HOSPITAL DEPARTAMENTAL SAN VICENTE DE PAÚL E.S.E.

GARZÓN – HUILA

PROCEDIMIENTO PARA LA GESTIÓN DE INCIDENTES DE SEGURIDAD DIGITAL

EMPRESA SOCIAL DEL ESTADO
HOSPITAL DEPARTAMENTAL SAN VICENTE DE PAÚL
GARZON - HUILA

PROCEDIMIENTO PARA LA GESTIÓN DE INCIDENTES DE SEGURIDAD DIGITAL

PROCESO
GESTION DE APOYO CORPORATIVO

CARLOS DANIEL MAZABEL CORDOBA
Gerente

DIANA LUCIA MONTES CABRERA
Subdirector Administrativo

GARZON – HUILA

Calle 7 No. 14-69 PBX (608) 8332441 Ext: 256 Fax (608) 8333225 Gerencia (608) 8332570
web: www.hospitalgarzon.gov.co – Email: coordinadorsistemas@hospitalsvpgarzon.gov.co, gerencia@hospitalsvpgarzon.gov.co
Garzón (Huila).

CUERPO DIRECTIVO
EMPRESA SOCIAL DEL ESTADO
HOSPITAL DEPARTAMENTAL SAN VICENTE DE PAUL.

CARLOS DANIEL MAZABEL CORDOBA
Gerente

JAIME ORLANDO GOMEZ GONZALEZ
Asesor de Control Interno

PABLO LEON PUENTES QUESADA
Subdirector Científico

DIANA LUCIA MONTES CABRERA
Subdirector Administrativo

LUIS FERNANDO CASTRO MAJE
Asesor Jurídico

MARYBEL CASTAÑO RODRIGEZ
Líder de Mejora Continua

HECTOR LEANDRO RENDON
Coordinador de sistemas
Autor(a).

GARZON HUILA

Calle 7 No. 14-69 PBX (608) 8332441 Ext: 256 Fax (608) 8333225 Gerencia (608) 8332570
web: www.hospitalgarzon.gov.co – Email: coordinadorsistemas@hospitalsvpgarzon.gov.co, gerencia@hospitalsvpgarzon.gov.co
Garzón (Huila).

MARCO ESTRATEGICO

1. PROPÓSITO

El objetivo de este procedimiento es establecer un marco organizado para gestionar, resolver y aprender de los incidentes que puedan ocurrir en la organización. Asegura la correcta identificación, evaluación, respuesta y documentación de cada incidente, con el fin de minimizar su impacto y mejorar la resiliencia organizacional.

2. ALCANCE

Este procedimiento cubre todos los incidentes que puedan afectar las operaciones, sistemas, procesos o recursos de la ESE Hospital departamental San Vicente de Paul. Los incidentes pueden incluir, pero no se limitan a:

- Fallos en sistemas tecnológicos.
- Brechas de seguridad.
- Desastres naturales (inundaciones, terremotos, etc.).
- Accidentes de trabajo.
- Incidentes de salud.
- Otros eventos inesperados.

3. DEFINICIÓN DE INCIDENTE

Un **incidente** es cualquier evento no planificado que interrumpe o podría interrumpir el funcionamiento normal de los servicios o procesos dentro de la organización.

4. CLASIFICACIÓN DE INCIDENTES

Los incidentes se clasificarán según:

- **Gravedad**:
  - Crítico (impacta operaciones esenciales y requiere acción inmediata).
  - Alto (afecta operaciones importantes, pero con opciones de mitigación).
  - Medio (no afecta gravemente las operaciones, pero debe ser resuelto).
  - Bajo (no tiene impacto inmediato o significativo, se resuelve a largo plazo).

- **Tipo de Incidente**:
  - Ciberseguridad
  - Tecnológico (sistemas, software, hardware)
  - Físico (daños materiales, fallos estructurales)
  - Salud y Seguridad

5. PROCEDIMIENTO DETALLADO DE GESTIÓN DE INCIDENTES

Paso 1: Identificación del Incidente

- **Responsable**: Personal de sistemas.
- **Acción**: Detectar, identificar y reportar el incidente inmediatamente a través de un sistema de notificación preestablecido (correo electrónico, teléfono, plataforma de gestión de incidentes, etc.).
- **Documento generado**: Formulario de reporte de incidente.

Calle 7 No. 14-69 PBX (608) 8332441 Ext: 256 Fax (608) 8333225 Gerencia (608) 8332570
web: www.hospitalgarzon.gov.co – Email: coordinadorsistemas@hospitalsvpgarzon.gov.co, gerencia@hospitalsvpgarzon.gov.co
Garzón (Huila).

Paso 2: Registro del Incidente

- **Responsable**: Equipo de sistemas encargado de la gestión de incidentes.
- **Acción**: Registrar el incidente, Incluir los detalles: tipo de incidente, descripción, fecha y hora de ocurrencia, clasificación (por gravedad), y responsable de la atención inicial.
- **Documento generado**: Registro del incidente en el sistema.

Paso 3: Evaluación y Priorización

- **Responsable**: Equipo de sistemas.
- **Acción**: Evaluar el impacto y la urgencia del incidente, priorizándolo según su gravedad. Determinar la necesidad de escalar el incidente a otros niveles.
- **Documento generado**: Análisis preliminar del impacto y prioridad.

Paso 4: Respuesta Inicial

- **Responsable**: Equipo de sistemas.
- **Acción**: Tomar acciones inmediatas para contener el incidente (por ejemplo, desconectar sistemas afectados, bloquear accesos, activar protocolos de seguridad, activar planes de emergencia).
- **Documento generado**: Registro de acciones iniciales.

Paso 5: Investigación y Resolución

- **Responsable**: Equipo de sistemas.
- **Acción**: Realizar una investigación más detallada para identificar la causa raíz del incidente. Desarrollar una solución para resolver el incidente. Esto puede incluir reparación de sistemas, restauración de servicios, etc.
- **Documento generado**: Informe de investigación y resolución.

Paso 6: Comunicación

- **Responsable**: Coordinador de sistemas.
- **Acción**: Mantener a todas las partes interesadas informadas. Esto incluye:
    - Comunicación con empleados o usuarios internos afectados.
    - Notificaciones a partes externas (clientes, proveedores, autoridades).
    - Informes de estado periódicos.
- **Documento generado**: Comunicados de estado.

Paso 7: Recuperación y Restauración

- **Responsable**: Equipo de TI.
- **Acción**: Una vez resuelto el incidente, restaurar los servicios afectados a su funcionamiento normal. Verificar que todos los sistemas estén operativos y realizar pruebas para asegurar la efectividad de la solución.
- **Documento generado**: Informe de restauración y validación.

Paso 8: Cierre del Incidente

- **Responsable**: Coordinador de sistemas
- **Acción**: Después de que el incidente ha sido resuelto y los servicios se hayan restaurado, cerrar el incidente formalmente. Documentar todas las acciones tomadas, resultados y cualquier lección aprendida.
- **Documento generado**: Informe de cierre del incidente.

Paso 9: Análisis Post-Incidente (Lecciones Aprendidas)

- **Responsable**: Equipo de gestión de incidentes y partes interesadas.
- **Acción**: Reunir al equipo para realizar un análisis post-mortem. Evaluar la respuesta, identificar áreas de mejora y actualizar los procedimientos, si es necesario.
- **Documento generado**: Informe de lecciones aprendidas y recomendaciones.

Calle 7 No. 14-69 PBX (608) 8332441 Ext: 256 Fax (608) 8333225 Gerencia (608) 8332570
web: www.hospitalgarzon.gov.co – Email: coordinadorsistemas@hospitalsvpgarzon.gov.co, gerencia@hospitalsvpgarzon.gov.co
Garzón (Huila).

6. ROLES Y RESPONSABILIDADES

- **Reportador del Incidente**: Cualquier empleado o usuario que detecte el incidente.
- **Equipo de Primera Respuesta**: Equipo de sistemas, contener el incidente y registrar el caso.
- **Equipo de Soporte Técnico**: Especialistas encargados de investigar, diagnosticar y resolver el incidente.
- **Gerentes de Comunicación**: Responsables de mantener informadas a las partes interesadas sobre el estado del incidente.
- **Líder de Gestión de Incidentes**: responsable general de coordinar la resolución, comunicación y cierre del incidente.

7. HERRAMIENTAS Y RECURSOS

- **Sistema de gestión de incidentes**: Plataforma donde se registran, hacen seguimientos y gestionan los incidentes (Formulario de google).
- **Protocolos y procedimientos documentados**: Guías claras para la acción ante incidentes de cada tipo (ciberseguridad, desastre natural, fallos técnicos).
- **Planes de contingencia**: Incluir documentos para planes de recuperación ante desastres o incidentes graves.

8. REVISIÓN Y MEJORA CONTINUA

- Después de cada incidente, realizar una **revisión periódica** para evaluar la respuesta, las áreas de mejora y actualizar procedimientos y políticas según sea necesario.
- Incluir sesiones de **formación y simulacros** regulares para mantener al personal entrenado en la gestión efectiva de incidentes.

PROCEDIMIENTO PARA LA GESTIÓN DE INCIDENTES DE SEGURIDAD DIGITAL		
Actualizado por: HECTOR LEANDRO RENDON RUIZ	**Revisado por:** DIANA LUCIA MONTES CABRERA	**Aprobado por:** CARLOS DANIEL MAZABEL CORDOBA
Cargos: COORDINADOR DE SISTEMAS DE INFORMACIÓN	**Cargo:** SUBDIRECTORA ADMINISTRATIVA	**Cargo:** GERENTE
Aprobado mediante resolución N° 0050 de 31 de enero de 2025. Adoptan los planes de acción vigencia 2025 por virtud de la ley 1474 de 2011 y los planes institucionales fijados por el decreto 612 de 2018 para la ESE Hospital Departamental San Vicente de Paúl		

Calle 7 No. 14-69 PBX (608) 8332441 Ext: 256 Fax (608) 8333225 Gerencia (608) 8332570
web: www.hospitalgarzon.gov.co – Email: coordinadorsistemas@hospitalsvpgarzon.gov.co, gerencia@hospitalsvpgarzon.gov.co
Garzón (Huila).