SOLICITUD DE INFORMACION

Entidad: HOSPITAL SAGRADO CORAZON DE JESUS
Responsable: JOSE FERNANDO DIAZ PETEVI
Area: GESTION INFROMATICA

En atención a la solicitud realizada, la entidad presenta el siguiente informe con el fin de dar respuesta a las preguntas relacionadas con el inventario de equipos, licenciamiento de software, mecanismos de control y destino final del software dado de baja. La información aquí consignada se encuentra respaldada por los documentos anexos y refleja las prácticas actuales de la organización.

1. **¿Con cuántos equipos cuenta la entidad y en qué áreas se encuentran ubicados?**

Área / Dependencia	Cantidad de equipos
Almacén	12
Ambulatorios – Promoción y Prevención	56
Apoyo diagnóstico – Imagenología	1
Apoyo diagnóstico – Laboratorio clínico	4
Apoyo terapéutico – Rehabilitación y terapias	3
Área financiera	22
Conexos a salud – Otros	1
Control interno	1
Coordinación científica	4
Farmacia	3
Gerencia	1
Hospitalización general	3
Mantenimiento	1
Pagaduría	1
Quirófano	8
Recursos humanos	18
Sistemas y comunicación	20
Servicios ambulatorios – Consulta externa y procedimientos	22
Servicio de urgencias	14
TOTAL	195

Total, general: 195 equipos de computo

2. ¿El software instalado en estos equipos se encuentra debidamente licenciado, anexe copia de las licencias?

Los equipos de cómputo de la entidad están certificados para operar con el software de sistemas de información hospitalaria **SIHOS** y cuentan adicionalmente con el programa **Compuconta**, licenciado por la empresa prestadora del servicio; todos los equipos que ingresan disponen de **licencias de software debidamente certificadas**, incluyendo los sistemas operativos que se encuentran licenciados conforme a los términos de los proveedores, y se garantiza la legalidad del software en uso mediante la **documentación anexa**, la cual respalda las licencias de los sistemas operativos y de las aplicaciones específicas adquiridas, asegurando así el cumplimiento normativo y la trazabilidad de cada licencia registrada.
Anexo 2.

3. ¿Qué mecanismos de control se han implementado para evitar que los usuarios instalen programas o aplicativos que no cuenten con la licencia respectiva, anexe los documentos soporte?

Todos los equipos pertenecen al dominio del hospital, lo que permite una gestión centralizada de usuarios y contraseñas, garantizando el control de permisos y accesos; las restricciones a nivel de usuario establecen que únicamente los administradores del sistema tienen autorización para instalar software, mientras que los usuarios estándar requieren autenticación previa para ejecutar procesos de instalación; adicionalmente, la política de seguridad informática contempla un protocolo de monitoreo y auditoría que asegura la supervisión periódica de los programas instalados en cada equipo y el cumplimiento de las normativas de software; finalmente, se anexan los documentos soporte, entre ellos la política de seguridad de TI y los procedimientos internos de gestión de software, como evidencia de los mecanismos de control implementados.

La entidad ha implementado un **Plan de Seguridad y Privacidad de la Información**, en el cual se establecen políticas y procedimientos que garantizan el uso adecuado de los equipos de cómputo y del software licenciado. Dentro de este plan se destacan los siguientes mecanismos de control:

- **Servidor centralizado con políticas de seguridad:** Se cuenta con un servidor que administra las autorizaciones y credenciales necesarias para la instalación de programas. Ningún usuario puede instalar software sin la debida autorización.
- **Restricción de permisos de usuario:** Los perfiles de los usuarios están configurados de acuerdo con los requerimientos de cada área, limitando la posibilidad de instalar aplicaciones no autorizadas.
- **Supervisión y control administrativo:** El área de sistemas realiza monitoreo constante para verificar el cumplimiento de las políticas de seguridad y prevenir la instalación de software no licenciado.

Documentos anexos:
- Plan de Seguridad y Privacidad de la Información
- Políticas de control de instalación de software

Anexo 3

4. **¿Cuál es el destino final que se le da al software dado de baja en su entidad, anexe documentos soporte?**

Destino final del software dado de baja
Durante la vigencia 2025 no se realizó baja de Software, sin embargo, se recomienda que implementar un protocolo de retiro y eliminación segura del software, que contemple los siguientes aspectos.

Desactivación de licencias: En caso de software con activaciones en línea, es recomendable desactivarlas antes de la baja del sistema.
Eliminación segura: Se debe garantizar la eliminación completa del software del sistema mediante herramientas de gestión que impidan su uso posterior sin licencia.
Registro de baja: Se debe documentar cada baja de software en un registro oficial, asegurando trazabilidad y cumplimiento normativo.
Análisis de reutilización: En caso de que las licencias sean transferibles, evaluar su posible reutilización en otros equipos dentro de la entidad.

1. **Desinstalación técnica:** El software se elimina de todos los equipos donde estaba instalado, asegurando que no quede operativo ni accesible para los usuarios.
2. **Retiro del inventario:** Se actualizan los registros oficiales de activos tecnológicos, marcando el software como “dado de baja” para que no aparezca como vigente.
3. **Archivo documental:** Se guarda el acta de baja junto con la licencia vencida o el contrato correspondiente, como soporte para auditorías futuras.
4. **Sustitución o reemplazo:** En muchos casos, el software dado de baja es reemplazado por una nueva versión o por otra aplicación que cumpla con los requisitos actuales de la entidad.
5. **Disposición segura:** Si el software contenía claves, configuraciones o datos sensibles, se asegura su eliminación definitiva para evitar riesgos de seguridad.

Anexo4.

MINISTERIO DEL INTERIOR Y DE JUSTICIA
DIRECCION NACIONAL DE DERECHO DE AUTOR
UNIDAD ADMINISTRATIVA ESPECIAL
OFICINA DE REGISTRO

CERTIFICADO DE REGISTRO DE ACTOS Y CONTRATOS

Libro - Tomo - Partida
11-98-431
Fecha Registro
17-Jun-2010

1. DATOS DE LAS PERSONAS

PARTE INTERVINIENTE — CEDENTE

Nombres y Apellidos JULIO CESAR GOMEZ GUZMAN — **No de identificación CC** 11319037

Nacional de COLOMBIA
Dirección MZ C CS 106 BARRIO EL REMANZO — **Ciudad** IBAGUE

PARTE INTERVINIENTE — CESIONARIO

Razón Social TECNOLOGIAS SINERGIA SAS — **Nit** 900349841

Nacional de --
Dirección -- — **Ciudad** BOGOTA D.C.

2. CLASE DE CONTRATO O ACTO

TRANSFERENCIA DE DERECHOS PATRIMONIALES

DURACION — TERMINO INDEFINIDO

3. OBJETO Y AÑO DE CREACIÓN

Objeto

POR EL CONTRATO DE TRANSFERENCIA EL AUTOR SE OBLIGA A TRANSFERIR LA TITULARIDAD DE LOS DERECHOS DE AUTOR DEL PROGRAMA DE COMPUTADOR SIHOS, DEBIDAMENTE INSCRITO ANTE EL MINISTERIOS DEL INTERIOR Y DE JUSTICIA.

4. VALOR

Gratuito
Cuantia 0
--

5. LUGAR Y FECHA DE LA FIRMA

IBAGUE — **08-Junio-2010**

6. OBSERVACIONES GENERALES DE LA OBRA

7. DATOS DEL SOLICITANTE

Nombres y Apellidos: JULIO CESAR GOMEZ GUZMAN — No de Identificacion: 11319037
Nacionalidad: COLOMBIA — Medio Radicacion: REGISTRO EN LINEA
Direccion: MZ C CS 106 BARRIO EL REMANZO — Teléfono 2[illegible]3 — Ciudad IBAGUE
Correo electrónico: COMERCIAL@SINERGIAONLINE.COM — Radicación de la Planilla: 1-2010-24532
En representación d: EN NOMBRE PROPIO

OSCAR EDUARDO SALAZAR ROJAS
JEFE DE LA OFICINA DE REGISTRO

MZP

Nota: El derecho de autor protege exclusivamente la forma mediante la cual las ideas del autor son descritas, explicadas, ilustradas o incorporadas a las obras . No son objeto de protección las ideas contenidas en las obras literarias y artísticas, o el contenido ideológico o técnico de las obras científicas, ni su aprovechamiento industrial o comercial (artículo 7o. de la Decisión 351 de 1993)

MINISTERIO DEL INTERIOR

DIRECCION NACIONAL DE DERECHO DE AUTOR

UNIDAD ADMINISTRATIVA ESPECIAL

OFICINA DE REGISTRO

CERTIFICADO DE REGISTRO DE SOPORTE LOGICO - SOFTWARE

Libro - Tomo - Partida
13-19-174
Fecha Registro
24-oct-2007

1. DATOS DE LAS PERSONAS

AUTOR

Nombres y Apellidos JULIO CESAR GOMEZ GUZMAN
No de identificación CC 11319037
Nacional de COLOMBIA
Dirección CRA 5 48 31 PIEDRA PINTADA ALTA
Ciudad: IBAGUE

PRODUCTOR

Nombres y Apellidos JULIO CESAR GOMEZ GUZMAN
No de identificación CC 11319037
Nacional de COLOMBIA
Dirección CRA 5 48 31 PIEDRA PINTADA ALTA
Ciudad: IBAGUE

2. DATOS DE LA OBRA

Título Original SIHOS

Año de Creación 1998 **País de Origen** COLOMBIA **Año Edición**

CLASE DE OBRA	INEDITA
CARACTER DE LA OBRA	OBRA INDIVIDUAL
CARACTER DE LA OBRA	OBRA ORIGINARIA
ELEMENTOS APORTADOS DE SOPORTE LOGICO	PROGRAMA DE COMPUTADOR
ELEMENTOS APORTADOS DE SOPORTE LOGICO	DESCRIPCIÓN DEL PROGRAMA

3. DESCRICIPCIÓN DE LA OBRA

SOFTWARE PARA INSTITUCIONES PRESTADORAS DE SERVICIOS DE SALUD QUE INTEGRA LAS AREAS ADMINISTRATIVAS Y ASISTENCIALES A TRAVES DE SUS DIFERENTES MODULOS. VER ANEXO DESCRIPCION DEL PROGRAMA

4. OBSERVACIONES GENERALES DE LA OBRA

CODIGO ENCRIPTADO DESARROLLADO EN PHP Y JAVA SCRIPT, SCRIPT DE LA BASE DE DATOS PARA MYSQL.

SE ANEXA 1 CD

5. DATOS DEL SOLICITANTE

Nombres y Apellidos **JULIO CESAR GOMEZ GUZMAN**
Nacional de **COLOMBIA**
Dirección **LOS ALPES MZ. L CASA 20 AMBALA**
Correo electrónico **ingjuliocesargomez@yahoo.com**
En representación de **EN NOMBRE PROPIO**

No de Identificación **11319037**
Medio Radicación **ENTREGA PERSONAL**
Ciudad **IBAGUE**
Teléfono **2752033**
Radicación de entrada **1-2007-28591**

MANUEL ANTONIO MORA CUELLAR

JEFE OFICINA DE REGISTRO

JRI

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

2024

	ELABORÓ	REVISÓ	REVISO	APROBÓ
NOMBRE	KENNY ROGER QUINDIGUA	THALIA NASNER	JHON FREDI REINA	CRISTIAN DANIEL AREVALO
FIRMA				
CARGO	COORDINADOR DE SISTEMAS	COORDINADORA DE CALIDAD	PROF. PLANEACION	GERENTE

1. OBJETIVO

Implementar estrategias para fortalecer la integridad, confidencialidad y disponibilidad de los activos de información de la E.S.E Hospital Sagrado Corazón de Jesús del Valle del Guamuez, que permitan minimizar los riesgos de pérdida de información, conforme a los lineamientos establecidos por el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) y alineado con las mejores prácticas en la protección de datos.

2. ALCANCE

El plan de Seguridad y privacidad de la Información abarca todos los activos de información de la E.S.E Hospital Sagrado Corazón de Jesús, incluidos los sistemas de información, bases de datos, redes, servidores y dispositivos utilizados por el personal. Se extiende a todos los funcionarios y contratistas que manejan información relacionada con los procesos misionales y de atención al paciente. Las áreas críticas cubiertas incluyen:

- Información de pacientes (historias clínicas, diagnósticos, tratamiento).
- Información financiera y de facturación.
- Información de gestión y administración hospitalaria.

Este plan incluye procedimientos específicos para la gestión, almacenamiento, protección y respaldo de la información crítica.

3. TALENTO HUMANO RESPONSABLE

- **Gerente**: Responsable de liderar la implementación del plan de seguridad y privacidad de la información. Aprobar las políticas y tomar decisiones estratégicas en cuanto a recursos y medidas de seguridad.
- **Coordinador de Gestión Informática**: Encargado de garantizar la seguridad e integridad de los datos de la ES.E. Hospital Sagrado Corazón de Jesús, velar por el control de accesos a la información y supervisar los mecanismos de protección de la información, así mismo llevando a cabo la coordinación y supervisión de los mantenimientos preventivos y correctivos de equipos tecnológicos.
- **Auxiliar de Sistemas**: Responsable de la infraestructura tecnológica de la E.S.E Hospital Sagrado Corazón de Jesús, implementar medidas técnicas de seguridad, como cortafuegos, sistemas de respaldo y también está encargado de la parte técnica de los equipos tecnológicos realizando los mantenimientos preventivos y correctivos de los mismo.
- **Coordinadores y Líderes de Procesos**: Responsables de asegurar que los activos de información utilizados en sus áreas de trabajo estén protegidos según los lineamientos del plan, supervisar el uso correcto de los sistemas de información.

4. RECURSOS TECNOLÓGICOS

La infraestructura tecnológica de la. E.S.E Hospital Sagrado Corazón de Jesús está compuesta por los siguientes recursos:

- **Servidores**: Sistemas de almacenamiento de datos críticos, incluidos los servidores que alojan las historias clínicas y la información financiera.
- **Redes**: El hospital cuenta con una red interna (intranet) segura y protegida por cortafuegos configurados para evitar accesos no autorizados.
- **Software**: La gestión de la información hospitalaria se realiza a través de sistema SIHOS, con el que se maneja la información de pacientes, facturación y administración general.
- **Dispositivos de Acceso**: Computadoras, tablets y otros dispositivos utilizados por el personal médico y administrativo para el acceso a los sistemas.

5. METAS

Las metas principales de este plan son:

- Garantizar la protección de la información crítica del hospital mediante políticas de acceso restringido.
- Implementar un sistema robusto de respaldo y recuperación de datos, asegurando la disponibilidad ante cualquier contingencia.
- Establecer controles de acceso físicos y lógicos para minimizar los riesgos de brechas de seguridad.
- Mantener un sistema de auditoría continua para monitorear el uso y acceso a la información del hospital.

6. DEFINICIONES

- **Activos de Información**: Información o elementos relacionados con su procesamiento (sistemas, bases de datos, personas) que tienen valor para la organización.
- **Clasificación de la Información**: Proceso de clasificar la información en función de su sensibilidad, criticidad y valor, con el fin de establecer los niveles de protección necesarios.
- **Confidencialidad**: Asegurar que la información solo esté disponible para quienes tienen derecho de acceso.
- **Integridad**: Mantener la exactitud y completitud de la información, evitando su modificación no autorizada.
- **Disponibilidad**: Asegurar que la información esté accesible y utilizable cuando sea necesario.

7. ESTRATEGIAS DE SEGURIDAD

El hospital implementará las siguientes estrategias para asegurar la información:

- **Gestión de Riesgos**: Evaluación continua de los riesgos asociados a los activos de información, determinando las vulnerabilidades y aplicando controles preventivos y correctivos.
- **Control de Accesos**: Implementación de políticas de acceso basadas en roles, asegurando que solo personal autorizado acceda a información sensible. Uso de autenticación multifactor y contraseñas robustas.
- **Respaldo de Información**: Realización de copias de seguridad periódicas en servidores locales y externos. Asegurar la redundancia en las copias de seguridad, con planes de recuperación ante desastres.

8. PLAN DE ACCIÓN

Gestión de Activos

La E.S.E. Hospital Sagrado Corazón de Jesús realizará un inventario de todos los activos de información, este inventario será administrado por el proceso de Gestión de la Tecnología, utilizando un sistema automatizado de gestión de activos que permita la identificación, clasificación y monitoreo de los mismos. Se utilizarán etiquetas y otros mecanismos tecnológicos para asegurar el control y la trazabilidad de los activos.

Custodia de Activos

La E.S.E. Hospital Sagrado Corazón de Jesús implementará políticas estrictas de respaldo de datos, se realizarán copias de seguridad automáticas de los sistemas críticos, con almacenamiento en servidores internos y en la nube para asegurar la redundancia. Además, se utilizarán medidas de cifrado para proteger los datos en tránsito y en reposo.

CRONOGRAMA PLAN DE ACCIÓN: GESTIÓN Y CUSTODIA DE ACTIVOS (2 AÑOS)

Línea de Acción	Objetivo	Actividad	Indicador	Fecha de Evaluación	Meta	Responsable
Gestión de activos de información	Identificar, clasificar y proteger los activos de información del hospital.	- Planificación del inventario de activos. - Selección e implementación de un sistema automatizado de gestión de activos.	Inventario planificado y sistema seleccionado.	Trimestre 1, Año 1	100% de activos inventariados.	Coordinador Sistemas

		- Realización del inventario inicial de activos. - Clasificación y etiquetado de activos críticos usando tecnología de trazabilidad.	% de activos clasificados y etiquetados.	Trimestre 2, Año 1	Clasificación del 100% de activos.	Coordinador Sistemas
		- Finalización del inventario.	Inventario terminado y monitoreo operativo.	Trimestre 3, Año 1	Monitoreo continuo habilitado.	Coordinador Sistemas
Respaldo y recuperación de datos	Garantizar la disponibilidad y la seguridad de los datos institucionales.	- Implementación de políticas estrictas de respaldo (copias de seguridad semestrales). - Almacenamiento en servidores internos.	% de copias realizadas y verificadas.	semestre 1, Año 2	Respaldo semestral de todos los datos.	Coordinador Sistemas
		- Almacenamiento de respaldos en disco externo para garantizar redundancia.	% de respaldos almacenados en la nube.	Trimestre 2, Año 2	Redundancia completa habilitada.	Coordinador Sistemas
Seguridad de la información	Proteger la confidencialidad y la integridad de la información mediante cifrado y acceso controlado.	- Implementación de medidas de cifrado en tránsito y reposo.	% de datos cifrados y pruebas exitosas.	Trimestre 3, Año 2	100% de datos cifrados y probados.	Coordinador Sistemas
		- Implementación de políticas de control de	% de roles configurados y ajustes	Trimestre 4, Año 2	Roles ajustados según auditoría.	Coordinador Sistemas / Auditoría Interna

		accesos basadas en roles.	completados.			

9. NORMATIVA

Legislación Colombiana sobre Protección de Datos Personales:

1. **Ley 1581 de 2012** - **"Por la cual se dictan disposiciones generales para la protección de datos personales"**
   Esta ley establece el marco normativo para el tratamiento de datos personales en Colombia, regulando los derechos de los titulares de los datos y las obligaciones de las entidades responsables del tratamiento.
2. **Decreto 1377 de 2013** - **"Por el cual se reglamenta parcialmente la Ley 1581 de 2012"**
   Regula los procedimientos para la autorización del tratamiento de datos personales, especialmente en lo relativo al tratamiento de datos de personas que no han sido registradas previamente.
3. **Ley 1266 de 2008** - **"Por la cual se dictan disposiciones sobre el Habeas Data en relación con la información financiera, crediticia, comercial, de servicios y la proveniente de terceros países"**
   Regula el tratamiento de datos relacionados con el historial crediticio y la información financiera de los consumidores.
4. **Ley 1712 de 2014** - **"Por la cual se adopta la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional"**
   Esta ley tiene implicaciones en términos de acceso y manejo de la información pública y la protección de datos personales en el contexto gubernamental.
5. **Sentencias de la Corte Constitucional de Colombia**
   Las sentencias relacionadas con el habeas data (como la Sentencia C-748 de 2011) también son relevantes, ya que establecen principios clave sobre la protección de los derechos de los titulares de datos personales.
6. **Resolución 097 de 2015 de la Superintendencia de Industria y Comercio (SIC)**
   Esta resolución establece el procedimiento para la inscripción en el Registro de Bases de Datos de la SIC, requisito para las entidades que tratan datos personales en Colombia.

10. EVALUACIÓN Y MONITOREO

La evaluación del Plan de Seguridad y Privacidad de la Información de la E.S.E Hospital Sagrado Corazón de Jesús, se realizará mediante auditorías trimestrales, supervisando el cumplimiento de las políticas de seguridad, se utilizarán herramientas de monitoreo. Además, se actualizará el plan en función de los nuevos riesgos identificados y de los cambios en la infraestructura tecnológica de la entidad.

Línea de acción	Herramienta	Descripción	Objetivo	Procedimiento	Indicador	Fecha de evaluación	Metas	Responsable
Protección	Antivirus Windows Defender	Software para detecció	Garantizar la protecció	- Instalar en equipos	Porcentaje de	Trimestral	100% de equipos	Coordinador de

contra malware		n, eliminación y prevención de malware.	n de equipos críticos.	críticos.	equipos protegidos.		protegidos.	Sistemas
Seguridad de red	Firewall (Cortafuegos)	Control del tráfico de entrada y salida de la red.	Prevenir accesos no autorizados.	- Configurar reglas de acceso según políticas. -Actualizar configuraciones ante nuevas amenazas.	Cantidad de intentos bloqueados.	Semestral	Reducir incidentes a <2% del tráfico.	Coordinador de Sistemas
Respaldo de información	Copias de seguridad	Creación de réplicas de datos críticos en servidores externos o en la nube.	Garantizar la disponibilidad de información.	- Programar copias semestrales en horario nocturno. - Verificar la integridad de las copias mensualmente.	Porcentaje de respaldos exitosos.	Trimestral	100% de integridad en copias.	Coordinador de Sistemas
Gestión de accesos	Políticas de acceso	Normas definidas para garantizar el control adecuado de usuarios en sistemas.	Asegurar que solo usuarios autorizados accedan.	- Revisar y actualizar permisos trimestralmente. - Implementar autenticación de dos factores. - Realizar auditorías de acceso semestrales.	Porcentaje de accesos autorizados.	Semestral	100% de accesos controlados.	Coordinador de Sistemas

11. ANEXOS

- **Tabla de Identificación de Riesgos de Seguridad y Privacidad de la Información**

Diagnóstico para la Identificación de Riesgos de Seguridad

1. Objetivo del Diagnóstico

El objetivo del diagnóstico es identificar, evaluar y priorizar los riesgos que puedan afectar la seguridad de la información y los sistemas en el ámbito organizacional, asegurando la implementación de controles adecuados para mitigar las amenazas.

2. Metodología de Identificación de Riesgos

Basado en la Guía de Administración de Riesgos, Versión 6 del DAFP:

1. **Contextualización del proceso:**
   - Identificar los activos críticos de información (datos personales, registros médicos, sistemas de red, infraestructura tecnológica).
   - Definir el alcance: áreas, procesos y actores involucrados en la seguridad de la información.
2. **Identificación de riesgos:**
   - **Eventos de riesgo:** Posibles eventos que podrían impactar la seguridad, confidencialidad, integridad o disponibilidad de la información.
   - **Factores de riesgo:** Elementos internos o externos que pueden desencadenar un evento.
   - **Amenazas:** Identificar amenazas como ciberataques, errores humanos, fallos técnicos, desastres naturales o malas prácticas en la gestión de la información.
   - **Vulnerabilidades:** Identificar debilidades en los sistemas, procesos o controles de seguridad.
3. **Técnicas de identificación:**
   - Análisis documental (políticas internas, procedimientos).
   - Encuestas y entrevistas con los responsables de procesos y tecnología.
   - Talleres de identificación participativa.
   - Revisiones de auditorías previas y análisis de incidentes pasados.

3. Análisis de Riesgos

Realizar un análisis de los riesgos identificados para determinar:

- **Probabilidad de ocurrencia:** Alta, media, baja.
- **Impacto:** Crítico, alto, medio, bajo, con base en la afectación a la organización (económica, reputacional, legal, operativa).

Utilizar matrices de probabilidad-impacto para priorizar riesgos.

4. Clasificación de los Riesgos Identificados

Organizar los riesgos según las categorías principales:

- **Riesgos tecnológicos:** Fallos en hardware, software desactualizado, vulnerabilidades en la red.
- **Riesgos humanos:** Capacitación insuficiente, errores operativos, manejo negligente de la información.
- **Riesgos físicos:** Robo o daño de equipos, acceso no autorizado a instalaciones.
- **Riesgos organizacionales:** Ausencia de políticas claras, incumplimiento normativo.

5. Evaluación de Controles Existentes

Determinar los controles actuales para mitigar los riesgos identificados, como:

- Políticas y procedimientos de seguridad.
- Capacitación y sensibilización de personal.
- Uso de herramientas tecnológicas de seguridad (antivirus, firewalls, cifrado).

Identificar brechas en los controles y proponer mejoras.

6. Recomendaciones para Mitigación de Riesgos

- Establecer un plan de acción para cada riesgo identificado.
- Priorizar la implementación de controles según la criticidad del riesgo.
- Monitorear continuamente los riesgos y la eficacia de los controles.

Identificación de Riesgos de Seguridad y Privacidad de la Información

Riesgo	Descripción del Riesgo	Clase o Tipo de Riesgo	Causas (Factores Internos o Externos)	Efectos	Tipo de Impacto	Controles Existentes	Zona de Riesgo	Acciones	Responsable
Software sin licencias y desactualización	Uso de software ilegal o vencimiento de licencias	Riesgos de Cumplimiento	- Desconocimiento de normas de derechos de autor - Falta de presupuesto - Falta de control de usuarios	Sanciones legales	Impacto Legal	Usuarios locales con restricciones de instalación y desinstalación	Alta	Implementar controles para limitar instalación de software no autorizado.	Dependencia de Sistemas y Gerencia
Copias de seguridad	Custodia y administración inadecuada de las copias de seguridad	Riesgos Operativos	- Problemas eléctricos - Daño de equipos externos	Pérdida de información alojada en servidores	Impacto Operativo	Copias de seguridad diarias almacenadas en discos duros externos	Alta	Realizar copias de seguridad periódicas y verificar su integridad.	Dependencia de Sistemas
Daño en la estructura tecnológica	Pérdida de conexión y recuperación de bases de datos	Riesgos Operativos	- No cumplimiento de mantenimiento - Desastres naturales - Ataques cibernéticos	Pérdida de información y suspensión de servicios	Impacto Operativo	Actualización de hardware y cronograma de mantenimiento preventivo	Baja	Incluir nuevos equipos al cronograma de mantenimiento preventivo.	Dependencia de Sistemas
Daño en bases de datos	Pérdida de información y datos inconsistentes	Riesgos Operativos	- Accesos no restringidos a servidores - Ausencia de políticas de seguridad informática	Pérdida de información y datos inconsistentes	Impacto Operativo	Claves de acceso a servidores	Alta	Eliminar software de conexión remota no autorizado y configurar claves seguras.	Dependencia de Sistemas

PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

	ELABORÓ	REVISÓ	RVISO	APROBÓ
NOMBRE	KENNY ROGER QUINDIGUA B	THALIA NASNER MORA	JHON FREDI REINA	CRISTIAN DANIEL AREVALO
FIRMA				
CARGO	COORDINADOR DE SISTEMAS	COORDINADORA DE CALIDAD	PROF. PLANEACION	GERENTE

1. OBJETIVO

Establecer medidas preventivas, correctivas y de mitigación ante riesgos relacionados con la seguridad y privacidad de la información en el Hospital Sagrado Corazón de Jesús del Valle del Guamuez. Esto incluye la protección de datos sensibles, la prevención de amenazas, y el aseguramiento del cumplimiento normativo, de acuerdo con las directrices del MinTIC y las leyes de protección de datos personales en Colombia (Ley 1581 de 2012).

2. ALCANCE

El plan cubre los sistemas de información, redes, bases de datos y cualquier plataforma que almacene, procese o transmita información sensible dentro del hospital, incluyendo:

- **Datos personales y clínicos de los pacientes**: Información sensible que debe protegerse contra acceso no autorizado, pérdida o robo.
- **Sistemas Hospitalario (SIHOS)**: Garantizar la integridad, confidencialidad y disponibilidad de la información almacenada en las HC.
- **Sistemas Administrativos**: Protección de datos financieros, de recursos humanos y otros relacionados con la gestión operativa del hospital.
- **Infraestructura Tecnológica**: Incluye servidores, redes, estaciones de trabajo y dispositivos móviles utilizados en el hospital.

3. TALENTO HUMANO RESPONSABLE

3.1 Roles y Responsabilidades Claves:

- **Gerente**: Lidera la implementación del plan de seguridad y privacidad de la información. Es responsable de aprobar las políticas y tomar decisiones estratégicas sobre los recursos necesarios para garantizar la protección de la información sensible del hospital.
- **Coordinador de Gestión Informática**: Garantiza la seguridad e integridad de los datos del hospital. Supervisa el control de accesos a la información y asegura que se implementen medidas adecuadas de protección para mantener la confidencialidad y disponibilidad de los datos.
- **Auxiliar de Sistemas**: Son responsables de la infraestructura tecnológica del hospital. Implementan medidas técnicas de seguridad, tales como la configuración de cortafuegos, la realización de respaldos y la utilización de herramientas de auditoría para asegurar la continuidad operativa.
- **Coordinadores y Líderes de Procesos**: Supervisan que los activos de información en sus áreas de trabajo estén protegidos según los lineamientos del plan. Promueven el uso seguro y adecuado de los sistemas de información entre sus equipos de trabajo.
- **Trabajadores y colaboradores de la ESE Hospital Sagrado Corazon de Jesus**: Son responsables de seguir las políticas y procedimientos de seguridad establecidos. Deben adoptar buenas prácticas en el manejo de la información, proteger los datos a los que tengan acceso y reportar cualquier incidente de seguridad que detecten.

4. RECURSOS TECNOLÓGICOS

Los principales recursos tecnológicos involucrados en el tratamiento de riesgos de seguridad y privacidad de la información son:

- **Sistemas de Seguridad Perimetral**: Firewalls, sistemas de detección y prevención de intrusiones (IPS), redes privadas virtuales (VPN) para el acceso seguro.
- **Software de Protección de Datos**: Soluciones antivirus y antimalware, cifrado de datos, herramientas de monitoreo de actividad en la red.
- **Infraestructura de Almacenamiento**: Sistemas de respaldo y recuperación ante desastres (backups), servidores y almacenamiento seguro para datos sensibles.
- **Sistemas de Control de Acceso**: Implementación de políticas de control de acceso basadas en roles y gestión de contraseñas seguras.

5. METAS

1. **Reducción del Riesgo de Violaciones de Datos**: Minimizar en un 90% los incidentes de seguridad relacionados con violaciones de datos personales y clínicos en los próximos 12 meses.
2. **Cumplimiento Normativo**: Asegurar el cumplimiento del 100% de las normativas de seguridad de la información y privacidad según los lineamientos del MinTIC y la Ley 1581.
3. **Fortalecimiento de la Infraestructura de Seguridad**: Implementar soluciones tecnológicas avanzadas para la protección perimetral y la detección de amenazas en tiempo real.
4. **Capacitación del Personal**: Lograr que el 100% del personal administrativo y asistencial de la E.S.E Hospital Sagrado Corazón de Jesús esté capacitado en las políticas de seguridad y manejo seguro de la información en los próximos 6 meses.
5. **Verificaciones Periódicas**: Realizar verificaciones semestrales de los sistemas de seguridad y privacidad para identificar y corregir vulnerabilidades.

6. DEFINICIONES

- **Riesgo:** Probabilidad de un impacto negativo en activos de información.
- **Privacidad:** Protección de datos personales contra accesos no autorizados.
- **Amenaza:** Potencial evento que afecta la seguridad de la información.
- **Vulnerabilidad:** Debilidad que puede ser explotada por una amenaza.
- **Impacto:** Consecuencia de un riesgo materializado.
- **Controles:** Medidas para mitigar riesgos de seguridad.
- **Incidentes:** Eventos inesperados que comprometen la información.
- **Ciberseguridad:** Protección de sistemas contra ataques digitales.
- **Auditoría:** Evaluación periódica de procesos y controles.

- **Respaldo:** Copia de datos para recuperación ante incidentes.
- **Continuidad:** Plan para mantener operaciones en emergencias.
- **IPv6:** Protocolo de red con mayor seguridad y capacidad.
- **Matriz de Riesgos:** Herramienta para identificar y evaluar riesgos.
- **Cumplimiento:** Conformidad con normativas de seguridad.
- **Confidencialidad:** Restricción de acceso a información sensible.

7. MARCO NORMATIVO

- **Decreto 612 de 2018:** Por el cual se fijan las directrices para la integración de los planes institucionales y estratégicos al plan de acción por parte de las entidades del estado.

- **Ley 1712 de 2014:** Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.

- **Norma Técnica Colombiana - NTC ISO 27001.** Norma internacional de sistemas de gestión de seguridad y confidencialidad de la información.

8.ESTRATEGIAS

1. **Implementación de Controles Preventivos:**
   - Uso de firewalls, antivirus y herramientas de detección de intrusos.
   - Aplicación de políticas de contraseñas seguras y autenticación multifactorial.
   - Configuración de permisos de acceso y privilegios mínimos.
2. **Capacitación y Concientización:**
   - Formación del personal en buenas prácticas de seguridad de la información.
   - Realización de talleres sobre protección de datos personales y ciberseguridad.
3. **Gestión de Incidentes:**
   - Definir un procedimiento claro para identificar, responder y aprender de incidentes de seguridad.
   - Designar roles y responsabilidades en caso de incidentes.
4. **Monitoreo y Auditoría:**
   - Implementación de herramientas de monitoreo para identificar actividades inusuales.
   - Realización de auditorías periódicas para garantizar el cumplimiento de normativas.
5. **Plan de Contingencia:**
   - Crear un plan de respaldo y recuperación de datos en caso de incidentes.
   - Establecer protocolos para la continuidad del negocio durante emergencias.
6. **Transición a IPv6:**
   - Planificar la migración de IPv4 a IPv6 para garantizar una mayor seguridad en las redes.

- Actualizar las configuraciones de hardware y software para soportar IPv6.

7. **Evaluación de Riesgos Continuos:**
   - Revisar regularmente la matriz de riesgos para identificar nuevas amenazas o vulnerabilidades.
   - Ajustar el plan de tratamiento de riesgos basado en los resultados de estas evaluaciones.
8. **Gestión de Terceros:**
   - Asegurar que proveedores y aliados cumplan con las normativas de seguridad y privacidad.
   - Firmar acuerdos de confidencialidad y servicio.

9. PLAN DE ACCIÓN

El Plan de Acción se basa en las actividades necesarias para mitigar y gestionar los riesgos de seguridad y privacidad de la información en el hospital. Se sigue un cronograma basado en los lineamientos del MinTIC.

ACTIVIDAD	RESPONSABLE	RECURSOS	PLAZO	INDICADORES DE ÉXITO
Evaluación inicial de riesgos de seguridad	Coordinación sistemas.	Recursos humanos y financieros	1 mes	Informe de evaluación de riesgos
Implementación de controles de acceso avanzados	Coordinación sistemas.	Software de control de acceso	2 meses	100% de sistemas con control de acceso
Actualización de sistemas de ciberseguridad	Coordinación sistemas.	Firewalls, IDS/IPS, SIEM	3 meses	90% de reducción en incidentes de seguridad
Capacitación en protección de datos personales	Coordinación sistemas.	Recursos de capacitación	6 meses	100% del personal capacitado
Pruebas de restauración y recuperación de datos	Coordinación sistemas.	Infraestructura de backup	4 meses	100% de efectividad en pruebas de backup

9.1 Cronograma De Implementación

MES	ACTIVIDAD
1	Evaluación de riesgos, auditoría inicial
2	Implementación de controles de acceso
3	Actualización de ciberseguridad, monitoreo continuo

4	Pruebas de restauración y recuperación de datos
5	Auditoría de cumplimiento de privacidad
6	Capacitación del personal, revisión de resultados

Este cronograma sigue los lineamientos del MinTIC para la gestión de riesgos de seguridad y privacidad de la información.

10. EVALUACIÓN

La evaluación de la efectividad del plan será continua, con auditorías periódicas y revisiones semestrales de los indicadores clave. Cada 6 meses se generarán informes de evaluación de riesgos, con el fin de ajustar y mejorar las medidas de seguridad según los nuevos desafíos tecnológicos y normativos.

- **Indicadores Clave**:
  - Reducción de incidentes de seguridad en un 90% anual
  - Cumplimiento del 100% en normativas de seguridad y privacidad
  - Efectividad del sistema de respaldo (>99%)
  - Satisfacción del personal con las capacitaciones (>85%)

CONTROL DE VERSION

FECHA	VERSION	DESCRIPCION DEL CAMBIO	DISTRIBUIDO A
Enero 2024	1	Creación del Documento	Todos los Procesos