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