PLAN DE LA SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

ESE HOSPITAL NAZARETH QUINCHIA RISARALDA

2021

Contenido

INTRODUCCIÓN 4
1. ALCANCE 5
2. OBJETIVO GENERAL 5
3. DEFINICIONES 5
4. NORMATIVIDAD RELACIONADA 6
5. COMPROMISO DE LA DIRECCIÓN 6
6. MISION 8
7. VISION 8
8. OBJETIVOS INSTITUCIONALES 8
9. GOBIERNO DE SEGURIDAD 7
9.1. Estructura de roles 8
9.1.1. Comité de gerencia de la información 8
9.1.2. Oficial de seguridad CISO 11
9.1.3. Administradores de seguridad de la información 13
9.1.4. Líderes de proceso 15
9.2. Objetivos de seguridad 16
10. COMUNICACIÓN CON EL COMITÉ DE GOBIERNO DE INFORMACIÓN 17
11. LINEAMIENTOS DE SEGURIDAD 18
11.1. Gestión de activos 18
11.2. Uso aceptable de los activos 18
11.2.1. Acceso a Internet: 19
11.2.2. Correo electrónico: 20
11.2.3. Recursos tecnológicos 22
11.3. Acuerdos sobre confidencialidad 24
11.4. Partes externas 24
11.5. Clasificación de la información 24
11.6. Seguridad de los recursos humanos 25
9.6.1. Roles y responsabilidades 26
9.6.2. Selección de personal 26
9.6.3. Términos y condiciones laborales 26
9.6.4. Educación, formación y concientización sobre la Seguridad de la Información 27
9.6.5. Proceso disciplinario 27
9.6.6. Terminación o cambio de la contratación laboral 28
9.6.7. Responsabilidades en la terminación o cambio de funciones 28
9.6.8. Devolución de Activos. 28
9.7. Seguridad física y del entorno 28
9.7.1. Controles de Acceso Físico 29
9.7.2. Protección y ubicación de los equipos 29

9.7.3. Seguridad de los equipos y medios de información fuera de las instalaciones 31
9.7.4. Eliminación o reutilización segura de equipos y medios 31
9.8. Gestión de comunicaciones y operaciones 32
9.8.1. Documentación de procedimientos operativos 32
9.8.2. Control de Cambios 32
9.8.3. Segregación de funciones 32
9.8.4. Separación de los ambientes de desarrollo, prueba y producción 33
9.8.5. Gestión de la capacidad 34
9.8.6. Aceptación de sistemas 35
9.8.7. Protección contra software malicioso 35
9.8.8. Copias de Respaldo 36
9.8.9. Gestión de medios removibles 37
9.8.10. Intercambio de información 37
10. BIBLIOGRAFÍA 39
11. SEGUIMIENTO, CONTROL Y MEJORA 39
12. MODIFICACIONES 39
13. APROBACIÓN. 40

INTRODUCCIÓN

ESE Hospital Nazarteh de Quinchía Risaralda reconoce la información como un activo importante para la atención de los pacientes y el desarrollo de sus procesos internos, por lo tanto, se preocupa por definir lineamientos que permitan mitigar los posibles riesgos para la Información.

El plan de seguridad y privacidad de la información es un documento que contiene los lineamientos que apoyan la gestión y administración de los planes y procedimientos de seguridad de la información dando claridad sobre las prácticas de seguridad aplicadas a la institución.

1. ALCANCE

El plan contempla la estructura de gobierno y los lineamientos principales para la seguridad de la información en el Hospital Nazareth. Los lineamientos definidos en este documento deben ser conocidos y cumplidos por empleados, contratistas y todos los terceros que tengan acceso, almacenen, procesen o trasmitan información de la institución o sus pacientes.

2. OBJETIVO GENERAL

Establecer los lineamientos principales de gobierno y gestión de la seguridad de la información para el Hospital Nazareth de Quinchia

3. DEFINICIONES

3.1. **Activos de información:** Elementos de Hardware y de Software de procesamiento, almacenamiento y comunicaciones, bases de datos y procesos, procedimientos y recursos humanos asociados con el manejo de los datos y la información misional, operativa y administrativa de cada entidad, órgano u organismo.
Este tipo de activo representa los datos de la organización, información que tiene valor para los procesos de negocio, independientemente de su ubicación: puede ser un documento físico debidamente firmado, un archivo guardado en un servidor, un aplicativo o cualquier elemento que permita almacenar información valiosa o útil para el Hospital Nazareth de Quinchia.

3.2. **Comité de Seguridad de la Información** (CSI): Instancia del nivel superior, que deben validar la Política de Información, así como los procesos, procedimientos y metodologías específicas de seguridad de la información para el adecuado uso y administración de los recursos informáticos y físicos, asignados a los servidores públicos de cada ente público.

3.3. **Confidencialidad**: Propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados.

3.4. **Control:** Es toda actividad o procesos encaminado a mitigar o evitar un riesgo. Incluye políticas, procedimientos, guías, estructuras organizacionales, buenas Gprácticas que pueden ser de carácter administrativo, técnico o legal.

3.5. **Disponibilidad:** Propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada.

3.6. **Evento de seguridad de la información:** Se considera un Evento de Seguridad de la Información a cualquier situación identificada que indique una posible brecha en la Política de Información o falla en los controles y/o protecciones establecidas.

3.7. **Incidente de seguridad de la información:** Un incidente de seguridad de la información se define como un acceso, uso, divulgación, modificación o destrucción no autorizada de la información del Hospital Nazareth y de sus usuarios; un impedimento en la operación normal de las redes, sistemas o recursos informáticos; o cualquier otro acto que implique una violación a la Política de Información.

3.8. **Integridad:** Propiedad de salvaguardar la exactitud y estado completo de los activos.

3.9. **Propietario/responsable de activo de información**: Individuo, entidad o unidad de negocio que ha aceptado la responsabilidad de la administración para el control, producción, desarrollo, mantenimiento, uso y seguridad de los activos de información.

3.10. **Servicio:** Es cualquier acto o desempeño que una persona puede ofrecer a otra que es esencialmente intangible y que no conlleva ninguna propiedad. Su producción puede o no estar ligada a un producto físico.

3.11. **Usuario:** Es el nombre (o alias) que se le asigna a cada persona para ser identificado por el servidor, de esta manera el proveedor de Internet o de correo electrónico lo identifica, es única en cada servidor, y cada usuario tiene asignado una contraseña para poder acceder a su cuenta.

4. NORMATIVIDAD RELACIONADA

Para la construcción de este plan se tiene como base, la norma ISO – IEC 27001:2013 Sistema de Gestión de la Seguridad de la Información, el modelo de gestión de la seguridad de la información y la política de información del Hospital Nazareth de Quinchia.

5. COMPROMISO DE LA DIRECCIÓN

La Junta Directiva y Alta Dirección del Hospital Nazareth muestra su compromiso y apoyo en el diseño, implementación y mantenimiento del Sistema de Gestión de Seguridad de la Información a través de la asignación de recursos, la definición

de la política de

información, los lineamientos de seguridad y el establecimiento del Gobierno de seguridad, cuya conformación y responsabilidades se describen a continuación.

6. MISIÓN

Somos una empresa social del estado que presta servicios de salud de baja y mediana complejidad en el municipio de Quinchia y áreas circunvecinas, que cuenta con un equipo humano idóneo, comprometido y con alto sentido de responsabilidad social, enfocado al mejoramiento de las condiciones de salud de nuestros usuarios.

7. VISIÓN

Seremos en el año 2019 una institución de salud reconocida a nivel regional por sus altos estándares de calidad y humanización de los servicios, ofreciendo una atención integral orientada a la satisfacción de las necesidades de salud de la comunidad Quinchieña.

8. OBJETIVOS INSTITUCIONALES

- Propender por la interrelación entre los sistemas de gestión y los procesos institucionales con el fin de buscar la eficiencia.
- Prestar servicios de salud con estándares de calidad, buscando el fortalecimiento de la empresa.
- Capacitación del talento humano buscando el mejoramiento continuo de los procesos institucionales
- Establecer mecanismos de gestión administrativa y financiera que permitan la sostenibilidad económica a corto, mediano y largo plazo.
- Mejoramiento continuo encaminado al cumplimiento de los estándares de acreditación

9. GOBIERNO DE SEGURIDAD

La definición de un modelo de gobierno de seguridad adecuado representado en una estructura organizacional definida y aprobada por la institución permite la correcta toma de decisiones y ofrece una alineación y rumbo adecuado en las actividades para proteger los activos de información.

Una estructura organizacional es un organismo viviente dentro de la organización que puede cambiar según la estructura y las necesidades de la institución pero que en todo momento debe ser clarificada con el fin de que se conozca la cadena de

toma de decisión de cada uno de los temas necesarios para la gestión de la seguridad de la información.

Cada rol dentro del Gobierno debe tener unas responsabilidades asociadas para realizar su tarea, estas responsabilidades se asignan haciendo uso de una matriz RACI donde cada tipo de responsabilidad se asigna a los roles definidos. Los tipos de responsabilidades usados son los siguientes:

Tipo de responsabilidad			Descripción
R	***Responsible***	**Responsable**	Este rol corresponde a quien efectivamente realiza la tarea. Lo más habitual es que exista sólo un encargado (R) por cada tarea.
A	***Accountable***	**Quien rinde cuentas**	Este rol se responsabiliza de que la tarea se realice y es quien debe rendir cuentas sobre su ejecución. Sólo puede existir una persona que deba rendir cuentas (A) de que la tarea sea ejecutada por su responsable (R).
C	***Consulted***	**Consultado**	Este rol posee alguna información o capacidad necesaria para realizar la tarea. Se le informa y se le consulta información (comunicación bidireccional)
I	***Informed***	**Informado**	Este rol debe ser informado sobre el avance y los resultados de la ejecución de la tarea. A diferencia del consultado (C), la comunicación es unidireccional.

A continuación, se presenta la estructura de roles para el gobierno de seguridad de la información el Hospital Nazareth de Quinchía.

9.1. Estructura de roles

Rol	Objetivo
Comité de Gerencia de la información	• El comité de gerencia de la información toma las responsabilidades en el Hospital Nazaret del Comité de seguridad de la información. • Como objetivo principal para la seguridad de la información este comité realiza la aprobación de lineamientos estratégicos en cuanto a seguridad de la información, garantiza los recursos y la toma de decisiones orientadas al cumplimiento de la estrategia por ellos definida.
Comité de gobierno en línea	• Supervisa la aplicación de los requisitos definidos por gobierno en línea en lo relacionado con la seguridad de la información.
Oficial de seguridad de la información (CISO)	• Tiene la responsabilidad de guiar y realizar el seguimiento de la implementación de los planes de seguridad definidos.
Administrador de seguridad de la información (ISM)	• Tienen la responsabilidad de la gestión de los esfuerzos de seguridad de la información, encargado de labores específicas de seguridad.
Líderes de procesos	• Tienen la responsabilidad de dar la cobertura de los lineamientos de seguridad a cada uno de sus procesos operacionales.

9.1.1. Comité de gerencia de la información.

Objetivo	• Garantizar a través del monitoreo y la revisión, la aplicación de las buenas prácticas en seguridad de la información y la toma de decisiones orientadas al cumplimiento de la estrategia. • Aprobar los lineamientos estratégicos en cuanto a seguridad de la información y garantizar los recursos para su cumplimiento.

Principios de operación	• El comité se debe reunir de forma mensual o cuando una eventualidad lo requiera. • La participación de los designados en el Comité es obligatoria, en caso de no poder asistir se debe enviar un sustituto que contará con el mismo poder de decisión. • El número de miembros del comité se limita a un grupo relativamente pequeño de líderes estratégicos y tácticos

	para asegurar la comunicación y toma de decisiones apropiado. • Las actas de todas las reuniones deben ser aprobadas y almacenadas por un plazo de 2 años. • El CISO preside las reuniones del comité.
Responsabilidades	• El comité es el responsable de que las decisiones de seguridad de la información estén orientadas al apoyo de las decisiones estratégicas.

9.1.1.1. Conformación de Comité de seguridad

Rol	Descripción
CISO	• Responsable del seguimiento global de la seguridad de la información. • Debe administrar las iniciativas de seguridad definidas en el comité • Debe tener una comprensión de los riesgos empresariales/operativos, costos y beneficios, y los requisitos específicos de seguridad de la información aplicables al hospital.
Director financiero	• Responsable de la asignación presupuestal para las iniciativas de seguridad definidas por el comité. • Responsable de aplicar las iniciativas de seguridad concernientes a la captura, procesamiento y distribución de la información financiera.
Comunicador	• Responsable de definir la manera apropiada de dar a conocer las iniciativas de seguridad a todas las partes interesadas.
Director Apoyo Logístico	• Debe tener una comprensión de los riesgos de las áreas de apoyo administrativo en cuanto al manejo de la información y sobre los requisitos específicos de seguridad de la información aplicables al hospital.
Profesional de Calidad	• Debe definir los lineamientos generales de procesos aplicables a las iniciativas de seguridad. • Tiene la responsabilidad de revisar el cumplimiento de los procesos de seguridad definidos en la institución. • Garantizar que las prácticas documentadas seguridad de la información son eficaces y se aplican.

Líder de estadística	• Compresión de los riesgos de la generación y disponibilidad de los informes que se deben entregar a los entes regulatorios.

Rol	Descripción
Líder de Sistemas	• Responsable de aplicar los controles y las iniciativas de seguridad de tipo tecnológico definidas en el comité.
Director de Gestión Humana	• Responsable de aplicar las iniciativas de seguridad concernientes a la vinculación, mantenimiento y retiro o cambio de personal.
Profesional de gestión documental	• Responsable de definir el manejo de la información a nivel documental que se maneja en toda la institución.
Director de Ayudas Diagnosticas	• Apoya la definición de lineamientos de seguridad para las áreas asistenciales aportando su conocimiento en pro de evitar en mayor medida los impactos operacionales. • Debe tener una comprensión de los riesgos de las áreas asistenciales en cuanto al manejo de la información y sobre los requisitos específicos de seguridad de la información aplicables al hospital.

9.1.1.2. RACI de prácticas del Comité de seguridad

Práctica	Nivel de participación (RACI)
Definir y comunicar una estrategia de seguridad de la información que está alineada con la estrategia de negocio.	Accountable
Investigar, definir y documentar los requisitos de seguridad de la información.	Accountable
Validar los requisitos de seguridad de la información con las partes interesadas y personal de implementación técnica.	Accountable
Desarrollar políticas y procedimientos de seguridad de la información.	Accountable
Desarrollar un plan de seguridad de la información que identifique las actividades a ser implementadas por el equipo de seguridad para proteger los activos de la organización de seguridad de información.	Accountable
Asegúrese de que el impacto potencial de los cambios se evalúa.	¬countable
Recopilar y analizar los datos de rendimiento y de cumplimiento relacionados con la seguridad de la información y la gestión de riesgos de la información.	Accountable
Establecer, acordar y comunicar el rol del CISO y los ISM.	Responsible

9.1.1.3. Competencias de rol

Habilidades

- Establecer y mantener un marco de gobierno de la seguridad de la información y procesos de apoyo para asegurar que la estrategia de seguridad de la información está alineada con las metas y objetivos de la organización.
- Definir e implementar la visión, misión y objetivos de seguridad de la información alineados con la estrategia y cultura corporativa.

Experiencia

Varios años de gestión empresarial, incluyendo experiencia en:

- Definición y seguimiento de lineamientos de seguridad de la información.
- Alinear la estrategia de seguridad de la información con el gobierno corporativo.
- Creación de políticas de seguridad de la información que se alinean con las necesidades del negocio y los métodos para medir la elaboración.
- Comunicación con liderazgo ejecutivo.
- Experiencia en la creación e implementación de estrategias y principios de seguridad de información.

9.1.2. Oficial de seguridad CISO

Objetivo	Tiene la responsabilidad general del programa de seguridad de la información empresarial.
Principios de operación	El CISO debería ser el enlace entre la junta directiva y los administradores de seguridad. El CISO también debe comunicasre y coordinar las relaciones con los actores clave del negocio para hacer frente a las necesidades de protección de la información. El CISO debe: • Tener una comprensión exacta de la visión estratégica de negocios. • Ser un comunicador eficaz. • Ser hábil en la construcción de relaciones efectivas con los líderes empresariales. • Ser capaz de traducir los objetivos de negocio a los requisitos de seguridad de la información.

Responsabilidades	• Establecer y mantener el sistema de gestión de seguridad de la información (SGSI). • Definir y gestionar un plan de tratamiento de riesgos de seguridad de información. • Hacer seguimiento y revisión del SGSI

9.1.2.1. RACI de prácticas de Oficial de seguridad

Práctica	Nivel de participación (RACI)
Identificar y comunicar las amenazas de seguridad de la información, las conductas deseables y los cambios necesarios para hacer frente a estos puntos.	Accountable
Tomar decisiones sobre la protección contra malware.	Accountable
Administrar la red y la seguridad de la conectividad.	Accountable
Administrar la seguridad del punto final.	Accountable
Gestione la identidad del usuario y de acceso lógico.	Accountable
Administrar el acceso físico a los activos de TI.	Accountable
Monitorear la infraestructura para eventos relacionados con la seguridad.	Accountable
Proporcionar formas de mejorar la eficiencia y eficacia de la función de seguridad de la información (por ejemplo, mediante la capacitación del personal de seguridad de la información; documentación de los procesos, la tecnología y las aplicaciones, y la estandarización y la automatización de procesos).	Accountable
Desarrollar un plan de seguridad de la información que identifique las actividades a ser implementadas por el equipo de seguridad para proteger los activos de la organización de seguridad de información.	Responsible
Supervisar la gestión de riesgos de TI.	Responsible
Definir y comunicar una estrategia de seguridad de la información que está en línea con la estrategia de negocio.	Responsible
Investigar, definir y documentar los requisitos de seguridad de la información.	Responsible
Validar los requisitos de seguridad de la información con las partes interesadas y personal de implementación técnica.	Responsible
Desarrollar políticas y procedimientos de seguridad de la información.	Responsible
Definir e implementar estrategias de evaluación de riesgos y cooperar con la oficina de riesgos para gestionar el riesgo de la información.	Responsible
Asegúrese de que el impacto potencial de los cambios frente a la seguridad de la información se evalúa.	Responsible

Recopilar y analizar los datos de rendimiento y de cumplimiento relacionados con la seguridad de la información y la gestión de riesgos de la información.	Responsible

9.1.2.2. Competencias de rol

Habilidades

- Gestionar adecuadamente los riesgos de la información.
- Administrar los recursos del programa de seguridad manera responsable.
- Crear un modelo de medición del desempeño basado en los indicadores de gobernabilidad de seguridad de la información para asegurar que se logran los objetivos organizacionales.
- Desarrollar un modelo de negocio que justifique las inversiones en seguridad de la información.
- Líder probado con excelentes habilidades de comunicación y capacidad de interactuar con todos los niveles de la empresa.
- Método de trabajo con orientación de procesos.
- Comprensión sobre como las funciones de seguridad de la información se relacionan con el negocio.

Experiencia

Varios años de experiencia en seguridad de la información, incluyendo experiencia en:

- Cumplimiento de la seguridad de la información con las regulaciones externas.
- Alinear la estrategia de seguridad de la información con el gobierno corporativo.
- Creación de políticas de seguridad de la información que se alinean con las necesidades del negocio y eficacia de las políticas.
- Comunicación y liderazgo ejecutivo.

Conocimiento

- Los requisitos legales y reglamentarios que afectan a la seguridad de información.
- Roles y responsabilidades necesarias para la seguridad de la información en toda la empresa.
- Métodos para poner en práctica las políticas de gobierno de seguridad de información.
- El buen entendimiento de las prácticas de seguridad de la información que se aplican a la institución.
- Los conceptos fundamentales de la gobernabilidad y cómo se relacionan con la seguridad de información.
- Normas, marcos y mejores prácticas relacionadas con la gobierno de la seguridad de información internacionalmente reconocidos y desarrollo de estrategias.

9.1.3. Administradores de seguridad de la información

Objetivo	La responsabilidad de la gestión de los esfuerzos de seguridad de la información, encargado de labores específicas de seguridad.
Principios de operación	• Reportar las actividades realizadas al CISO. • Desarrollar los planes de seguridad definidos.
Responsabilidades	• Gestionar la seguridad de la información de aplicaciones, infraestructura, accesos. • Identificar y ejecutar controles para los riesgos. • Llevar registro de métricas, y evaluaciones de seguridad.

9.1.3.1. RACI de prácticas de Administrador de seguridad

Práctica	Nivel de participación (RACI)
Desarrollar y comunicar una visión común para el equipo de seguridad de la información que está en consonancia con la declaración de la visión corporativa.	Responsible
Llevar a cabo las evaluaciones de riesgos de la información y definir el perfil de riesgo de la información.	Responsible
Administrar roles, responsabilidades, privilegios de acceso y niveles de autoridad.	Responsible
Desarrollar un plan de seguridad de la información y los controles para ser implementado en nuevos proyectos, para proteger los activos de la organización.	Responsible
Monitorear los controles internos y ajustarlos o mejorarlos cuando sea necesario.	Responsible
Proporcionar formas de mejorar la eficiencia y eficacia de la función de seguridad de la información (por ejemplo, mediante la capacitación del personal de seguridad de la información; documentación de los procesos, la tecnología y las aplicaciones, y la estandarización y la automatización del proceso).	Responsible
Recopilar y analizar los datos de rendimiento y de cumplimiento relacionados con la seguridad de la información y la gestión de riesgos de la información.	Responsible

Habilidades

- Capacidad para incluir en la arquitectura de TI los diseños de seguridad

(como las tecnologías interactúan con las políticas de seguridad).

- Habilidades para la gestión de proyectos.
- Habilidad para resolver problemas.
- Habilidades de comunicación y facilitación fuertes.
- Habilidades de gestión del tiempo fuerte.

Experiencia

Varios años de experiencia en seguridad de la información, incluyendo:

- Experiencia de trabajo en los sistemas de hardware y software, incluyendo SO, bases de datos, aplicaciones y redes.
- Comprensión técnica de cómo diversos sistemas de interconexión entre sí.

Conocimiento

- El buen entendimiento del protocolo de red, bases de datos, aplicaciones y sistemas operativos, y la forma en que son aplicables a los procesos de negocio.
- Amplio conocimiento de gestión de accesos, gestión de amenazas y vulnerabilidad, arquitectura de seguridad de la información y protección de datos en cada plataforma.
- Estándares de la industria de seguridad de la Información / mejores prácticas (por ejemplo, la norma ISO / IEC 27000 serie, ISF, NIST, PCI).
- Legislación relacionada con la seguridad de información.
- Nuevas tecnologías de seguridad de la información y metodologías de desarrollo.
- Detectar, investigar, responder y recuperarse de incidentes de seguridad de la información para reducir al mínimo impacto en el negocio.
- Realizar tareas de aprovisionamiento de usuario para sistemas empresariales y entornos de aplicaciones.
- Asistir en la definición de roles y modelos de acceso para diferentes aplicaciones y entornos de plataforma.
- Plataformas de vigilancia y mantenimiento de tecnología.

9.1.4. Líderes de proceso

Los líderes de proceso actúan como enlace entre las funciones empresariales y de seguridad de la información. Pueden estar asociados con tipos de información, aplicaciones específicas, o unidades de negocio de la organización. La persona en este rol debe poseer un buen conocimiento de la empresa y del tipo de información que requiere protección del proceso que representa. Los custodios sirven como asesores y agentes de supervisión con respecto a la información dentro de la empresa.

Este papel debe equilibrar el impacto de los riesgos del negocio y la información para que las decisiones de seguridad estén alienadas con las del negocio.

RACI de prácticas de Custodios de información

Práctica	Nivel de participación (RACI)
Comunicar, coordinar y asesorar sobre los esfuerzos de gestión de riesgos de la información con los gerentes de línea.	Responsible
Informar sobre los cambios en los procesos y/o estrategias (por ejemplo, nuevos productos o servicios) a la ISSC.	Responsible

Habilidades

- Gestionar adecuadamente los riesgos de la información.
- Líder probado con excelentes habilidades de comunicación y capacidad de interactuar con todos los niveles de la empresa.
- Método de trabajo con orientación de procesos.
- Comprensión sobre como las funciones de seguridad de la información se relacionan con el negocio.

Experiencia

- Cumplimiento de la seguridad de la información con las regulaciones externas.
- Comunicación y liderazgo ejecutivo.

Conocimiento

- Los requisitos legales y reglamentarios que afectan a la seguridad de información en su área de desempeño.
- Métodos para poner en práctica las políticas de gobierno de seguridad de información.
- El buen entendimiento de las prácticas de seguridad de la información que se aplican a la institución.

92. Objetivos de seguridad

El gobierno de seguridad tiene unos objetivos de seguridad primordiales los cuales rigen sus decisiones. Todos los lineamientos de seguridad establecidos para el HOSPITAL NAZARETH están orientados a cumplir con los siguientes objetivos:

- Alinear las iniciativas de seguridad de la información con la estrategia de negocio y dar cumplimiento con las regulaciones internas y externas aplicables.

- Mitigar los riesgos de negocio relacionados con problemas en la seguridad de la información.

- Asegurar en una medida razonable la confidencialidad, integridad y disponibilidad de la información asistencial e interna relevante para la toma de decisiones en el Hospital.

10. COMUNICACIÓN CON EL COMITÉ DE GOBIERNO DE INFORMACIÓN

Para que el comité de gobierno pueda cumplir con sus actividades y tomar las decisiones pertinentes según los acontecimientos en la institución, se debe llevar la información necesaria. Dentro de la agenda de reunión el comité debe recibir la siguiente información como mínimo:

- El estado de las acciones de las revisiones previas:
  - Seguimiento de las decisiones o actividades asignadas por el comité.
  - Solicitudes al comité para lograr el cumplimiento de las actividades designadas.
  - Resultados de las acciones finalmente implementadas.
- Cambios externos e internos que son relevantes para el sistema de gestión de seguridad de la información:
  - Cambios en regulaciones.
  - Cambios en ambiente físico y social.
  - Cambios de herramientas o infraestructura que soporta los procesos.
- Retroalimentación sobre el desempeño de la seguridad de la información, incluyendo las tendencias en:
  - Estado de los hallazgos de auditoría, las no conformidades y acciones correctivas.
  - Seguimiento y medición de las actividades de seguridad desarrolladas.
- Retroalimentación de las partes interesadas:
  - Resultados de encuestas de satisfacción de los cambios implementados.
- Resultados de la evaluación del riesgo y el estado del plan de tratamiento de riesgos.
- Las oportunidades o propuesta de mejora en temas relacionados con la seguridad de la información.

Las decisiones tomadas por el comité quedarán documentadas en la correspondiente acta de reunión, dentro de la cual para cada una de las decisiones tomadas se establecerá el responsable.

Las actas de comité deben incluir las decisiones relacionadas con las oportunidades de mejora continua y de cualquier necesidad de cambios en el

sistema de gestión de seguridad de la información.

11. LINEAMIENTOS DE SEGURIDAD

11.1. Gestión de activos

- Las diferentes áreas con el fin de garantizar la administración y control sobre los activos de la entidad, deben mantener un inventario actualizado de los activos que se encuentran dentro del alcance del modelo de gestión de seguridad de la información y que están cargados a cada proceso, el cual debe estar alineado con el inventario general de activos de información.
- En el inventario se identificará el propietario del activo, quien debe asegurar que la información y los activos asociados con su proceso están clasificados de manera apropiada, así como de establecer controles necesarios para el acceso a éstos de acuerdo con los procedimientos definidos.

11.2. Uso aceptable de los activos

- La información, archivos físicos, los sistemas, los servicios y los equipos (estaciones de trabajo, portátiles, impresoras, redes, Internet, correo electrónico, herramientas de acceso remoto, aplicaciones, teléfonos y faxes, entre otros) propiedad del HOSPITAL NAZARETH, son activos de la Institución y se proporcionan a los funcionarios, contratistas y terceros autorizados, para cumplir con los propósitos del negocio.

- El HOSPITAL NAZARETH podrá monitorear, supervisar y utilizar su información, sistemas, servicios y equipos, de acuerdo con lo establecido en este plan y en cualquier proceso legal que se requiera.

- El acceso a los documentos físicos y digitales estará determinado por las normas relacionadas con el acceso y las restricciones a los documentos públicos, a la competencia del área o dependencia específica y a los permisos y niveles de acceso de los funcionarios, contratistas y terceros determinadas por los Líderes de área y Subgerentes.

- La consulta de expedientes o documentos que reposan en las diferentes oficinas y/o áreas del HOSPITAL NAZARETH se permitirá en días y horas laborales, con la presencia del funcionario o servidor responsable de aquellos.

- El funcionario y/o contratista se compromete a cumplir con los procedimientos establecidos para el servicio y consulta de documentos según lo definido en el proceso de ***Planificación y Consolidación del Sistema de Gestión Integral***

de Calidad y el área propietaria de la información.

- Para la consulta de documentos cargados en SAP se establecerán privilegios de acceso a los funcionarios, terceros y/contratistas de acuerdo con el desarrollo de sus funciones y competencias. Dichos privilegios serán establecidos por el Líder o Director del área, quien comunicará al grupo encargado de la administración del software el listado con los funcionarios y sus privilegios.

- El Líder o Director del área, serán quienes determinen el carácter de reserva o restricción de los documentos físicos. Todos los funcionarios y terceros que manipulen información en el desarrollo de sus funciones deberán firmar un "Acuerdo de Confidencialidad de la Información", donde individualmente se comprometan a no divulgar, usar o explotar la información confidencial a la que tengan acceso, respetando los lineamientos definidos en la Política de Información del HOSPITAL NAZARETH y los lineamientos del presente documento. En caso de violación de la información será considerado como un incidente de seguridad y se procederá de acuerdo a lo definido al tratamiento de este tipo de incidentes.

11.2.1. Acceso a Internet:

- No está permitido:

  - El acceso a páginas relacionadas con pornografía, drogas, alcohol, webproxys, hacking y /o cualquier otra página que vaya en contra de la ética moral, las leyes vigentes o políticas aquí establecidas.

  - El acceso y el uso de servicios interactivos o mensajería instantánea que tengan como objetivo crear comunidades para intercambiar información o bien para fines diferentes a las actividades propias del Hospital.

  - El Intercambio no autorizado de información de propiedad del Hospital, de sus clientes, usuarios y/o de sus funcionarios, con terceros.

  - La descarga, uso, intercambio y/o instalación de juegos, música, películas, protectores y fondos de pantalla, software de libre distribución, información y/o productos que de alguna forma atenten contra la propiedad intelectual de sus autores, o que contengan archivos ejecutables y/o herramientas que atenten contra la integridad, disponibilidad y/o confidencialidad de la infraestructura tecnológica (hacking), entre otros.

- La descarga, uso, intercambio y/o instalación de información audiovisual (videos e imágenes) utilizando sitios públicos en Internet debe ser autorizada por el Líder respectivo y el Líder de los estándares de Gerencia de la Información, o a quienes ellos deleguen de forma explícita para esta función, asociando los procedimientos y controles necesarios para el monitoreo y aseguramiento del buen uso del recurso.

- El hospital Nazareth de Quinchia realizar monitoreo permanente de tiempos de navegación y páginas visitadas por parte de los funcionarios, contratistas y/o terceros. Así mismo, puede inspeccionar, registrar y evaluar las actividades realizadas durante la navegación, de acuerdo a la legislación nacional vigente.

- Cada uno de los usuarios es responsable de dar un uso adecuado a este recurso y en ningún momento puede ser usado para realizar prácticas ilícitas o mal intencionadas que atenten contra terceros, la legislación vigente y los lineamientos de seguridad de la información, entre otros.

- Los funcionarios, contratistas y terceros, al igual que los empleados o subcontratistas de estos, no pueden asumir en nombre del Hospital, posiciones personales en encuestas de opinión, foros u otros medios de comunicación externos similares.

- El uso de Internet no considerado dentro de las restricciones anteriores, es permitido siempre y cuando se realice de manera ética, razonable, responsable, no abusiva y sin afectar la productividad ni la protección de la información del Hospital Nazareth de Quinchia.

11.2.2. Correo electrónico:

- El correo electrónico corporativo es una herramienta de comunicación o intercambio de información oficial entre personal o instituciones, no es una herramienta de difusión indiscriminada de información.

- La cuenta de correo electrónico debe ser usada para el desempeño de las funciones asignadas dentro del Hospital.

- Los mensajes y la información contenida en los buzones de correo son propiedad del Hospital Nazareth y cada usuario, como responsable de su buzón, debe mantener solamente los mensajes relacionados con el desarrollo de sus funciones.

- El tamaño de los buzones de correo es determinado por el área de Sistemas de la entidad de acuerdo con las necesidades de cada usuario y previa autorización del Jefe y/o Líder del área correspondiente.

- El tamaño de envío y recepción de mensajes, sus contenidos y demás características propios de estos deberán ser definidos e implementados por el área de Sistemas del Hospital Nazareth.

- El envío de información corporativa debe ser realizado exclusivamente desde la cuenta de correo que el Hospital Nazareth proporciona. De igual manera, las cuentas de correo genéricas no se deben emplear para uso personal dentro de la institución.

- El envío masivo de mensajes publicitarios corporativos deberá contar con la aprobación del área de Comunicaciones y la autorización del área de Sistemas del Hospital. Además, para terceros se deberá incluir un mensaje que le indique al destinatario como ser eliminado de la lista de distribución. Si una dependencia debe por alguna circunstancia, realizar envío de correo masivo, de manera frecuente, este debe ser enviado a través de una cuenta de correo electrónico a nombre del área respectiva y/o servicio habilitado para tal fin y no a través de cuenta de correo electrónico asignadas a un usuario particular.

- Toda información del HOSPITAL NAZARETH generada con los diferentes programas computacionales (Office, Project, Access, Wordpad, ect.), que requiera ser enviada fuera de la entidad, y que por sus características de confidencialidad e integridad deba ser protegida, debe estar en formatos no editables, utilizando las características de seguridad que brindan las herramientas proporcionadas por el área de Sistemas. La información puede ser enviada en el formato original bajo la responsabilidad del usuario y únicamente cuando el receptor requiera hacer modificaciones a dicha información.

- Todos los mensajes enviados deben respetar el estándar de formato e imagen corporativa definido por el Hospital Nazareth y deben conservar en todos los casos el mensaje legar corporativo de confidencialidad.

- Los archivos que se adjuntan en los mensajes de correo en lo posible deben comprimirse para evitar la saturación en las diferentes cuentas de correos.

- El usuario que tiene asignada una cuenta de correo electrónico es el único y directo responsable de todas las acciones y mensajes que se lleven a cabo en

su nombre, por lo tanto el Hospital no se hace responsable por lo que diga o haga. Esta información se incluirá en todos los mensajes que se envíen.

- Las únicas áreas de la institución autorizadas para enviar mensajes a través de la lista de correo denominada personal en la cual se incluyen todas las direcciones de correo del Hospital son: La Gerencia, Comunicaciones, Sistemas y Proyección Humana.

- El correo electrónico corporativo es la única vía de remisión o envío de documentos de carácter administrativo interno en el hospital.

- Se aplicarán además los parámetros para la utilización del correo electrónico del Hospital Nazareth de Quinchia dictados por el área de Comunicaciones.

No está permitido:

- Enviar cadenas de correo, mensajes con contenido religioso, político, racista, sexista, pornográfico, publicitario no corporativo o cualquier otro tipo de mensajes que atenten contra la dignidad y la productividad de las personas o el normal desempeño del servicio de correo electrónico en la Institución, mensajes mal intencionados que puedan afectar los sistemas internos o de terceros, mensajes que vayan en contra de las leyes, la moral y las buenas costumbres y mensajes que inciten a realizar prácticas ilícitas o promuevan actividades ilegales.

- Utilizar la dirección de correo electrónico del Hospital Nazareth punto de contacto en comunidades interactivas de contacto social, tales como Facebook, Instagram, entre otras, o cualquier otro sitio que no tenga que ver con las actividades laborales.

- El envío de archivos que contengan extensiones ejecutables, bajo ninguna circunstancia.

- El envío de archivos de música y videos. En caso de requerir hacer un envío de este tipo de archivos deberá ser autorizado por la dirección respectiva y las áreas de Sistemas y Comunicaciones del Hospital Nazareth.

11.2.3. Recursos tecnológicos:

- La instalación de cualquier tipo de software o hardware en los equipos de cómputo del Hospital Nazareth es responsabilidad del área de Sistemas, y por tanto son los únicos autorizados para realizar esta labor. Así mismo, los medios

de

instalación de software deben ser los proporcionados por el Hospital Nazareth a través de esta área.

- Los usuarios no deben realizar cambios en las estaciones de trabajo relacionados con la configuración del equipo, tales como conexiones de red, usuarios locales de la máquina, papel tapiz y protector de pantalla corporativo, entre otros. Estos cambios son realizados únicamente por el área de Sistemas.

- El área de Sistemas del Hospital Nazareth definirá y actualizará, de manera periódica, la lista de software y aplicaciones de trabajo de los usuarios. Así mismo, realizar el control y verificación de cumplimiento del licenciamiento del respectivo software y aplicaciones instaladas y administradas por el Hospital.

- Los funcionarios serán conectados a la red del con previa solicitud Hospital Nazareth escrita y autorizada por el Líder del área. Los terceros y/o contratistas se conectarán a la red del Hospital Nazareth, bajo los lineamientos del área de Sistemas, asegurando la legalidad del equipo a través de certificados emitidos por la empresa contratista, de acuerdo a lo definido por el área de sistemas.

- Los usuarios que requieren acceder a la infraestructura tecnológica del Hospital Nazareth desde redes externas, deben utilizar una conexión bajo los esquemas y herramientas de seguridad autorizados y establecidos por el área de Sistemas. Además, deberán informar previamente a la misma área para autorizar el acceso y brindar los permisos respectivos para la protección de la información, de acuerdo a lo definido por el área de sistemas.

- La sincronización de dispositivos móviles, tales como PDAs, Smartphone, celulares u otros dispositivos electrónicos sobre los que se puedan realizar intercambios de información con cualquier recurso de la Organización, debe ser autorizado de forma explícita por el líder de la dependencia respectiva, en conjunto con el apoyo del área de Sistemas del Hospital Nazareth

- El Hospital Nazareth brindará el servicio de Internet a los usuarios que accedan a uno de los servicios de salud del Hospital (usuarios y/o acompañante), estipulados en la ES-GIC-AU001D01 Guía de Información y Orientación al Usuario**,** con previo aviso al área de Sistemas**.**

- Las estaciones de trabajo y en general cualquier recurso de la organización no debe ser empleado para actividades recreativas, entre otras, jugar o grabar música.

- Ningún funcionario, contratista o tercero podrá copiar para uso personal archivos o programas de propios del Hospital.

11.3. Acuerdos sobre confidencialidad

- Todos los funcionarios, colaboradores y/o terceros que presten sus servicios al Hospital Nazareth deberán aceptar los acuerdos de confidencialidad definidos por la institución, los cuales reflejan los compromisos de protección y buen uso de la información de acuerdo con los criterios establecidos en ella.

- Para los contratistas, los respectivos contratos deben incluir una cláusula de confidencialidad, de igual manera cuando se permita el acceso a la información y/o a los recursos del Hospital Nazareth a personas o entidades externas.

- Estos acuerdos deben aceptarse por cada uno de ellos como parte del proceso de contratación, razón por la cual dicha cláusula y/o acuerdo de confidencialidad hace parte integral de cada uno de los contratos.

11.4. Partes externas

- El Hospital Nazareth identifica los posibles riesgos que pueden generar el acceso, procesamiento, comunicación o gestión de la información y la infraestructura para su procesamiento por parte de los terceros, con el fin de establecer los mecanismos de control necesarios para que la seguridad se mantenga.

- Los controles que se establezcan como necesarios a partir del análisis de riesgos deben ser comunicados y aceptados por el tercero mediante la firma de acuerdos, previamente a la entrega de los accesos requeridos.

11.5. Clasificación de la información

- El Hospital Nazareth con el fin de resguardar la información que pueda ser divulgada de forma no autorizada o manipulada erróneamente por parte de sus funcionarios, contratistas, proveedores o clientes, ha establecido niveles para la clasificación de la información, incluyendo la información que puede encontrarse en medio electrónico, impreso, verbal o que sea transmitida por cualquier medio.

- Toda la información del Hospital Nazareth debe ser identificada, clasificada y documentada de acuerdo con los criterios de clasificación establecidos por el Comité de gerencia de la información.

- Los niveles de clasificación de la información definidos en el Hospital Nazareth

    - EXTERNA
    - CATEGORÍA PÚBLICA
    - PÚBLICA USO INTERNO
    - PÚBLICA CLASIFICADA
    - PÚBLICA RESERVADA

- Los criterios, niveles de clasificación y aplicación se encuentran detallados en los Lineamientos de Inventario del Documento AP-INF-TI001D01 Inventario Consolidado de TI y el ***Documento de Clasificación de Activos de Información*** y estos son revisados y aprobados de manera periódica por el Comité de Seguridad de la Información Hospital Nazareth

- Los propietarios de los activos de información son los responsables de identificar y asociar el nivel de clasificación a cada activo, teniendo en cuenta los criterios de clasificación, y su protección se establece de acuerdo con lo definido en el inventario de activos de información del Hospital Nazareth.

11.6. Seguridad de los recursos humanos

- Todos los funcionarios del Hospital Nazareth, contratistas y terceros que tengan la posibilidad de acceder a la información de la organización y a la infraestructura para su procesamiento, son responsables de conocer y cumplir con las políticas y procedimientos establecidos en el Modelo de Gestión de Seguridad de la Información del Hospital Nazareth de igual forma, son responsables de reportar por medio de los canales apropiados, el incumplimiento de las políticas y procedimientos establecidos.

- Todos los funcionarios del Hospital Nazareth deben ser cuidadosos de no divulgar información confidencial en lugares públicos, en conversaciones o situaciones que pongan en riesgo la seguridad y el buen nombre de la organización.

- Todos los funcionarios del Hospital Nazareth deben hacer buen uso de la escarapela que los acredita como sus servidores, este documento debe ser devuelto al Hospital Nazareth en el momento de desvinculación.

9.6.1. Roles y responsabilidades

- El área de Gestión Humana será la encargada de diseñar, documentar y actualizar el manual AP-GHU-AP001M01 de funciones y competencias del Hospital Nazareth, donde se detallan los roles, las responsabilidades y funciones a ser ejecutadas durante el desarrollo de las actividades en la Institución. Para los contratistas y terceros se describirán las responsabilidades en los contratos respectivos que intervienen con el Hospital.

9.6.2. Selección de personal

- Toda vinculación laboral realizada por el Hospital Nazareth se rige por las leyes de la República de Colombia y por dispuesto en el Código Sustantivo del Trabajo.

- Todo funcionario contratado por el Hospital Nazarethes seleccionado adecuadamente, de acuerdo con los requerimientos de cada cargo y siguiendo las tareas descritas en el AP-GHU-AP002 Procedimiento Selección de Funcionarios y Colaboradores**.** En caso que el proceso de selección o la contratación se realice por intermedio de terceros, el Hospital Nazareth debe asegurar la definición clara de las responsabilidades y los mecanismos para manejar el incumplimiento de los requisitos. Sin importar el método de contratación, todo funcionario recibe y acepta las políticas de seguridad de la Institución.

- El Hospital Nazareth verifica la información brindada durante el proceso de vinculación de los funcionarios; de igual forma, de acuerdo a lo dispuesto en el AP-GHU- AP002 Procedimiento Selección de Funcionarios y Colaboradores, se realiza estudio de seguridad a todos los candidatos a cargos de la Institución.

9.6.3. Términos y condiciones laborales

- Todos los funcionarios y aquellos terceros definidos por el Hospital Nazareth, deben acorde a las políticas de Seguridad de la Información, así como los términos de uso adecuado de los recursos de información que le son

entregados, que éstos son extensibles fuera de la Institución.

- Todos los funcionarios y aquellos terceros que tengan acceso a información sensible de la Institución o a la Infraestructura Tecnológica que contenga este

tipo de información, deben firmar, previamente a la entrega del acceso, un acuerdo de confidencialidad y no divulgación, en el que se especifique el período por el cual debe mantener el acuerdo y las acciones que se toman cuando se incumpla este requerimiento.

- Adicionalmente, con funcionarios y terceros deben quedar establecidos en aspectos como propiedad intelectual, protección de la información y leyes aplicables.

9.6.4. Educación, formación y concientización sobre la Seguridad de la Información

- El Hospital Nazareth debe asegurar que todos los funcionarios que tengan definidas responsabilidades en de Seguridad de la Información son competentes para desempeñar sus funciones y que cuentan con los programas de capacitación y entrenamiento requeridos para ello.

- De igual forma, todos los funcionarios y, cuando sea relevante, los terceros tendrán un proceso formal de concientización, mediante el cual se capacitará sobre las políticas de seguridad de la Institución y los riesgos conocidos a los que se puede ver expuesta, en caso que estas no se cumplan.

- Los programas de concientización, educación y entrenamiento se encuentran diseñados de manera apropiada y relevante para los roles, responsabilidades y habilidades de las personas que deben asistir a ellos.

9.6.5. Proceso disciplinario

- En el caso de identificarse un incidente de seguridad, éste será registrado en la herramienta de gestión designada, y se hará la investigación respectiva para determinar las causas y responsables posteriormente, el Hospital Nazareth tomará las acciones pertinentes para el funcionario y/o tercero vinculado con el incidente, mediante un proceso disciplinario formal de acuerdo con la naturaleza, gravedad y/o el impacto que haya podido generar a la organización dicho incidente de acuerdo a los procedimientos del proceso Gestión Disciplinaria: Procedimiento AP-GHU-DI001 Recepción y Evaluación de Noticia Disciplinaria, Procedimiento AP-GHU-DI002 Indagación Preliminar y Procedimiento AP- GHU-DI003 Investigación Disciplinaria.

9.6.6. Terminación o cambio de la contratación laboral

- La Subgerencia de Procesos Administrativos y Financieros y/o Subgerencia de Procesos Asistenciales, será la encargada de informar a las áreas implicadas en los procesos de vinculación y desvinculación, los movimientos del personal según los lineamientos establecidos en el Hospital.

9.6.7. Responsabilidades en la terminación o cambio de funciones.

- La Subgerencia de Procesos Administrativos y Financieros y/o Subgerencia de Procesos Asistenciales, en conjunto con el jefe directo del funcionario y/o responsable del tercero, son los encargados del proceso de terminación de labores y asegurar que todos los activos propios de la organización sean devueltos, los accesos físicos y lógicos sean eliminados, y la información pertinente sea transferida, de acuerdo con los procedimientos establecidos en el proceso de “Retiro”.

- En caso que un funcionario y/o tercero tenga un cambio de funciones, se debe seguir los mismos procedimientos donde se asegure la entrega de activos, el retiro de los accesos físicos y lógicos, la transferencia de información y la posterior entrega de los mismos de acuerdo a su rol.

9.6.8. Devolución de Activos.

- Todo funcionario al momento de su retiro o cambio de funciones en la institución debe hacer entrega a su jefe inmediato del equipo que se le había asignado, con toda la información contenida en él y una relación de la misma.

9.7. Seguridad física y del entorno

- El Hospital Nazareth será el responsable de definir el perímetro de la seguridad física de acuerdo a la clasificación de los activos de la información, controlando el acceso a la información a través de controles (Ejemplo: acceso a áreas restringidas con tarjeta, registro de entrada de equipos, autenticación), los cuales disminuyen la posibilidad de riesgo de divulgación o pérdida de información.

9.7.1. Controles de Acceso Físico

- Todas las áreas destinadas al procesamiento o almacenamiento de información sensible, así como aquellas en las que se encuentren los equipos y demás infraestructura de soporte a los sistemas de información y comunicaciones, se consideran área de acceso restringido. En consecuencia, deben contar con medidas de control de acceso físico en el perímetro tales que puedan ser auditadas, así como con procedimientos de seguridad operacionales que permitan proteger la información, el software y el hardware de daños intencionales o accidentales.

- De igual forma, los centros de cómputo, cableado y cuartos técnicos de las oficinas deben contar con mecanismos que permitan garantizar que se cumplen los requerimientos ambientales (temperatura, humedad, etc.), especificados por los fabricantes de los equipos que albergan y que pueden responder de manera adecuada ante incidentes como incendios e inundaciones.

- Las áreas de carga, descarga, entrega de mercancías y demás puntos de acceso a las instalaciones del Hospital Nazareth, deben ser controladas y en lo posible separadas de las áreas seguras para evitar el acceso no autorizado a estas últimas.

- Los funcionarios, contratistas y terceros del Hospital Nazareth, así como los visitantes, deben portar su identificación y/o escarapela de manera visible durante el tiempo que permanezca dentro de las instalaciones de la organización.

- Los privilegios de acceso a las áreas seguras y restringidas del HOSPITAL NAZARETH deben ser periódicamente revisados, actualizados y monitoreados.

- En caso de retiro o desvinculación laboral del funcionario, contratistas y/o tercero, éste debe hacer devolución de la respectiva escarapela asignada en desarrollo de sus funciones, previa liquidación de sus prestaciones sociales y demás obligaciones.

9.7.2. Protección y ubicación de los equipos

- Los equipos que hacen parte de la Infraestructura tecnológica del Hospital Nazareth tales como servidores, equipos de comunicaciones y seguridad electrónica, centros de cableado, UPS, subestaciones eléctricas, aires acondicionados, plantas

telefónicas, así como estaciones de trabajo y dispositivos de almacenamiento y/o comunicación móvil que contengan o brinden servicios de soporte a la información crítica de las áreas, deben ser ubicados y protegidos adecuadamente para prevenir la pérdida, daño, robo o acceso no autorizado de los mismos. De igual manera, se debe adoptar los controles necesarios para mantener los equipos alejados de sitios que puedan tener riesgo de amenazas potenciales como fuego, explosivos, agua, polvo, vibración, interferencia electromagnética y vandalismo, entre otros.

- Los funcionarios y terceros, incluyendo sus empleados o subcontratistas, que tengan acceso a los equipos que componen la infraestructura tecnológica del Hospital Nazareth no pueden fumar, beber o consumir algún tipo de alimento cerca de los equipos.

- Cualquier traslado de equipos de cómputo se realizará con la coordinación del área de Sistemas previa verificación de las condiciones técnicas y de seguridad.

- Toda persona que note algún problema de funcionamiento o ataque de virus en una estación de trabajo debe reportarlo de inmediato al personal de soporte técnico del Departamento de Sistemas mediante el uso de los canales de comunicación definidos para ello.

- El Hospital Nazareth mediante mecanismos adecuados monitoreará las condiciones ambientales de las zonas donde se encuentren los equipos.

- El Hospital Nazareth debe proveer suministros y equipamiento de soporte como electricidad, aire acondicionado, planta eléctrica y un sistema de alimentación no interrumpida (UPS) que asegure el tiempo necesario para apagar adecuadamente los servidores donde se alojan los sistemas de información ante una falla en el suministro de cualquiera de estos elementos, evitando así la pérdida o corrupción de información. Estos suministros deben ser monitoreados, revisados y medidos permanentemente para asegurar su funcionamiento y condiciones normales de operación y evitar futuros daños.

- De igual manera, el Hospital Nazareth debe establecer un programa de planeación y ejecución de mantenimientos preventivos anuales (como mínimo), a la infraestructura tecnológica.

- Ningún empelado, contratista o tercero podrá desarmar o destapar equipos sin la autorización previa del Departamento de Sistemas.

9.7.3. Seguridad de los equipos y medios de información fuera de las instalaciones

- Independientemente del propietario, todos los funcionarios son responsables de velar por la seguridad de los equipos del Hospital Nazareth que se encuentren fuera de las instalaciones de la organización.

- Bajo ninguna circunstancia los equipos de cómputo pueden ser dejados desatendidos en lugares públicos o a la vista, en el caso que esté siendo transportado en un vehículo.

- Los equipos de infraestructura del Hospital Nazareth deben ser transportados con las medidas de seguridad apropiadas, que garanticen la integridad física de los dispositivos.

- Los equipos portátiles siempre deben ser llevados como equipaje de mano y se debe tener especial cuidado de no exponerlos a fuertes campos electromagnéticos.

- Los equipos del Hospital Nazareth deberán contar con un seguro que los proteja de robo.

- En caso de pérdida o robo de un equipo del Hospital Nazareth se deberá informar inmediatamente al Líder del Proceso para que se inicie el trámite interno y se deberá poner la denuncia ante la autoridad competente.

- El retiro de equipos de cómputo, periféricos, dispositivos de almacenamientos, software e información considerada crítica propiedad de Hospital Nazareth, fuera de las instalaciones de la organización debe seguir los procedimientos establecidos por la Subgerencia de Procesos Administrativos y Financieros y el área de Sistemas del Hospital Nazareth.

9.7.4. Eliminación o reutilización segura de equipos y medios

- El Hospital Nazareth debe identificar los riesgos potenciales que puede generar destruir, reparar o eliminar equipos y medios de almacenamiento. Para ello, debe definir e implementar los mecanismos y controles adecuados para que la información sensible contenida en ellos sea eliminada de manera segura.

- Cuando un equipo sea reasignado o dado de baja, se deberá realizar el

proceso de acuerdo al procedimiento establecido AP-GRF-AF003 baja de

Inventarios y de acuerdo a la actividad 6.8 del Instructivo AP-INF-TI003I05 Gestión de Activos de TI.

9.8. Gestión de comunicaciones y operaciones

9.7.1. Documentación de procedimientos operativos

- Se debe contar con procedimientos, registros e instructivos de trabajo debidamente documentados y actualizados, con el fin de asegurar el mantenimiento y operación adecuada de la infraestructura tecnológica del Hospital Nazareth. Cada procedimiento debe tener un responsable para su definición y mantenimiento y debe garantizar la disponibilidad del mismo.

9.7.2. Control de Cambios

- Todo cambio que se realice sobre la infraestructura tecnológica para el procesamiento de la información, comunicaciones y seguridad electrónica debe ser controlado, gestionado y autorizado adecuadamente, y debe ser sometido a una evaluación que permita identificar los riesgos asociados que pueden afectar la operación del negocio de acuerdo con los lineamientos establecidos en el Instructivo AP-INF-TI004I01 Gestión de Cambios.

- Los cambios estructurales que se planteen realizar sobre las plataformas críticas deben ser revisados por el Comité de Seguridad de la Información, el cual debe establecer los requerimientos de seguridad necesarios conforme a las políticas establecidas por el Hospital Nazareth, que tengan como fin evitar un impacto adverso en las operaciones del negocio.

- La Gestión de Cambios debe contener como mínimo la identificación, justificación y evidencia de los cambios que se vayan a realizar sobre la infraestructura tecnológica, el alcance, autorización, el plan de trabajo para la definición de pruebas funcionales, responsabilidades definidas, la evaluación apropiada sobre el impacto potencial que estos pueden generar, un plan alternativo para abortar cambios no satisfactorios (Rollback), eventos imprevistos y cualquier otro aspecto que se considere importante por los responsables del cambio, todo ello deberá estar registrado en los Formatos AP-INF-TI004F04 Requerimiento de Cambio de TI y el AP-INF-TI004F01 Control De Cambios.

9.7.3. Segregación de funciones

- Toda tarea en la cual sus funcionarios tengan acceso a la infraestructura tecnológica y a los sistemas de información, debe contar con una definición clara de los roles y responsabilidades, así como del nivel de acceso y los privilegios correspondientes, con el fin de reducir y evitar el uso no autorizado o modificación sobre los activos de información de la organización.

- Todos los sistemas de disponibilidad crítica o media de la Institución, en lo posible, deben implementar las reglas de acceso de tal forma que haya segregación de funciones entre quien administre, opere, mantenga, audite y en general, tenga la posibilidad de acceder a los sistemas de información, así como entre quien otorga el privilegio y quien lo utiliza.

- Los módulos ejecutables nunca deberán ser trasladados directamente de las librerías de pruebas a las librerías de producción sin que previamente sean compilados por el área asignada para tal efecto.

- El nivel de súper usuario de los sistemas debe tener un control dual, de tal forma que exista una supervisión de las actividades realizadas por el administrador del sistema.

- Deben estas claramente segregadas, en lo posible, las funciones de soporte técnicos, planificadores y operadores.

9.7.4. Separación de los ambientes de desarrollo, prueba y producción

- El Hospital Nazareth ha definido diferentes ambientes para la ejecución de actividades de desarrollo, pruebas y puesta en producción de sus aplicaciones de negocio, con el fin de garantizar la integridad de la información procesada y evitar interferencias en el desempeño y seguridad de cada uno de los ambientes.

- Dado lo anterior, los ambientes establecidos por el Hospital Nazareth se definen así:

    - **Ambiente de Desarrollo:** Conjunto de elementos de hardware y software como compiladores, editores, instaladores de lenguajes de programación, donde residen todos los recursos informáticos necesarios para efectuar tareas relacionadas con la generación o modificación de aplicaciones, entre otros.

    - **Ambiente de Pruebas:** Conjunto de elementos de hardware y software

que soportan los sistemas de información utilizados para verificar la funcionalidad de los desarrollos de software y aplicativos para realizar los

ajustes necesarios antes de ser puestos en funcionamiento en el ambiente de producción del Hospital Nazareth.

- **Ambiente de Producción:** Conjunto de elementos de hardware y software que soportan los sistemas de información utilizados por los funcionarios para la ejecución de las operaciones del Hospital Nazareth. En este ambiente deben residir aplicaciones en producción, bibliotecas o directorios que contengan archivos de datos, base de datos, programas ejecutables o compilados.

- A través de las políticas de control de acceso físico y lógico definidas por la Institución, se controla el acceso a cada uno de los ambientes. Adicionalmente, los ambientes de desarrollo, pruebas y producción están totalmente separados, contando cada uno con su plataforma, servidores, aplicaciones, dispositivos y versiones independientes de los otros dos ambientes, evitando que las actividades de desarrollo y pruebas puedan poner en riesgo la integridad de la información de producción.

- El área de Sistemas debe proveer los mecanismos, controles y recursos necesarios para tener niveles adecuados de separación física y lógica entre los ambientes de desarrollo, pruebas y producción para toda su plataforma tecnológica, con el fin de reducir el acceso no autorizado y evitar cambios inadecuados.

- Igualmente debe asegurar, mediante los controles adecuados, que los usuarios utilicen diferentes perfiles para el ambiente de desarrollo, pruebas y de producción, así mismo que los menús muestren los mensajes de identificación apropiados para reducir los riesgos de error.

9.7.5. Gestión de la capacidad

- El Hospital Nazareth mantendrá un proceso continuo de monitoreo, análisis y evaluación del rendimiento y capacidad de su infraestructura tecnológica de procesamiento de información, con el fin de identificar y controlar el consumo de sus recursos y prever su crecimiento de forma planificada.

- Periódicamente, se realizarán mediciones de las variables críticas de operación de la infraestructura tecnológica con el objetivo de verificar el estado y uso de los recursos. De esta forma, es posible definir proyecciones de crecimiento que aseguren la integridad de procesamiento y disponibilidad de la infraestructura.

- Los resultados de dichas mediciones serán analizados y presentados al Comité de Seguridad de la Información y en caso de ser necesario la adquisición de nuevos recursos o elementos para soportar la demanda, se proceda a planificar la consecución de dichos elementos previa autorización de la alta dirección.

9.7.6. Aceptación de sistemas

- El área de Sistemas debe asegurar que los requerimientos y criterios, tanto funcionales como técnicos, para la aceptación de nuevos sistemas, actualizaciones y nuevas versiones de software estén claras y adecuadamente definidos, documentados y aprobados acordes a las necesidades del Hospital Nazareth. Estos nuevos requerimientos, actualizaciones y/o nuevas versiones de tecnología, sólo deben ser migrados al ambiente de producción después de haber sido formalmente aceptados de acuerdo a las necesidades técnicas y funcionales establecidas en el Instructivo AP-INF-TI004I01 Gestión de Cambios.

- Todo sistema que se implemente o instale en el Hospital Nazareth, sea comprado o en comodato, debe tener la capacidad de integrarse al sistema corporativo y será evaluado por el área de Sistemas para verificar su buen funcionamiento y los procedimientos de mantenimiento y soporte de la solución.

9.7.7. Protección contra software malicioso

- El Hospital Nazareth establece que todos los recursos informáticos deben estar protegidos mediante herramientas y software de seguridad como antivirus, anti spam, antispyware y otras aplicaciones que brindan protección contra código malicioso y prevención del ingreso del mismo a la red institucional, en donde se cuente con los controles adecuados para detectar, prevenir y recuperar posibles fallos causados por código móvil y malicioso. Será responsabilidad del área de Sistemas autorizar el uso de las herramientas y asegurar que estas y el software de seguridad no sean deshabilitados bajo ninguna circunstancia, así como de su actualización permanente.

- Así mismo, el Hospital Nazareth define que no está permitido:

    - La desinstalación y/o desactivación de software y herramientas de

seguridad avaladas previamente por el Hospital Nazareth.

- Escribir, generar, compilar, copiar, propagar, ejecutar o intentar introducir cualquier código de programación diseñado para auto replicarse, dañar o afectar el desempeño de cualquier dispositivo o infraestructura tecnológica.

- Utilizar medios de almacenamiento físico o virtual que no sean de carácter corporativo. Si estos medios son requeridos por la organización, deben se provisto por ella con previa autorización del Líder del Proceso y del área de Sistemas.

- El uso de código móvil, solo podrá ser utilizado si opera de acuerdo con las políticas y normas de seguridad definidas y debidamente autorizado por el área de Sistemas.

9.7.8. Copias de Respaldo

- El Hospital Nazareth debe asegurar que la información con cierto nivel de clasificación, definida en conjunto con el área de Sistemas y las áreas responsables de la misma, contenida en la plataforma tecnológica de la Institución, como servidores, dispositivos de red para almacenamiento de información, estaciones de trabajo, archivos de configuración de dispositivos de red y seguridad, entre otros, sea periódicamente resguardada mediante mecanismos y controles adecuados que garanticen su identificación, protección, integridad y disponibilidad.

- Adicionalmente, se deberá establecer un plan de restauración de copias de seguridad que serán probados a intervalos regulares con el fin de asegurar que son confiables en caso de emergencia y retenidas por un periodo de tiempo determinado.

- El área de Sistemas establecerá procedimientos explícitos de resguardo y recuperación de la información que incluyan especificaciones acerca del traslado, frecuencia, identificación y definirá conjuntamente con las dependencias los períodos de retención de la misma. Además, debe disponer de los recursos necesarios para permitir la identificación relacionada de los medios de almacenamiento, la información contenida en ellos y la ubicación física de los mismos para permitir un rápido y eficiente acceso a los medios que contienen la información resguardada.

- Los medios magnéticos que contienen la información crítica deben ser

almacenados en otra ubicación diferente a las instalaciones donde se

encuentra dispuesta. El sitio externo donde se resguardan dichas copias, debe tener los controles de seguridad adecuados, cumplir con máximas medida de protección y seguridad física apropiados. Lo anterior se debe realizar de acuerdo con lo establecido en el AP-INF-TI002I01Instructivo Copias de Respaldo (Backup).

- Es responsabilidad de todo funcionario realizar periódicamente una copia de seguridad de la información almacenada en el disco duro del equipo que le fue asignado, para ello solicitará al área de Sistemas los medios necesarios, los cuales entregará para que sean resguardados de acuerdo con las medidas de protección y seguridad física apropiados.

9.7.9. Gestión de medios removibles

- El uso de medios de almacenamiento removibles (ejemplo: CD, DVD, USB, memorias flash, discos duros externos, Iphone, celulares, cintas) sobre la infraestructura para el procesamiento de la información del Hospital Nazareth, estará autorizado para aquellos funcionarios cuyo perfil de cargo y funciones lo requiera.

- El área de Sistemas es responsable de implementar los controles necesarios para asegurar que en los sistemas de información del Hospital Nazareth sólo los funcionarios autorizados pueden hacer uso de los medios de almacenamiento removibles. Así mismo, el funcionario se compromete a asegurar física y lógicamente el dispositivo a fin de no poner en riesgo la información del Hospital Narareth.

- El almacenamiento, etiquetado y eliminación de cualquiera de estos medios de almacenamiento, debe estar de acuerdo con el esquema de clasificación y seguir los Lineamientos del Documento AP-INF-TI001D01 Inventario Consolidado de TI y de la Clasificación de Activos de Información.

9.7.10. Intercambio de información

- El Hospital Nazareth firmará acuerdos de confidencialidad con los funcionarios, clientes y terceros que por diferentes razones requieran conocer o intercambiar información restringida o confidencial de la Institución. En estos acuerdos quedarán especificadas las responsabilidades para el intercambio de la información para cada una de las partes y se deber firmar antes de permitir el

acceso o uso de dicha información.

- Todo funcionario del Hospital Nazareth es responsable por proteger la confidencialidad e integridad de la información y debe tener especial cuidado en el uso de los diferentes medios para el intercambio de información que puedan generar una divulgación o modificación no autorizada, cuyo uso aceptable se especifica en el presente plan **"9.2. Uso aceptable de los activos".**

- Los propietarios de la información que se requiere intercambiar son responsables de definir los niveles y perfiles de autorización para acceso, modificación y eliminación de la misma y los custodios de esta información son responsables de implementar los controles que garanticen el cumplimiento de los criterios de confidencialidad, integridad, disponibilidad y requeridos.

- En todo caso no se permite el acceso al equipo y/o datos de otro funcionario a través de la red sin el consentimiento de éste.

- Los medios transportados fuera de las instalaciones del Hospital Nazareth deberán cumplir con los controles establecidos.

9.8. Gestión con Proveedores

Todos los proveedores que por actividades internas tengan un contrato con el Hospital Nazareth de Quinchia, deberán acogerse a los siguientes lineamientos:

- Todo proveedor deberá cumplir con los lineamientos de seguridad de la información establecidos en el Hospital Nazareth, así mismo como con la normatividad definida en sus procesos internos.

- Los proveedores deberán hacer reporte de las debilidades de seguridad que puedan encontrar durante la ejecución del contrato con el Hospital Nazareth de Quinchia.

- Se deberá Informar sobre todas las actualizaciones existentes de cada plataforma que mejoren el desempeño de los procesos y subprocesos del Hospital.

- Todo proveedor adquiere el compromiso de reportar los impactos de los cambios aplicados en productivo a los procesos y subprocesos del Hospital.

- Los proveedores deberán hacer el reporte de eventos que afecten el desarrollo de los cambios que se aplicarán en productivo, desde la realización de las pruebas

hasta la salida a producción del requerimiento.

- Todos los proveedores deberán adherirse al flujo de requerimientos e incidentes establecido como proceso interno del Hospital Nazareth de Quinchia.

- Se deberá realizar transferencia de conocimiento y/o acompañamiento a los funcionarios responsables del proceso en el Hospital Nazareth.

- Los proveedores tienen el compromiso de aportar y realizar sugerencias para el mejoramiento de los procesos y óptimo aprovechamiento del servicio que se está prestando.

- El Hospital Nazareth será el único dueño de los derechos de autor de los desarrollos que se realicen internamente, los proveedores deberán respetar su confidencialidad

- Para el control de las actividades y según se haya definido en los contratos el proveedor deberá entregar a manera de informe según las estadísticas y métricas de:

  - Horas estimadas vs horas reales consumidas
  - Estado de los requerimientos
  - Cumplimiento de tiempos de entrega

10. BIBLIOGRAFÍA.

- ISO/IEC 27001:2013
- ISO/IEC 27002:2013
- COBIT 5 for information Security

11. SEGUIMIENTO, CONTROL Y MEJORA

Las acciones y actividades articuladas al plan de acción de acuerdo a lo estipulado en el decreto 612 de 2018 se encuentran diligenciadas en el formato ES-PLI-GP003F01 Formulación y Evaluación Plan de Acción.

Ver: Articulación de los planes MIPG HOSPITAL NAZARETH 2021.xlsx

12. MODIFICACIONES.

VERSIÓN	FECHA	RAZÓN DE LA ACTUALIZACION
00	18/03/2021	No aplica

		Se actualiza los procedimientos y la normatividad en base a la ISO27000:2013 con base a la herramienta de MSPI

13. APROBACIÓN.

ELABORÓ:	REVISÓ:	APROBÓ:
NOMBRE(S):	NOMBRE:	NOMBRE:
CARGO(S):	CARGO:	CARGO: