendidas.
- Ejecutar las actividades post incidentes, sobre aquellos incidentes de SI en los cuales se hay requerido su participación para dar atención a los mismos.

Responsable nacional de Seguridad de la Información (SI)

- Definir la metodología para gestionar incidentes de seguridad de la información.
- Analizar y proponer mejoras a los controles con base en las lecciones aprendidas.
- Definir los insumos para tener una mejor preparación para enfrentar incidentes.
- Socializar a nivel nacional las lecciones aprendidas.

- Socializar al Comité Nacional de Seguridad de la Información las lecciones aprendidas.
- Informar al responsable nacional de Aseguramiento de la Calidad.

Responsable local de Seguridad de la Información (SI)

- Receptar y registrar los incidentes de SI.
- Coordinar la participación de los miembros del Comité Local de SI según corresponda para la gestión del incidente de seguridad de la información.
- Participar en la atención de los incidentes de seguridad.
- Realizar el seguimiento hasta el cierre del incidente de SI.
- Coordinar la ejecución de las actividades post incidentes de seguridad.
- Proponer ajustes a los controles de seguridad y normativa según corresponda.
- Reportar a la máxima autoridad de la sede los incidentes de severidad alta.
- Reportar al responsable nacional de SI la bitácora de incidentes con las lecciones aprendidas.

Responsable local de Tecnología

- Receptar y registrar los incidentes de SI.
- Establecer, implementar y monitorear los controles de seguridad de los servidores, servicios, bases de datos, aplicaciones, equipos de seguridad perimetral, y cualquier equipo institucional de carácter tecnológico o relacionado.
- Identificar, analizar, contener, erradicar, documentar y notificar la solución de un incidente de seguridad de la información.
- Conservar la evidencia de los incidentes de seguridad de la información.
- Colaborar en la ejecución de las actividades post – incidentes.
- Definir, elaborar y ejecutar los protocolos para la atención de los incidentes de seguridad de la información en el ámbito tecnológico.

Responsable local de la Gestión Administrativa

- Establecer, implementar y monitorear los controles de seguridad física en la institución
- Apoyar en la identificación, análisis, atención de los incidentes de seguridad de la información relacionados con los controles físicos instalados.
- Conservar la evidencia de los incidentes de seguridad de la información.
- Colaborar con la ejecución de las actividades post – incidentes.
- Definir, elaborar y ejecutar los protocolos para la atención de los incidentes de seguridad de la información en el ámbito tecnológico.

Responsable local de Comunicación

- Definir, elaborar y ejecutar los protocolos para la atención de los incidentes de seguridad de la información en el ámbito de su competencia.
- Colaborar con las iniciativas requeridas con el propósito de reforzar el conocimiento y responsabilidad respecto de la seguridad de la información de los colaboradores.

6. DESARROLLO DEL CONTENIDO

Para gestionar los incidentes de seguridad de la información, se tiene las siguientes fases:

PLANIFICACIÓN

En esta fase se trata de prevenir, detectar, evaluar y gestionar las vulnerabilidades oportunamente.

Para ello, el **área responsable local de tecnología** debe contar con herramientas que permitan:

- Configurar alertas de seguridad respecto del funcionamiento de los servidores, servicios, bases de datos, aplicaciones y equipos de seguridad perimetral.
- Sincronizar los relojes (servidores, equipos de usuarios finales, equipos de comunicación).

Además:

- Listado de activos de información de: desarrollo, infraestructura tecnológica, equipos de conectividad, dispositivos institucionales de usuario final. (ver formulario 1).
- Catálogo de servicios (ver formulario 2).
- Diagrama de redes.

- Identificación del tráfico normal de la red.
- Políticas configuradas en los equipos de seguridad perimetral.
- Políticas configuradas para la prevención de código malicioso.
- Listado de contactos de proveedores de tecnología. (ver formulario 3).
- Respaldos de información de usuarios, bases de datos y de imágenes de servidores.
- Plan de continuidad de TI.
- Planes de contingencia.
- Plan de gestión de cambios.
- Protocolos.
- Bitácora de incidentes de seguridad de la información. (ver formulario 4).

En lo que respecta a la información física, el **área local responsable de la gestión administrativa** tiene que disponer y actualizar los siguientes insumos:

- Listado de bienes.
- Listado de ubicación de controles físicos instalados.
- Listado de áreas seguras.
- Informe de planes de mantenimiento realizados.
- Listado de contactos de proveedores.
- Listado de propietarios de los activos de información.

IDENTIFICACIÓN

En esta fase el **área local responsable de tecnología** tiene que disponer de:

- Reportes de usuarios (finales, administradores, de servicios) respecto de los accesos y acciones realizadas en los servidores, servicios, bases de datos, aplicaciones y equipos de seguridad perimetral.
- Reporte de alertas y notificaciones de incidentes.
- Reporte de la aplicación de parches de seguridad. (ver formulario 5).
- Reporte del tráfico de red.
- Reporte de eliminación segura de equipos, información crítica.
- Reportes de monitoreo de comportamiento, funcionamiento y rendimiento de servidores, servicios, bases de datos, aplicaciones y seguridad perimetral.
- Informes de mantenimiento de servidores, bases de datos, aplicaciones y equipos de seguridad perimetral.
- Logs de servidores, bases de datos, aplicaciones y equipos de seguridad perimetral.
- Bitácoras de respaldo de información de usuarios, bases de datos y de las imágenes de servidores.

Los mencionados insumos permitirán la identificación de incidentes de seguridad de la información.

En lo que respecta a la información física, **el área local responsable de la gestión administrativa** tiene que disponer y actualizar los siguientes insumos:

- Bitácoras de acceso de usuarios a las instalaciones de la institución, en especial de las áreas seguras. (ver formulario 6).
- Bitácoras de las grabaciones de las cámaras de seguridad.
- Respaldo de las grabaciones de las cámaras de seguridad.
- Reportes de monitoreo del funcionamiento de los controles de seguridad física instalados.
- Reportes de monitoreo de los controles de seguridad física instalados respecto de los accesos a las instalaciones de la institución.
- Informes de mantenimientos realizados a los controles de seguridad física instalados.
- Reporte de alertas y notificaciones del funcionamiento de los controles de seguridad física instalados
- Reporte de eliminación segura de información crítica.

ANÁLISIS

Al presentarse un incidente de seguridad de la información se debe:

a) Analizar la amenaza materializada (ver Formulario 4).
b) Categorizar la severidad del incidente, para lo cual se debe evaluar los siguientes parámetros:
   i. **Afectación a que categoría de activo de información:** esto se refiere, a que se debe evaluar si el incidente afectó a activos relacionados con la operación de los procesos clave de la institución, a los cuales se les valorará con un puntaje mayor (ver anexo 1).
   ii. **Afectación a qué tipo de información:** en este punto se debe considerar a que tipo de información afectó la ocurrencia del incidente de seguridad de la información, a la información confidencial y restringida se le valorará con un puntaje mayor (ver anexo 2).
   iii. **Rango de usuarios afectados (expresado en porcentaje):** en este parámetro cada sede deberá considerar el tamaño de la población y con base en esta analizar en qué rango con base en el número de usuarios afectados (ver anexo 3).
   iv. **Rango de afectación económica (expresado en porcentaje):** a través del parámetro se ubica con base en el costo del activo de información afectado cual sería el impacto económico a la institución. (ver anexo 4).
   v. **Incumplimiento legal:** en este punto se debe evaluar si la información afectada impide poder cumplir o presentar información de cumplimiento legal (ver anexo 5).
   vi. **Afectación a la reputación institucional:** a través de este parámetro se evalúa si el incidente afectó a la reputación de la imagen institucional (ver anexo 6).
c) Con la evaluación de estos parámetros, se definir el nivel de severidad del incidente de seguridad de la información (ver anexo 7).
d) Para la atención de incidentes de seguridad se establece tiempos máximos en que el incidente debe ser atendido de acuerdo con su severidad (no es el tiempo en el cual el incidente debe ser solucionado, debido a que el tiempo para solución de los incidentes puede variar dependiendo del caso). (ver anexo 8).

e) Definir la estrategia de contención, erradicación y recuperación según corresponda.

CONTENCIÓN, ERRADICACIÓN Y RECUPERACIÓN

Una vez que se ha materializado la amenaza se debe adoptar la estrategia que permita evitar la propagación del incidente, disminuir los daños en los activos de información respecto de la pérdida de la confidencialidad, integridad y disponibilidad de la información. Con base en lo mencionado se tiene:

- **Contención**: busca la detección del incidente con el fin de que no se propague y pueda generar más daños a la información o a los servicios y sistemas informáticos, la estrategia de contención depende del tipo de incidente, para facilitar esta tarea la universidad debe poseer una estrategia de contención previamente definida para poder tomar decisiones, por ejemplo: apagar sistema, desconectar red, deshabilitar servicios.

- **Erradicación y Recuperación:** una vez ejecutada la contención del incidente se realiza la recuperación a través de la restauración de los sistemas y/o servicios afectados; así como fortalecer los sistemas para prevenir incidentes similares.

Dependiendo de la afectación, en esta fase a veces es necesario activar el BCP (Plan de Continuidad del Negocio) o el DRP (Plan de Recuperación de Desastres).

POST-INCIDENTE

El accionar en la fase post-incidente, se refiere a las acciones y medidas que se toman después de contener, erradicar y recuperarse como parte de atención del incidente de seguridad de la información.

Los miembros del CSI, deben ejecutar las siguientes actividades con base en su ámbito de competencia.

- Bitácora del incidente de seguridad de la información (registro del incidente y lecciones aprendidas). (ver formulario 4)
- Comunicación con las partes afectadas a través de correos electrónicos o llamadas telefónicas.
- Elaboración informe de cierre de los incidentes críticos, en el cual deben constar las recomendaciones a ejecutarse por las distintas áreas articuladoras, entre las cuales, dependiendo del ámbito de aplicación, se podría tener:
    a. Implementación o mejora de los controles tecnológicos.
    b. Implementación o mejora de los controles físicos.
    c. Implementación o mejora de los controles organizacionales
    d. Definición o actualización de normativa y procesos.
    e. Definición y aplicación de sanciones disciplinarias y penales de ser el caso.

7. SEGUIMIENTO DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

Dependiendo de la severidad del incidente se empleará las acciones a implementarse con base en lo definido en las lecciones aprendidas (bitácora de incidentes) y en el informe de cierre del incidente.

Para lo cual, el presidente del Comité de Seguridad de la Información enviará con base en las recomendaciones definidas ya sea en las lecciones aprendidas o en el informe de cierre del incidente a las áreas que correspondan la comunicación solicitando la aplicación de las recomendaciones.

Posterior, se verificará si la solución implementada cubre el daño causado y se evaluará el estado de los incidentes reportados.

En los casos en los que los incidentes de seguridad de la información hayan sido catalogados como ALTOS y no se hayan resuelto dentro de las 24 horas de producido el mismo, se informará directamente a los niveles superiores de la universidad.

8. GLOSARIO

Incidente de seguridad de la información: es todo acceso o intento de acceso, uso, divulgación, modificación o destrucción no autorizada a un activo de información; que ocasiona daño a los activos de información de la institución.
Información Lógica: Datos organizados de manera coherente para facilitar su uso y comprensión.
Evento de seguridad de la información: es cualquier incidente o actividad que afecta la confidencialidad, integridad o disponibilidad de los datos y sistemas de una organización. Estos eventos pueden incluir accesos no autorizados, ataques cibernéticos, pérdida de datos, o fallos en los sistemas de seguridad.
Incidente de seguridad de la información: es un evento que compromete la confidencialidad, integridad o disponibilidad de los datos y sistemas de una organización. Esto puede incluir accesos no autorizados, violaciones de datos, ataques de malware, o cualquier otra actividad que ponga en riesgo la seguridad de la información.

9. ANEXOS

Anexo 1: escala de valoración con base en la categoría de activo de información

Categoría Activo de información	Valoración	Ejemplos
Almacenamiento	3	one drive, sharepoint, etc
Base de datos sistema misional	4	banner, sap, success factor, moodle
Base de datos sistemas de soporte	2	trámite, puce sostenible, etc
Grabaciones	2	en cintas, etc
Hardware (Usuario final)	1	pc de usuario final, etc
Información Digital	2	sylabus, contratos, hojas de vida, etc

Información Física	2	sylabus, contratos, hojas de vida, etc
Infraestructura Física	2	aulas, salas, oficinas, edificios, etc
Infraestructura Tecnológica	4	data center, dispositivos de comunicación, de redes, servidores, etc
Servicios	3	outlook, internet, intranet, etc
Software (de tecnología)	3	sistemas de monitoreo de bd, dispositivos de comunicación, de redes, etc
Software (Usuario final)	1	office, pdf, winzip, winrar, etc
Software (de sistemas misionales)	4	banner, sap, success factor, moodle
Software (de sistemas soporte)	2	trámite, puce sostenible, etc

Anexo 2: escala de valoración de acuerdo al nivel de confidencialidad de la información

Nivel de confidencialidad	Valoración
Pública	1
Uso Interno	2
Restringido	3
Confidencial	4

Anexo 3: escala de valoración por rangos de usuarios afectados y

Rango de usuarios afectados (expresado en %)	Valoración
<= 10%	1
11% - 30%	2
31% - 50%	3
>= 51%	4

Anexo 4: rango de afectación económica

Rango de afectación económica (expresado en porcentaje)	Valoración
<= 10%	1
11% - 30%	2
31% - 50%	3
>= 51%	4

Anexo 5: escala de valoración con base en el incumplimiento legal

Incumplimiento legal	Valoración
si	4
no	0

Anexo 6: escala de valoración con base en la afectación a la reputación institucional

Afectación a la reputación institucional	Valoración
bajo	1
medio	2
alto	4

Anexo 7: valoración del nivel de severidad del incidente de seguridad de la información

Valor	Severidad	Descripción
>= 25	alto	cuando el incidente afecta a activos de información que influyen directamente en la consecución de los objetivos misionales de la institución, afecten la reputación y el buen nombre o involucran aspectos legales
13 a 19	medio	el incidente afecta a activos de información considerados de impacto moderado que influyen directamente a los objetivos de un proceso determinado.
<= 12	bajo	el incidente de seguridad afecta a activos de información considerados de impacto menor e insignificante, que no influyen en ningún objetivo. Estos incidentes deben ser monitoreados con el fin de evitar un cambio en el impacto.

Anexo 8: tiempo atención de incidentes de seguridad de la información

Severidad del incidente de SI	Tiempo máximo de atención
Alto	30 minutos
Medio	2 horas
Bajo	5 horas

10.FORMULARIOS

Formulario 1: Activos de información del área encargada del desarrollo de aplicaciones

Sede	Nombre	Detalle	Tipo de Servicio	Tipo aplicación (web o escritorio)	Estado	Tipo de proceso institucional al que el sistema informático apoya	Fabricante	Tipo de Desarrollo	¿ Se trata de un Sistema / Servicio Legado?	¿Open Source o Licenciado?	¿On Premise o Nube?

Relación o afectación a otro aplicativo (el/los sistemas con el mismo nombre de la columna B)	Interfaces	¿ Se encuentra virtualizado por el Área de Operaciones?	Versión y/o Service Pack	Módulos que lo conforman	Lenguaje de programación / Plataforma tecnológica	Tipo de base de datos	Servidor APP	Servidor BBDD	Base de Datos	Area (s) requirente (s)	Unidad (es) funcional (es) o usuaria (s)

Unidad (es) que administra (n) el sistema informático (Cliente Principal)	Usuario principal (quien lo maneja)	Cliente Principal (Estudiantes, Docentes o Administrativos a quien apoya el servicio o sistema)	Tipo de procedencia	Fecha de adquisición o desarrollo (aaaa-mm-dd)	Fecha de puesta en producción (aaaa-mm-dd)	Cantidad de usuarios internos registrados en el sistema informático	Cantidad de usuarios externos del sistema informático	Observaciones DI	A cargo de	URL APP	Link documentación	Usuario Final

Formulario 2: Activos de información del área encargada de la infraestructura tecnológica – servidores

Sede	Ubicación	Nombre	Físico/Virtual	Marca	Modelo	Serie	Sistema Operativo	Función o servicio

Formulario 3: Activos de información del área encargada de la infraestructura tecnológica – equipos de conectividad

Sede	Equipo	Modelo	Serial	Nombre	Edificio	Sector	Ubicación	Código Activo

Formulario 4: Activos de información del centro informático

Sede	Técnico	Usuario	Cédula	Rol del usuario	Unidad	Nombre equipo	Marca CPU	Modelo CPU	Clase procesador	Velocidad procesador	Tamaño memoria RAM	Tipo memoria RAM

Capacidad máxima memoria RAM	Tamaño disco	Tipo de disco duro	Red CPU	Active Directory	Tipo CPU	Número de serie CPU	Control de activos CPU	Marca CPU	Conexión monitor	Tamaño monitor	Tipo monitor	Número de serie moniitor

Control de activos monitor	Marca proyector	Modelo proyector	Lúmenes proyector	Número de serie proyector	Control de activos proyector	Tipo adicionales	Marca adicionales	Modelo adicionales	Conexión adicionales	Número de serie adicionales	Control de activos adicionales

Formulario 5: Activos de información del área de operaciones de tecnología

Sede	Sección custodio	Unidad del custodio	Área	Departamento	Cargo usuario	Usuario	Nombre equipo	Marca CPU	Modelo CPU	Tipo procesador	Generación procesador	Tamaño memoria RAM(GB)	Tipo RAM

Capacidad (GB) del disco	Tipo de disco	Red CPU	Active directory	Tipo de equipo	Número de serie	Control de activos	Marca monitor	Conexión monitor	Tamaño monitor	Número de serie monitor	Control de activos monitor	Marca monitor2	Conexión monitor2

Tamaño monitor2	Número de serie monitor2	Control de activos monitor2	Marca proyector	Modelo proyector	Lúmenes proyector	Horas de uso proyector	Número de serie proyector	Control de activos proyector	Tipo adicionales	Marca adicionales	Modelo adicionales

Conexión adicionales	Capacidad adicionales	Número de serie adicionales	Control de activos adicionales	Sistema operativo	Versión de sistema operativo	Fecha último mantenimiento

Formulario 6: Catálogo de servicios

Sede	Clasificación	Servicio	Categoría	Tipo	Plantilla	SLAs	Grupos Soporte	Escalado	Accesibilidad	Autorización	Calendario	Campo personalizado	Observación	Grupo

Formulario 7: Listado de contactos de proveedores de tecnología

Area	Sistema /Aplicativo /Infraestructura	Empresa	Nombre Contacto PUCE	Teléfono del Contacto PUCE	Correo del Contacto PUCE	Proveedor	Teléfono Proveedor	Correo Proveedor	Descripción	Dirección	Página Web	Fax

Formulario 8: Bitácora de incidentes de seguridad de la información

Código del Incidente	Sede	Fecha de evento / Incidente	Hora de evento / Incidente	Área que reporta el Incidente	Quien reporto el Incidente	Presunción - Incidente	Amenaza Materializada	Vulnerabilidad	Detalles adicionales sobre el Incidente

Afectación a que categoría de activo de información	Afectación a que tipo de información	Rango de usuarios afectados (Expresado en %)	Afectación Económica (Expresado en %)	Incumplimiento legal	Afectación a la reputación Institucional	Afectación a que activo de información	Severidad	Registro / Información recolectada	Ubicación del registro

Evento / Incidente relacionado	Acciones tomadas / Lecciones aprendidas	Medidas preventivas	El incidente implica sanción?	Descripción de la sanción	Estado del incidente	Fecha de solución del incidente	Quien atendió el Incidente

Formulario 9: registro de aplicación de parches a los equipos

Sede	Nombre de equipo	Sistema Operativo	Versión Anterior	Versión Actual	Descripcion de Parches que se Implementaron	Fecha de actualización	Técnico responsable	Asignado a:	Tipo usuario: (Docente / Administrativo)	Ubicación

Formulario 10: Bitácora registro de accesos físicos al data center

Sede	Fecha	Nombres y apellidos	Empresa	Actividad a realizar (detallar)	Hora ingreso	Firma (entrada)	Hora Salida	Firma (Salida)

ACTA DE APROBACIÓN

Aprobación	Firma	Sumilla	Fecha
Mgtr. Mónica Mancheno **Directora de la DAC**			Marzo-2025

Revisión

Mgtr. Karina Molina **Oficial de Seguridad de la información (SI)** **Sede Quito**			Marzo-2025

Elaboración

Mtr. Karina Molina **Responsable de SI - Sede Quito**			Marzo-2025
Mtr. Cristhian Cobo **Responsable de SI - Sede Ambato**			Marzo-2025
Mtr. Cristhian Delgado **Responsable de SI - Sede Esmeraldas**			Marzo-2025
Mtr. Diego Baroja **Responsable de SI - Sede Ibarra**			Marzo-2025
Mtr. Jean Velesaca **Responsable de SI - Sede Manabí**			Marzo-2025
Mtr. Ricardo Morán **Responsable de SI - Sede Santo Domingo**			Marzo-2025