Edición N°: 2

Revisión N°:

Fecha: Noviembre de 2025

Fecha:

Responsable: Jefe de Gestión de la Información

Área: Gestión de la Información

MANUAL PARA LA GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

Manuel Uribe Angel
E.S.E HOSPITAL
Vinculados con la Vida!

Elaboró: Juan Carlos Arango Camacho
Técnico Operativo Gestión de Información

Firma:

Aprobó: Martha Lucía Vélez Arango
Gerente

Firma:

HOJA DE CONTROL DEL DOCUMENTO

EDICIÓN	REVISIÓN	FECHA	ELABORÓ	REVISÓ	APROBÓ	OBSERVACIONES
1		Diciembre de 2018	Oscar Alexander Cano	Diana Marcela Saldarriaga	Martha Lucía Vélez Arango	
2		Noviembre de 2025	Juan Carlos Arango Camacho Técnico Operativo Gestión de Información	Diana Marcela Saldarriaga Jefe Gestión de Información	Martha Lucía Vélez Arango Gerente	Se actualizan los procedimientos para la gestión de incidentes, incluyendo ajustes mejoras en las fases del proceso (Preparación, Detección y Análisis, Contención, Erradicación y Recuperación, y Post-Incidente), así como la actualización de roles, responsabilidades y tiempos de respuesta, la clasificación de eventos e incidentes, la priorización según impacto, y la incorporación de mecanismos de recolección de evidencia y lecciones aprendidas.
			Fecha de elaboración 26-11-2025	Fecha de revisión 26-11-2025	Fecha de aprobación 28-11-2025	

Resolución Número 4521
(27 de diciembre de 2018)

Por medio de la cual se Adapta el Manual para la gestión de incidentes de seguridad de la información.

El Gerente de la ESE Hospital Manuel Uribe Ángel Envigado, en uso de sus atribuciones legales y estatutarias y

CONSIDERANDO

- Que se hace necesario unificar los criterios para la elaboración, actualización y/o adaptación de los Manuales administrativos y asistenciales de la ESE, para una mejor aceptación, implementación y adherencia por parte del personal que presta sus servicios en la institución, y que a la vez permita su actualización conforme a los avances técnico-científico y las directrices del Ministerio de protección social.

- Que se considera importante describir paso a paso las actividades que se desarrollan en cada uno de los servicios, para garantizar la unificación en la ejecución de éstos y así lograr el manejo adecuado de los recursos, minimizando los riesgos en la prestación del servicio.

- Que los Manuales tanto asistenciales como administrativos serán el soporte para el entrenamiento de los funcionarios y para en el manejo del paciente de la ESE.

RESUELVE

Artículo Primero: adáptese y cúmplase con los lineamientos descritos en el Manual para la gestión de incidentes de seguridad de la información.

Dado en Envigado el día veintisiete del mes de Diciembre de 2018

MARTHA LUCÍA VÉLEZ ARANGO
Gerente

CONTENIDO

1. INTRODUCCION

Este Manual de Gestión de Incidentes de Seguridad de la Información establece las directrices, responsabilidades y procedimientos para identificar, reportar, analizar, atender y cerrar los incidentes que afecten la información de la E.S.E. Hospital Manuel Uribe Ángel. Su propósito es garantizar que la institución responda de manera oportuna, ordenada y eficaz ante cualquier situación que comprometa la confidencialidad, integridad o disponibilidad de los datos, especialmente aquellos relacionados con la historia clínica, información personal de pacientes, usuarios y funcionarios.
El manual se construye con base en la Guía 21 del MinTIC, las buenas prácticas nacionales e internacionales (ISO 27035), y la realidad operativa del hospital, ajustándose a las capacidades actuales del área de Gestión de la Información, Infraestructura, Aplicaciones, Jurídica y Protección de Datos Personales.

2. JUSTIFICACIÓN

La E.S.E. Hospital Manuel Uribe Ángel depende de diferentes sistemas de información que soportan actividades misionales críticas, como la atención asistencial y la operación administrativa. Cualquier incidente de seguridad puede afectar directamente la prestación del servicio de salud, causar filtraciones de datos sensibles, generar impactos legales y reputacionales, o interrumpir procesos esenciales.
Por esta razón, se requiere un manual formal, claro y adaptado a la realidad institucional que permita:

- Responder de forma organizada a incidentes de seguridad.
- Reducir el impacto sobre la operación asistencial y administrativa.
- Cumplir con las normas de protección de datos personales y seguridad de la información./
- Establecer roles definidos que faciliten la coordinación interna.
- Servir como guía para la toma de decisiones y la trazabilidad.

3. OBJETIVOS

3.1. Objetivo general

Establecer el modelo, los procedimientos y las responsabilidades necesarias para la gestión integral de incidentes de seguridad de la información en el hospital, garantizando una respuesta oportuna, coordinada y eficaz que minimice los impactos y asegure la continuidad de los servicios asistenciales y administrativos.

3.2. Objetivos Específicos

- Definir un proceso claro y sencillo para reportar, analizar y atender incidentes de seguridad.
- Establecer roles y responsabilidades para cada fase del proceso.
- Regular el uso de las herramientas y canales de comunicación para la atención de incidentes.
- Promover la detección temprana y la adecuada clasificación del incidente.
- Reducir riesgos asociados a la pérdida, alteración o divulgación no autorizada de datos.
- Garantizar que los incidentes se documenten, analicen y se generen acciones de mejora.
- Cumplir con los lineamientos establecidos por MinTIC y las normas de protección de datos.

4. ALCANCE

- Todos los funcionarios, contratistas y personal autorizado que use los sistemas de la E.S.E. Hospital Manuel Uribe Ángel.
- Todos los activos de información: estaciones de trabajo, servidores, portátiles, dispositivos móviles institucionales, equipos biomédicos, sistemas clínicos y administrativos, redes, bases de datos y cualquier recurso tecnológico.
- Todos los tipos de incidentes: pérdida de dispositivos, accesos indebidos, malware, phishing, fallas de sistemas, divulgación no autorizada, anomalías en historia clínica, entre otros.

El proceso inicia desde la **detección o reporte** del incidente y finaliza con su **cierre y registro de lecciones aprendidas**.

5. RESPONSABLES

Profesional Universitario de Gestión de la Información
Es el encargado de:

- Revisión de boletines de seguridad.
- **Recibir y documentar** todos los casos de incidentes.
- **Clasificar y priorizar** incidentes según su gravedad (bajo, medio, alto).
- Coordinar y despliega las capacidades según lo requiera en Infraestructura, Aplicaciones, Jurídica, Protección de Datos y/o jefe de gestión de la información.
- Canalizar incidentes de alto impacto a Jurídica y Protección de Datos.
- Participar en el análisis técnico, decisiones y el cierre documental del incidente.

Infraestructura y Aplicaciones

Actúan como responsables operativos del análisis técnico, contención y remediación según la naturaleza del incidente.

- Infraestructura responsable de incidentes relacionados con:
  - Redes / Firewall / IDS / IPS
  - Antivirus
  - Servidores
  - Equipos extraviados o robados
  - Malware
  - Accesos no autorizados
  - Configuraciones de red
  - Soporte a Servinte en temas técnicos
  -
- Aplicaciones responsables de incidentes relacionados con:
  - Datos asistenciales o administrativos Servinte.
  - Manipulación o acceso indebido a historias clínicas.
  - Caídas, anomalías o comportamientos irregulares de aplicaciones.

Oficial de protección de datos personales

Evalúa incidentes relacionados con datos personales o sensibles, determina medidas y orienta sobre notificación a entes externos.

Jurídica

Participa cuando existen indicios de suplantación, fraude, falsificación de documentos, accesos indebidos con implicaciones legales o disciplinarias según lineamientos institucionales.

Jefe de Gestión de la Información

Este cargo actúa como **coordinador estratégico**:

- Convoca a otros actores.
- Interviene en incidentes complejos.
- Valida reportes, decisiones y cierres.
- Garantiza cumplimiento del manual.
- Activar el plan de contingencia o continuidad si el incidente lo amerita.
- Informar a la Gerencia.

6. MARCO LEGAL

En la elaboración del presente Manual y Plan de Gestión de Incidentes de Seguridad de la Información se incorporan y cumplen los lineamientos definidos por las siguientes normas, guías y disposiciones:

Modelo de Seguridad y Privacidad de la Información – MSPI (MinTIC).

Incluye los lineamientos técnicos para la implementación de controles y procesos de seguridad de la información en entidades públicas, en especial:

- Guía 21: Gestión de Incidentes de Seguridad de la Información, adoptada dentro de la Política de Gobierno Digital.

Normas Internacionales ISO/IEC:

- ISO/IEC 27001:2013 (o 2022, según versión adoptada por la entidad) – Sistema de Gestión de Seguridad de la Información, específicamente el Numeral 16 – Gestión de Incidentes de Seguridad de la Información.
- ISO/IEC 27035 – Gestión de Incidentes de Seguridad de la Información (Buenas prácticas para identificación, reporte, análisis, respuesta y aprendizaje).

Normatividad Nacional sobre Protección de Datos Personales:

- Ley 1581 de 2012 — Régimen de Protección de Datos Personales.
- Decreto 1377 de 2013 — Reglamenta parcialmente la Ley 1581 de 2012.
- Decreto 886 de 2014 — Reglamenta aspectos del Registro Nacional de Bases de Datos.
- Ley 1266 de 2008 — Hábeas Data financiero (aplicable para casos especiales).
- Circular Única de la Superintendencia de Industria y Comercio – Capítulo de Protección de Datos.
- Guía de Responsabilidad Demostrada — Lineamientos para garantizar el cumplimiento del principio de responsabilidad demostrada en el tratamiento de datos personales.

Política de Gobierno Digital (Decreto 1008 de 2018 y normas asociadas).

Marco que exige a las entidades públicas implementar prácticas de seguridad de la información, continuidad y gestión de incidentes.

Normatividad interna de la E.S.E. Hospital Manuel Uribe Ángel:

- Política de seguridad y privacidad de la información y seguridad digital.
- Política de Protección de Datos Personales.
- Lineamientos y procedimientos internos asociados a TI, infraestructura, aplicaciones y gestión documental.

En el desarrollo de las actividades definidas en el presente Manual y Plan de Gestión de Incidentes de Seguridad de la Información, se incorporan los componentes establecidos en el Manual de Seguridad y Privacidad de la

Información (MSPI) del MinTIC, específicamente los lineamientos de la Guía 21 “Gestión de Incidentes”, en el marco de la Política de Gobierno Digital. Estos lineamientos se encuentran alineados con las mejores prácticas internacionales y corresponden a lo establecido en la Norma ISO/IEC 27001:2013, Numeral 16, referente al proceso de gestión de incidentes de seguridad de la información.

Asimismo, el manual integra los principios y obligaciones definidos en la “Guía de Responsabilidad Demostrada” para la protección de datos personales, emitida por la Superintendencia de Industria y Comercio, garantizando que el tratamiento de incidentes que involucren datos personales o datos sensibles cumpla con los estándares legales, técnicos y administrativos vigentes.

7. MARCO CONCEPTUAL

Activo de información: Es cualquier elemento que tenga valor para la organización y, en consecuencia, debe ser protegido.

Amenaza: Factor externo que aprovecha una debilidad en los activos de información y puede impactar en forma negativa en la organización. No existe una única clasificación de las amenazas, lo importante es considerarlas todas a la hora de su identificación.

Autenticidad: Aseguramiento de la identidad respecto al origen cierto de los datos o información que circula por la Red.

Confidencialidad: Garantía que la información sea accedida únicamente por usuarios y procesos autorizados.

Control: Medida que permite garantizar la reducción del nivel de un riesgo específico o mantenerlo dentro de límites aceptables.

Disponibilidad: Garantía que los usuarios y procesos autorizados tengan acceso a los activos de información cuando los requieran.

Evento de Seguridad de la información: Un evento de seguridad de la información es una ocurrencia identificada en el cambio del estado de la información, un sistema, servicio, o red que indica una posible violación de la política de seguridad y privacidad de la información, y seguridad digital o la falla de medidas de seguridad o una situación previamente desconocida que pueda ser relevante para la seguridad.

Keylogger: Es un software o hardware que puede interceptar y guardar las pulsaciones realizadas en el teclado de un equipo que haya sido infectado. Este malware se sitúa entre el teclado y el sistema operativo para interceptar y registrar la información sin que el usuario lo note. Además, un keylogger almacena los datos de forma local en el ordenador infectado y, en caso de

que forme parte de un ataque mayor, permite que el atacante tenga acceso remoto al equipo de la víctima y registre la información en otro equipo. Aunque el término keylogger se usa, normalmente, para nombrar este tipo de herramienta maliciosas, existen también herramientas de vigilancia legítimas que usan las autoridades policiales y que funcionan de la misma forma que los keyloggers.

Impacto: Consecuencias que produce un incidente de seguridad de la información sobre la E.S.E y sus sedes.

Incidente de seguridad de la información: Un incidente de seguridad de la información es la violación o amenaza inminente a la violación de la política de seguridad y privacidad de la información, y seguridad digital. También se entiende como un incidente de seguridad de la información, a un evento que compromete la seguridad de un sistema (confidencialidad, integridad y disponibilidad).

Se entienden por incidentes de seguridad de la información las violaciones de acceso, intento de acceso, uso inadecuado, divulgación, modificación o destrucción no autorizada de información, cambios no controlados en el sistema, errores humanos, incumplimiento de política de seguridad y privacidad de la información, y seguridad digital, pérdida o robo de información, recurso tecnológico, activo de información o mal funcionamiento, manipulación, sabotaje, virus, códigos maliciosos, negación del servicio, violaciones de confidencialidad, entre otros.

Integridad: Condición de seguridad que garantiza que la información es actualizada, en todo su ciclo de vida, sólo por el personal y procedimientos autorizados.

Manual de Seguridad y Privacidad de la Información MSPI: El Modelo de Seguridad y Privacidad de la Información (MSPI), pertenece al habilitador transversal de Seguridad y Privacidad, de la Política de Gobierno Digital y busca garantizar un adecuado manejo de la información pública en poder de las entidades, la cual es uno de los activos más valiosos para la toma de decisiones, acorde con las buenas prácticas de seguridad y privacidad de la información, reúne los cambios técnicos de la norma 27001 del 2013, legislación de la Ley de Protección de Datos Personales, Transparencia y Acceso a la Información Pública, entre otras, las cuales se deben tener en cuenta para la gestión de la información.

Registro de Eventos: En ingles Logs. Mecanismo mediante el cual se guarda en un archivo (generalmente de texto) toda la información correspondiente a las actividades o eventos de un determinado sistema, dispositivo o equipo.

Riesgo: Probabilidad o posibilidad de que una amenaza aprovechando la vulnerabilidad o vulnerabilidades de un sistema, equipo o cualquier otro tipo

de activo, se concrete, causando daños, perjuicios o pérdidas a la organización propietaria del mismo.

Vulnerabilidad: Ausencia o debilidad de un control. Condición que podría permitir que una amenaza se materialice con mayor frecuencia, mayor impacto o ambas. Una vulnerabilidad puede ser la ausencia o debilidad en los controles administrativos, técnicos y/o físicos.

8. GESTION DE EVENTOS E INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN.

FASES DE LA GESTION DE INCIDENTES

Para lograr una correcta gestión de eventos o incidentes de seguridad de la información, en este manual se involucran las siguientes fases de manera cíclica como lo muestra la imagen:

1Fuente: Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información.

8.1. Fase 1 Preparación

La preparación garantiza que la entidad esté en capacidad de atender incidentes de manera organizada, rápida y eficaz. Asegura que el hospital cuente con los recursos, contactos, procedimientos y capacitación necesaria para enfrentar incidentes de seguridad de la información.

En esta fase, la función del **Profesional Universitario de Gestión de la Información** debe velar por la disposición de los recursos de atención de incidentes y las herramientas necesarias para cubrir las demás etapas del ciclo de vida del mismo, creando (si no existen) y validando (si existen) los procedimientos necesarios y programas de capacitación.

Esta fase debe ser apoyada por el **Jefe de Gestión de la Información** o quien este designe, incluyendo las mejores prácticas para el aseguramiento de activos de información, redes, sistemas, y aplicaciones, etc.

Actividades

- Mantener actualizada la lista de contactos de los responsables del proceso (Infraestructura, Aplicaciones, Jurídica, Oficial de

Protección de Datos Personales, Profesional Universitario Responsable).

- Verificar disponibilidad de herramientas básicas: antivirus, registros casos (GLPI, correo o teléfono), copias de seguridad, configuraciones de firewall y redes. inventario de activos, catálogo de servicios de TI, catálogo de infraestructura nagios y savis.
- Mantener documentación operativa necesaria: instructivos, políticas, lineamientos, formatos.
- Capacitar a funcionarios sobre detección y reporte de incidentes.
- Realizar auditoria en la gestión de parches de seguridad y aseguramiento de plataformas.
- Garantizar que exista un mecanismo de escalamiento claro y vigente.

Responsables

- Profesional Universitario.
- Equipo de Infraestructura.
- Equipo de Aplicaciones.
- Oficial de Protección de Datos Personales.

8.2. Fase 2 detección y análisis

Es la fase donde se identifica que ocurrió un incidente y se analiza su impacto, para detectar oportunamente incidentes de seguridad, clasificarlos y determinar su nivel de gravedad.

Se aclara que los incidentes de seguridad de la información son sucesos que contravienen las políticas de seguridad de la información institucionales y/o que generan acciones en contra de los principios de disponibilidad, integridad y confidencialidad de la información.

Los eventos o incidentes de seguridad de la información son sucesos que impiden el correcto procesamiento de la misma o la no prestación de los servicios tecnológicos. Algunos de estos eventos pueden tomarse como incidentes de seguridad de la información debido al impacto que pueden generar sobre el cumplimiento de los objetivos de los procesos de la E.S.E. Hospital Manuel Uribe Ángel y sus sedes.

Fuentes de detección

- Reportes de usuarios. (GLPI, teléfono, correo)
- Alertas de antivirus o sistemas de monitoreo.
- Anomalías en sistemas asistenciales o administrativos.
- Pérdida o robo de activos institucionales.
- Errores o eventos inusuales registrados en sistemas.

Actividades

A. Recepción del incidente (Profesional Universitario**)**

1. Registrar el incidente en GLPI.
2. Documentar información mínima: quién reporta, cuándo, qué ocurrió, evidencia disponible.

B. Análisis inicial (Profesional Universitario)

1. Validar si es un incidente o un evento.
2. Determinar si afecta datos personales o historia clínica.
3. Clasificar el incidente (ej.: acceso indebido, phishing, pérdida de equipo, malware, etc.).
4. Determinar impacto: alto, medio o bajo.
5. Definir áreas que deben participar: Infraestructura, Aplicaciones, Jurídica, Oficial de Protección de Datos o Jefe de Gestión de la Información.

Tabla de impacto

Determinación del Impacto de un Incidente de Seguridad

Nivel de Impacto	Criterios	Ejemplos en el hospital
ALTO	• Afecta historia clínica o datos personales sensibles. • Interrumpe un servicio asistencial (Urgencias, Hospitalización, Servinte, etc.). • Representa riesgo legal o disciplinario. • Pérdida o robo de equipo con información sensible. • Acceso indebido confirmado. • Malware que compromete servidores o múltiples equipos. • Riesgo reputacional.	• Acceso no autorizado a historia clínica. • Falsificación de incapacidad o documento oficial. • Robo de portátil de funcionario que manejaba datos. • Caída de Servinte por causa de un incidente. • Malware en un servidor. • Divulgación de información personal a terceros.
MEDIO	• Afecta un proceso no crítico. • Impacta parcialmente la disponibilidad, pero no detiene servicios. • No involucra datos sensibles, pero sí información interna. • Requiere intervención técnica o análisis forense sencillo.	• Malware en un equipo de oficina. • Pérdida de un mouse, celular corporativo sin datos o periféricos. • Fallas intermitentes en una aplicación no asistencial.

	• Requiere acciones preventivas inmediatas.	• Intentos sospechosos de acceso sin compromiso confirmado. • Uso indebido menor de recursos.
BAJO	• No afecta procesos misionales. • No involucra datos personales. • No compromete sistemas críticos. • No tiene impacto legal o disciplinario. • Se resuelve fácilmente y no requiere escalamiento.	• Correo sospechoso recibido, pero no abierto. • Alarmas de antivirus sin infección real. • Intentos de inicio de sesión fallidos sin riesgo asociado. • Errores menores en equipos aislados.

Para evaluar el impacto de un incidente de seguridad de la información, el profesional responsable deberá revisar la información del caso y compararla con los resultados del análisis de riesgos y la clasificación de activos institucionales. Con base en estos insumos, deberá determinar si el incidente afecta activos críticos, datos personales, procesos asistenciales o cualquier elemento clasificado como de alto riesgo. Esta evaluación permitirá asignar el nivel de impacto (**alto, medio o bajo**) y definir las acciones de respuesta que correspondan.

Clasificación de eventos y/o incidentes de seguridad de la información

La correcta clasificación de un evento o incidente es el primer paso para gestionar adecuadamente cualquier situación que afecte la seguridad de la información. Todos los funcionarios deben seguir este procedimiento para registrar, clasificar y escalar los casos de manera uniforme.

¿Qué debe hacer el funcionario cuando recibe o detecta un caso?

El funcionario o responsable deberá realizar los siguientes pasos en orden:

Paso 1: Identifique si es un *evento* o un *incidente*

Use esta regla sencilla:

- **Evento:** anomalía o situación que *no* afecta la confidencialidad, integridad o disponibilidad de la información, pero que podría convertirse en incidente.
- **Incidente:** situación que *sí afecta* o *puede afectar directamente* la información, los sistemas o los servicios del hospital.

Si hay duda, siempre clasifíquelo como **incidente** y el Profesional Universitario responsable verificará.

¿Cómo diferenciar un evento de un incidente?

A continuación, se presentan ejemplos claros para facilitar la clasificación:

Evento de Seguridad (no hay afectación directa)

Situación	Qué significa	Por qué es evento
No puedo acceder al correo	Error puntual o falla temporal	No compromete información
Alarma del antivirus sin infección	Comportamiento sospechoso	No hay daño confirmado
Modificación de datos no sensibles	Cambios menores	No afecta información crítica
Pérdida de información no crítica	Archivos no sensibles	Bajo riesgo

Incidente de Seguridad (hay afectación o riesgo real)

Situación	*Qué significa*	*Por qué es incidente*
Suplantación de identidad	Alguien usa credenciales de otro usuario	Compromete confidencialidad
Modificación de datos sensibles	Cambios en historia clínica u otros datos sensibles	Afecta integridad
Virus informático	Infección real en un equipo	Afecta disponibilidad
Robo o pérdida de un equipo con datos	Posible exposición de información	Alto riesgo

¿Qué debe hacer después de clasificar?

Una vez identificado si es evento o incidente, el funcionario responsable deberá:

Paso 2: Registrar la situación en GLPI

Debe ingresar:

- Descripción clara.
- Usuario afectado.
- Fecha y hora.
- Evidencias disponibles (capturas, fotos, correos).
- Categoría del catálogo de servicios.
- Principio afectado (Disponibilidad / Integridad / Confidencialidad).
- Si no sabe cuál categoría usar, seleccione “Seguridad de la Información” y el Profesional Universitario ajustará la clasificación.

Determinación del impacto, priorización y tiempo de atención

El Profesional Universitario encargado deberá seguir este procedimiento:
Paso 3: Evaluar el impacto

Use la tabla de impacto (alto, medio o bajo) teniendo en cuenta:

- Si se afecta historia clínica.
- Si hay datos personales o sensibles.
- Si se afecta un servicio asistencial.
- Si hay riesgos legales o disciplinarios.
- Si hay exposición de información.

Paso 4: Asignar prioridad

La prioridad debe estar alineada con:

- El impacto definido.
- La afectación al servicio.
- La urgencia del caso.

Ejemplo:

- Impacto alto → Prioridad crítica.
- Impacto medio → Prioridad media.
- Impacto bajo → Prioridad baja.

Paso 5: Definir el tiempo de atención

Los tiempos se establecerán según la tabla institucional de Acuerdo de Nivel de Servicio y la criticidad del servicio.

Regla general para todos los funcionarios

Si no sabe si es evento o incidente, clasifíquelo como incidente y repórtelo al Profesional Universitario Responsable de Seguridad de la Información. Es preferible reportar de más que pasar por alto un incidente que pueda afectar pacientes, historia clínica, datos personales o servicios asistenciales.

Resultado esperado

Siguiendo este procedimiento, cualquier funcionario podrá:

- Clasificar correctamente el caso.
- Registrarlo adecuadamente en GLPI.
- Identificar el principio afectado.
- Determinar impacto y prioridad.

- Garantizar que el incidente sea atendido de manera organizada.

Priorización de los incidentes de seguridad de la información
La priorización permite definir qué incidentes deben atenderse primero según su impacto en los servicios del hospital, la criticidad del activo afectado y la continuidad operativa. Esta priorización asegura una respuesta ordenada y coherente con la misión asistencial de la E.S.E. Hospital Manuel Uribe Ángel.

La prioridad de un incidente está directamente relacionada con:

- El nivel de impacto (alto, medio o bajo).
- La criticidad del servicio o proceso afectado.
- La importancia del activo de información comprometido.
- El riesgo hacia la confidencialidad, integridad o disponibilidad.

Una vez el Profesional Universitario responsable analiza el incidente, deberá asignar el nivel de prioridad correspondiente.

Niveles de Prioridad

Los incidentes se clasifican en tres niveles:

Nivel de Prioridad	Definición
ALTA	Incidentes que afectan directamente servicios misionales, procesos asistenciales, activos clasificados como críticos o información sensible (incluye historia clínica, datos personales sensibles o servicios estratégicos como Servinte). Requieren atención inmediata.
MEDIA	Incidentes que afectan servicios de apoyo o varias dependencias, sin comprometer directamente la operación asistencial. Su atención no es inmediata, pero sí prioritaria.
BAJA	Incidentes de impacto limitado que afectan a un usuario o dependencia y no comprometen información sensible ni la prestación del servicio asistencial.

Esta clasificación está alineada con las buenas prácticas de **ISO 27035**, **ITIL v4** y la **Guía 21 del MinTIC**, adaptada a la realidad del hospital.

Tiempos de Respuesta (ANS)

Los siguientes tiempos representan el **tiempo máximo para iniciar la atención**, no el tiempo total de solución.
La solución dependerá del tipo de incidente, capacidad técnica y complejidad del caso.

Nivel de Impacto	Tiempo Máximo para Iniciar la Atención

ALTO	≤ 24 horas
MEDIO	24 a 48 horas
BAJO	3 a 10 días

Estos tiempos permiten garantizar la continuidad de los servicios asistenciales y administrativos, priorizando la protección de los datos personales y la historia clínica.

Relación entre Impacto, Prioridad y Tiempo de Atención

Para facilitar la toma de decisiones, la siguiente tabla resume la relación entre impacto, nivel de prioridad y tiempo de respuesta:

Nivel de Impacto	Prioridad Asignada	Tiempo Máximo de Atención
ALTO	ALTA	≤ 24 horas
MEDIO	MEDIA	24 a 48 horas
BAJO	BAJA	3 a 10 días

El Profesional Universitario deberá:

- Revisar el impacto del incidente según la tabla institucional.
- Verificar la criticidad del activo o servicio afectado, usando el inventario de activos y análisis de riesgos.
- Asignar la prioridad utilizando la tabla anterior.
- Registrar en GLPI la prioridad y el tiempo máximo para iniciar la atención.
- Informar al equipo correspondiente (Infraestructura, Aplicaciones, Jurídica o Protección de Datos) según la prioridad definida.
- Monitorear el cumplimiento del tiempo establecido.

Si existe cualquier duda sobre la prioridad, deberá asignarse prioridad ALTA y escalar inmediatamente al Jefe de Gestión de la Información.

8.3. Fase 3 contención erradicación y recuperación

Esta fase busca evitar la propagación del incidente, minimizar su impacto y restablecer la operación normal del hospital, garantizando la **confidencialidad, integridad y disponibilidad** de la información.

La etapa se divide en tres partes:

- **Contención**
- **Erradicación**
- **Recuperación**

Contención

La contención consiste en detener el avance del incidente y evitar que cause mayores afectaciones a los activos de información, a la infraestructura tecnológica o a los servicios asistenciales.
El Profesional Universitario, con apoyo de Infraestructura o Aplicaciones, deberá aplicar medidas inmediatas para aislar el incidente y proteger los sistemas.

Objetivos de la contención

- Impedir la expansión del incidente.
- Proteger activos críticos e información sensible.
- Evitar interrupciones adicionales en servicios tecnológicos o asistenciales.
- Preparar el entorno para la recolección adecuada de la evidencia.

Recolección y manejo de evidencias

Una vez aplicada la contención, se debe recolectar, registrar y preservar la evidencia del incidente.

Toda evidencia debe cumplir los siguientes principios:

Autenticidad

El funcionario responsable debe garantizar que la evidencia corresponde fielmente a lo ocurrido.

Cadena de custodia

Debe existir un registro detallado indicando:

- Quién la recolectó,
- Cómo fue recolectada,
- Dónde se almacenó,
- Quién la transportó,
- Quién la analizó.

Esto evita alteraciones que afecten posibles procesos administrativos o legales.

Integridad y validación

Se debe garantizar que la evidencia no fue modificada durante su manipulación y que puede ser usada ante autoridades si se requiere.

Acciones mínimas durante la recolección de evidencia

El funcionario designado deberá:

- Registrar la información relacionada con la evidencia.
- Tomar fotografías del entorno físico o digital de la evidencia.
- Tomar y asegurar la evidencia (física o digital).
- Rotular todos los medios recolectados.
- Registrar la evidencia en el formato correspondiente.
- Almacenar la evidencia en un lugar seguro.
- Generar copias de seguridad de la evidencia original.

Una vez controlado el incidente, se debe proceder con:

Erradicación

Consiste en eliminar la causa del incidente, incluyendo código malicioso, configuraciones indebidas o accesos no autorizados.

Ejemplos de acciones de erradicación:

- Eliminar malware o archivos maliciosos.
- Deshabilitar cuentas, puertos o servicios comprometidos.
- Sustituir archivos manipulados por versiones limpias.
- Aplicar parches o correcciones técnicas.
- Eliminar software no autorizado.
- Bloquear accesos indebidos en firewall o directorio activo.
- Identificar y cerrar vulnerabilidades.

Recuperación

La recuperación asegura el retorno del servicio o activo a su estado normal de funcionamiento, garantizando que no existan riesgos de reinfección o repetición del incidente.

Ejemplos de acciones de recuperación:

- Restaurar copias de seguridad.
- Reinstalar sistemas o aplicaciones.
- Restaurar equipos afectados.
- Validar la integridad de datos y configuraciones.
- Realizar endurecimiento del sistema (hardening).
- Monitorear por un tiempo prudente para evitar reaparición del incidente.

Ejemplos según clasificación y tratamiento de incidentes

A continuación, se presenta una tabla organizada por **clase de incidente**, con su **concepto**, **tipos identificados** y el **tratamiento recomendado** en las fases de contención, erradicación y recuperación.

Clase de incidente	Concepto	Tipo de incidente	Tratamiento
Denegación del Servicio (DoS / DDoS)	Incidentes donde un sistema, servicio o red deja de operar a su capacidad normal debido a saturación, eliminación o agotamiento de recursos.	• Tráfico masivo malicioso (mail bombing, SYN flood, UDP flood, DNS flood). • Peticiones excesivas desde uno o varios equipos (DoS / DDoS). • Bots o equipos zombis atacando un servicio.	**Contención:** • Bloquear o redirigir paquetes maliciosos. • Buscar canales alternos de comunicación. • Cambiar temporalmente la URL del servicio. • Detener IPs inválidas o sospechosas. • Cerrar procesos no deseados en servidores o routers. **Erradicación:** • Involucrar al proveedor de internet (ISP). • Aplicar filtrado avanzado de tráfico. • Restaurar el servicio afectado. **Recuperación:** • Restablecer el servicio a su estado original. • Verificar estabilidad post-incidente.
Acceso no autorizado	Acceso lógico o físico sin autorización a sistemas, aplicaciones o información.	• Ataques de fuerza bruta. • Captura de credenciales (keyloggers). • Consultas no autorizadas.	**Contención:** • Apagar el sistema afectado. • Bloquear usuarios o

Clase de incidente	Concepto	Tipo de incidente	Tratamiento
		• Acceso a carpetas o bases de datos privadas. • Creación de usuarios sin autorización. • Intrusión física.	accesos sospechosos. **Erradicación:** • Cambiar contraseñas. • Implementar bloqueos automáticos por intentos fallidos. • Identificar puntos de acceso usados por el atacante. • Reconfigurar firewall o deshabilitar dispositivos comprometidos. **Recuperación:** • Reactivar las cuentas autorizadas. • Habilitar nuevamente el sistema.
Modificación no autorizada de recursos	Alteración o eliminación no autorizada de información o software.	• Borrado de información. • Modificación de datos. • Instalación o eliminación de software sin autorización.	**Contención:** • Bloquear usuarios o accesos sospechosos. **Erradicación:** • Corregir los efectos producidos. • Reemplazar archivos comprometidos por versiones limpias. **Recuperación:** • Restaurar backups. • Instalar versiones actualizadas de software.

8.4. Fase 4 Post-Incidente

Las actividades post-incidentes permiten documentar lo ocurrido, analizar la efectividad de la respuesta y mejorar continuamente los controles de seguridad del hospital. Una adecuada gestión posterior al incidente contribuye a prevenir la repetición de eventos similares y fortalece la capacidad institucional.

Esta etapa incluye:

- Elaboración del informe de incidente.
- Identificación y documentación de lecciones aprendidas.
- Definición de medidas tecnológicas, disciplinarias o penales cuando corresponda.
- Registro del incidente en la base de conocimiento para fortalecer los indicadores del proceso.

Informe del incidente

Una vez restablecido el servicio o activo afectado, el Profesional Universitario responsable deberá preparar un informe completo del incidente, dirigido al nivel correspondiente (Infraestructura, Aplicaciones, Jurídica, Protección de Datos o Dirección, según el caso).

El informe debe contener como mínimo:

1. Descripción del incidente: qué ocurrió, cuándo y cómo se detectó.
2. Sistemas, usuarios o activos afectados.
3. Causa identificada del incidente.
4. Acciones de contención, erradicación y recuperación aplicadas.
5. Tiempo total del incidente:
    - Tiempo sin servicio.
    - Tiempo para iniciar la atención.
    - Tiempo total de resolución.
6. Evidencias recolectadas.
7. Lecciones aprendidas y medidas de mejora.
8. Recomendaciones y acciones preventivas**.**

Una copia del informe se registrará en GLPI y se incluirá en los indicadores del proceso de Gestión de la Información, así como en el informe gerencial correspondiente.

Lecciones aprendidas

El análisis de lecciones aprendidas permite mejorar continuamente el proceso de gestión de incidentes y fortalecer las capacidades institucionales. Este análisis debe realizarse:

- Después de incidentes de alto impacto.
- Periódicamente para incidentes de impacto medio y bajo.

El objetivo es identificar:

- Qué ocurrió realmente y cómo se gestionó.
- La eficacia de los procedimientos aplicados.
- Oportunidades de mejora en controles, herramientas y recursos.
- Acciones que podrían haber evitado o minimizado el incidente.
- Elementos que deben ajustarse para una respuesta más efectiva en el futuro.

Aspectos que debe analizar el equipo en las lecciones aprendidas

- Secuencia real de los hechos.
- Decisiones tomadas y su efectividad.
- Si los responsables actuaron según los procedimientos documentados.
- Controles que fallaron o no existían.
- Medidas preventivas que deben implementarse.
- Necesidades de capacitación o actualización del personal.
- Requerimientos de herramientas o recursos para mejorar la detección o mitigación.

Registro de las lecciones aprendidas

Actualmente, la herramienta GLPI no cuenta con un campo exclusivo para registrar lecciones aprendidas. Por ello, se debe:

- Registrar las lecciones aprendidas en el campo de observaciones del ticket.
- Incluir el código del incidente para relacionarlo con la base de conocimiento del hospital.
- Adjuntar en el ticket las evidencias, análisis, decisiones y acciones tomadas.
- Vincular el incidente con un registro en la base de conocimiento que detalle:
    - La causa.
    - Las acciones de respuesta.
    - Las recomendaciones para prevenir incidentes futuros.

Medidas Tecnológicas, Disciplinarias o Penales

Según la naturaleza del incidente, el Profesional Universitario deberá coordinar con:

- **Infraestructura o Aplicaciones:** implementación de mejoras técnicas.
- **Protección de Datos:** análisis de implicaciones legales o regulatorias.
- **Jurídica:** evaluación de posibles faltas disciplinarias o delitos.
- **Talento Humano:** aplicación de acciones correctivas o disciplinarias si corresponde.

Resultado de la fase post-incidente

Al finalizar esta etapa, el hospital deberá contar con:

- Un informe completo y formal del incidente.
- Un registro actualizado en GLPI con toda la trazabilidad.
- Lecciones aprendidas documentadas e incorporadas a la base de conocimiento.
- Medidas de mejora definidas e incluidas en el plan de trabajo del proceso.
- Un fortalecimiento real de los controles internos y capacidades institucionales.

9. MECANISMOS DE DIVULGACIÓN

La divulgación del proceso de gestión de eventos e incidentes de seguridad de la información se realizará de manera continua y estructurada, asegurando que todos los funcionarios, contratistas y personal autorizado conozcan las obligaciones, canales y procedimientos para el reporte de incidentes.

Los mecanismos establecidos por la E.S.E. Hospital Manuel Uribe Ángel son:

9.1. Programa de Inducción y Reinducción

Atreves del programa de inducción y reinducción institucional, se socializa:

- Qué es un evento y qué es un incidente de seguridad de la información.
- Cómo y a través de qué canales deben reportarse (GLPI, correo, teléfono).
- El rol del Profesional Universitario responsable.
- Las responsabilidades individuales frente al manejo adecuado de la información.

9.2. Capacitación periódica

El Profesional Universitario de Gestión de la Información, con apoyo de las capacidades de Infraestructura, Aplicaciones y Protección de Datos, realizará sesiones, charlas, boletines, entre otras para:

- Actualizar a los funcionarios sobre nuevas amenazas.
- Reforzar la detección temprana y el reporte oportuno.
- Socializar casos reales y lecciones aprendidas.
- Recordar la importancia de la seguridad de la información en los servicios asistenciales y administrativos.

9.3. Comunicaciones internas institucionales

Se utilizan los canales institucionales para divulgar información relevante como:

- Boletines de alertas de seguridad.
- Recomendaciones preventivas.
- Cambios en los procedimientos.
- Buenas prácticas para el uso seguro de sistemas, correo electrónico e Internet.

Los canales incluyen el correo institucional, la intranet, ventanas web y comunicados internos.

9.4. Actualización del manual y base de conocimiento

El manual y sus procedimientos asociados estarán disponibles para consulta en:

- La base de conocimiento y casos de GLPI.
- La intranet institucional.
- Los repositorios documentales del proceso de Gestión de la Información.

Esto permite que cualquier funcionario consulte el procedimiento oficial de forma rápida y actualizada.

10. MECANISMOS DE EVALUACIÓN

Los mecanismos de evaluación permiten medir la eficacia del proceso de gestión de eventos e incidentes de seguridad de la información, identificar tendencias, tomar decisiones de mejora y garantizar el cumplimiento de los lineamientos institucionales y normativos.

Para ello, la E.S.E. Hospital Manuel Uribe Ángel establece los siguientes indicadores:

10.1. Indicador de Eventos de Seguridad de la Información

Objetivo: Medir la cantidad de eventos de seguridad registrados en un periodo determinado y evaluar el comportamiento institucional frente a la detección temprana de anomalías.

Fórmula: Número total de eventos de seguridad registrados / periodo evaluado.

Interpretación: Un incremento sostenido puede indicar fallas en controles técnicos, errores de operación o necesidad de ajustar políticas; un descenso significativo puede estar asociado a controles efectivos o a falta de reporte, lo cual también debe evaluarse.

10.2. Indicador de Incidentes de Seguridad de la Información

Objetivo: Determinar la cantidad de incidentes gestionados, su criticidad y el cumplimiento de los tiempos de atención definidos en el manual.

Fórmulas:

1. Número total de incidentes atendidos / periodo evaluado.
2. Porcentaje de incidentes atendidos dentro del tiempo máximo definido (ANS):

(Incidentes atendidos dentro del tiempo establecido ÷ Incidentes totales) × 100

Interpretación: Permite evaluar la capacidad de respuesta del hospital y detectar necesidad de ajustes en recursos, procesos o controles de seguridad.

10.3. Uso de los indicadores

Los indicadores deben permitir:

- Monitorear tendencias en tipos de incidentes.
- Identificar áreas o servicios con mayor exposición o vulnerabilidad.
- Evaluar el desempeño del proceso y del equipo de respuesta.
- Alimentar el informe para Sub-mesa de Gobierno Digital liderada por el proceso de Gestión de la Información.
- Orientar acciones preventivas, correctivas y de capacitación.

Los resultados deben socializarse cuatrimestralmente con el Jefe de Gestión de la Información y reportarse en los informes de gestión institucional.

11. DOCUMENTOS RELACIONADOS

- FIF033 Autorización para el tratamiento de datos personales de paciente incapaz o con pérdida de consciencia
- FIF034 Autorización para el tratamiento de datos personales
- FIF035 Autorización para recolección y tratamiento de datos, y consulta en bases de datos funcionarios y candidatos
- IIF036 Instructivo de inventario clasificación de activos y etiquetado de información
- FIF038 Acuerdo para compartir datos personales
- FIF039 Autorización para recolección y tratamiento de datos, y consulta en bases de datos
- FAF325 Formato gestión de contingencias
- FIF026 Préstamo de elementos tecnológicos
- IIF016 Instructivo de respaldo y recuperación
- IIF038 Instructivo para la creación, modificación e inactivación de usuarios SIMUA
- IIF029 Instructivo para monitoreo y disponibilidad de infraestructura tecnológica
- IIF019 Instructivo para creación y seguimiento de tickets GLPI
- IIF031 Instructivo para el mantenimiento preventivo de hardware y software
- MIF013 Modelo de seguridad y privacidad de la información
- MIF024 Catálogo de componentes de información
- MIF022 Catálogo de elementos de infraestructura tecnológica
- MIF023 Ciclo de vida de los sistemas de información
- MIF021 Catálogo de sistemas de información
- MIF018 Manual catálogo de servicios tic
- MIF025 Esquema de gobierno de los componentes de información
- MIF026 Manual de protección de datos personales
- PIF005 Proceso activación del plan de contingencia
- MGE003 Manual del sistema integrado de gestión de riesgos
- LIF001 Política tratamiento y protección de datos personales
- LIF003 Política de seguridad y privacidad de la información y seguridad digital

12. BIBLIOGRAFIA

La presente bibliografía reúne los documentos, lineamientos y referencias normativas utilizados para la elaboración y actualización del Manual de Gestión de Incidentes de Seguridad de la Información de la E.S.E. Hospital Manuel Uribe Ángel.

Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC.
Guía 21: Gestión de Incidentes de Seguridad de la Información.
Modelo de Seguridad y Privacidad de la Información – MSPI, República de Colombia.

Superintendencia de Industria y Comercio – SIC.
Guía de Responsabilidad Demostrada para el Tratamiento de Datos Personales.
Dirección de Protección de Datos Personales, República de Colombia.

Ley 1581 de 2012.
Por la cual se dictan disposiciones generales para la protección de datos personales.

Decreto 1377 de 2013.
Por el cual se reglamenta parcialmente la Ley 1581 de 2012.

Norma ISO/IEC 27035-1:2023.
Gestión de incidentes de seguridad de la información – Principios y procesos.

Norma ISO/IEC 27001:2022.
Tecnologías de la Información – Sistemas de Gestión de Seguridad de la Información – Requisitos.

Política de Seguridad y Privacidad de la Información de la E.S.E. Hospital Manuel Uribe Ángel.
Versión vigente.