EMPRESA SOCIAL DEL ESTADO
HOSPITAL REGIONAL DE CHIQUINQUIRÁ
DEPARTAMENTO DE BOYACÁ

SEGURIDAD DE LAS COMUNICACIONES DE TI

CHIQUINQUIRÁ, DICIEMBRE DE 2024

1. Tabla de Contenido

2. Introducción

La seguridad de las comunicaciones es un componente crítico dentro de la gestión de la seguridad de la información en el Hospital Regional de Chiquinquirá. Este protocolo tiene como objetivo establecer las directrices y procedimientos necesarios para garantizar la protección de la información transmitida a través de las redes y sistemas de comunicación, tanto internos como externos.

La implementación de este protocolo es fundamental para prevenir accesos no autorizados, interceptaciones, modificaciones o pérdidas de información sensible. Este documento aplica a todos los funcionarios, contratistas y proveedores que interactúan con los sistemas de comunicación del hospital, incluyendo redes cableadas, inalámbricas, servicios de mensajería electrónica y transferencia de datos.

3. Identificación

PROCESO	**GESTION DE RECURSOS LOGISTICOS**
SUBPROCESO	Tecnologías de la Información y las Comunicaciones
OBJETIVO GENERAL	Establecer los controles y procedimientos necesarios para garantizar la seguridad de la información transmitida a través de las redes y sistemas de comunicación de la ESE Hospital Regional de Chiquinquirá.
OBJETIVOS ESPECÍFICOS	➢ Implementar controles de red para proteger la información en sistemas y aplicaciones. ➢ Establecer políticas y procedimientos para la transferencia segura de información. ➢ Garantizar la separación de redes y servicios de información para minimizar riesgos.
ALCANCE	Este protocolo aplica a todas las áreas de la ESE Hospital Regional de Chiquinquirá, incluyendo su sede Sucre y La Victoria y servicios prestados, así como a los proveedores externos que interactúan con los sistemas de comunicación del hospital.

4. Definiciones y Conceptos

Seguridad de las Comunicaciones: Conjunto de medidas y controles implementados para proteger la información transmitida a través de redes y sistemas de comunicación.

Redes Seguras: Infraestructura de red diseñada para prevenir accesos no autorizados y garantizar la confidencialidad, integridad y disponibilidad de la información.

Transferencia de Información: Proceso de enviar y recibir datos entre sistemas, aplicaciones o entidades, asegurando su protección durante el tránsito.

Mensajería Electrónica: Comunicación digital que incluye correos electrónicos, mensajes instantáneos y otros medios de transmisión de información.

5. Generalidades

La seguridad de las comunicaciones se basa en los siguientes principios:

1. **Confidencialidad:** Garantizar que la información solo sea accesible para personas autorizadas.
2. **Integridad:** Asegurar que la información no sea alterada durante su transmisión.
3. **Disponibilidad:** Mantener los servicios de comunicación operativos y accesibles cuando sean requeridos.

Se deben implementar controles técnicos y administrativos para proteger las redes, servicios de comunicación y la información transmitida.

6. Materiales e Insumos Requeridos

- **Hardware:** Routers, switches, firewalls, servidores de red.
- **Software:** Herramientas de cifrado, sistemas de detección de intrusiones, antivirus.
- **Documentación**: Políticas de seguridad, procedimientos de transferencia de información, acuerdos de confidencialidad.

7. Roles y responsabilidades

ROL	RESPONSABILIDAD
Líder de TI	Supervisar la implementación de los controles de seguridad en las redes y sistemas.
Administrador de Red	Configurar y mantener los dispositivos de red y servicios de comunicación.
Personal de Seguridad	Monitorear y responder a incidentes de seguridad en las comunicaciones.
Personal Operativo	Cumplir con las políticas y procedimientos de seguridad de las comunicaciones.

8. Contenido del Protocolo de Seguridad de las Comunicaciones

8.1 Gestión de la Seguridad de las Redes

8.1.1 Controles de Redes

Objetivo: Asegurar que las redes estén gestionadas y controladas para proteger la información en sistemas y aplicaciones.

Implementación:

Firewalls y Sistemas de Detección de Intrusiones (IDS):

- Instalar y configurar firewalls en todos los puntos de entrada y salida de la red.
- Implementar sistemas de detección de intrusiones para monitorear el tráfico de red y detectar actividades sospechosas.
- Configurar reglas de firewall para permitir solo el tráfico autorizado y bloquear accesos no autorizados.

Segmentación de Redes:

- Crear redes VLAN (Virtual Local Area Network) para separar el tráfico según su nivel de sensibilidad (por ejemplo, red de pacientes, red administrativa, red de proveedores).
- Aislar redes críticas (como las que manejan datos de pacientes) de redes menos sensibles (como las de acceso público).

Monitoreo Continuo:

- Implementar herramientas de monitoreo de red para detectar anomalías en el tráfico.
- Configurar alertas automáticas para actividades sospechosas, como intentos de acceso no autorizado o tráfico inusual.

Actualización de Firmware y Parches:

- Mantener actualizados los dispositivos de red (routers, switches, firewalls) con los últimos parches de seguridad.
- Realizar revisiones periódicas de vulnerabilidades en la infraestructura de red.

8.1.2 Seguridad de los Servicios de Red

Objetivo: Identificar y gestionar los mecanismos de seguridad, niveles de servicio y requisitos de gestión de los servicios de red.

Implementación:

Acuerdos de Nivel de Servicio (SLA):

- Establecer acuerdos de nivel de servicio con proveedores de red, especificando los requisitos de seguridad, disponibilidad y rendimiento.
- Incluir cláusulas de seguridad en los SLA, como la notificación de incidentes y la respuesta ante brechas de seguridad.

Autenticación y Cifrado:

- Implementar autenticación de usuarios mediante protocolos seguros como WPA3 para redes inalámbricas.
- Utilizar cifrado de datos (por ejemplo, **IPSec** o **TLS**) para proteger la información transmitida a través de la red.

Gestión de Accesos:

- Configurar controles de acceso basados en roles (RBAC) para limitar el acceso a servicios de red según las responsabilidades de cada usuario.
- Implementar autenticación de dos factores (2FA) para acceder a servicios críticos.

8.1.3 Separación en las Redes

Objetivo: Separar grupos de servicios de información, usuarios y sistemas de información en las redes para minimizar riesgos.

Implementación:

Segmentación de Redes:

- Crear redes separadas para diferentes tipos de usuarios (por ejemplo, personal médico, administrativo, proveedores).
- Aislar redes de dispositivos IoT (Internet de las Cosas) de las redes principales para evitar accesos no autorizados.

Control de Acceso entre Redes:

- Implementar reglas de firewall para controlar el tráfico entre redes segmentadas.
- Restringir el acceso entre redes sensibles y no sensibles.

Redes Privadas Virtuales (VPN):

- Configurar VPN para el acceso remoto seguro a la red del hospital.
- Asegurar que todas las conexiones remotas utilicen cifrado fuerte (por ejemplo, **AES-256**).

8.2 Transferencia de Información

8.2.1 Políticas y Procedimientos de Transferencia de Información

Objetivo: Establecer políticas y procedimientos formales para proteger la transferencia de información.

Implementación:

Protocolos de Transferencia Segura:

- Utilizar protocolos seguros como **SFTP** (Secure File Transfer Protocol) y **HTTPS** para la transferencia de archivos y datos.
- Implementar cifrado de extremo a extremo para todas las transferencias de información.

Políticas de Transferencia:

- Establecer políticas que definan los métodos aprobados para la transferencia de información (por ejemplo, no se permite el uso de servicios de almacenamiento en la nube no autorizados).
- Prohibir la transferencia de información sensible a través de correos electrónicos no cifrados.

Registro de Transferencias:

- Mantener un registro de todas las transferencias de información, incluyendo el tipo de datos, el destinatario y el método utilizado.
- Revisar periódicamente los registros para detectar transferencias no autorizadas.

8.2.2 Acuerdos sobre Transferencia de Información

Objetivo: Establecer acuerdos para la transferencia segura de información con entidades externas.

Implementación:

Acuerdos de Confidencialidad:

- Firmar acuerdos de confidencialidad (NDA) con proveedores y terceros que tengan acceso a información sensible.
- Incluir cláusulas que especifiquen las responsabilidades en caso de pérdida o filtración de información.

Revisión Periódica:

- Revisar y actualizar los acuerdos de transferencia de información al menos una vez al año.
- Asegurar que los acuerdos cumplan con las normativas vigentes (por ejemplo, Ley de Protección de Datos).

8.2.3 Mensajería Electrónica

Objetivo: Proteger adecuadamente la información incluida en la mensajería electrónica.

Implementación:

Cifrado de Correos Electrónicos:

- Implementar sistemas de correo electrónico que soporten cifrado de extremo a extremo (por ejemplo, **S/MIME** o **PGP**).
- Configurar políticas para que todos los correos electrónicos que contengan información sensible sean cifrados automáticamente.

Políticas de Uso Aceptable:

- Establecer políticas que prohíban el envío de información sensible a través de servicios de mensajería no autorizados (por ejemplo, WhatsApp o correos personales).

- Capacitar al personal en el uso seguro del correo electrónico y la mensajería instantánea.

Protección contra Phishing:

- Implementar filtros antispam y antiphishing en el servidor de correo electrónico.
- Realizar simulacros de phishing para concienciar al personal sobre los riesgos.

8.3 Monitoreo y Mejora Continua

8.3.1 Monitoreo de la Seguridad de las Comunicaciones

- Implementar herramientas de monitoreo continuo para detectar y responder a incidentes de seguridad en las comunicaciones.
- Revisar periódicamente los registros de actividad de red y transferencia de información.

8.3.2 Mejora Continua

- Realizar auditorías internas y externas para evaluar la efectividad de los controles de seguridad de las comunicaciones.
- Actualizar los procedimientos y políticas en función de los resultados de las auditorías y los cambios en el entorno de seguridad.

9. Recomendaciones

- Realizar auditorías periódicas de seguridad en las redes y sistemas de comunicación.
- Capacitar al personal en buenas prácticas de seguridad de las comunicaciones.
- Mantener actualizados los sistemas y software de seguridad.

10. Herramienta y Metodología de Evaluación

Lista de verificación basada en los controles del Anexo A.13 de la ISO/IEC 27001 y evaluación trimestral del cumplimiento de los controles de seguridad de las comunicaciones.

11. Documentos Relacionados del Sistema Integrado de Gestión

CODIGO	DESCRIPCION
3.3.2.D01	PLAN ESTRATEGICO DE TECNOLOGIAS DE LA INFORMACION
3.3.2.D02	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN
3.3.2.D02.F01	REGISTRO DE NACIMIENTOS ATENDIDOS ESE HRC
3.3.2.D02 F02	COMPROMISO DE SEGURIDAD, DISPONIBILIDAD Y CONFIDENCIALIDAD DE LA INFORMACION
3.3.2.D03	PLAN DE DATOS ABIERTOS
3.3.2.D03 F01	REGISTRO DE NACIMIENTOS ATENDIDOS EN LA E.S.E. HOSPITAL REGIONAL DE CHIQUINQUIRA
3.3.2.D03 F02	REGISTRO DE DEFUNCIONES ATENDIDOS EN LA E.S.E. HOSPITAL REGIONAL DE CHIQUINQUIRA
3.3.2.D03 F03	REGISTRO BASE DE DATOS SIVIGILA E.S.E. HOSPITAL REGIONAL DE CHIQUINQUIRA
3.3.2.D03 F04	REGISTRO BASES DE DATOS MORVILIDAD E.S.E. HOSPITAL REGIONAL DE CHIQUINQUIRA
3.3.2.D04	PLAN DE TRATAMIENTO DE RIESTGOS DE SEGURIDAD DE LA INFORMACION
3.3.2.P01	MANTENIMIENTO PREVENTIVO A EQUIPOS TECNOLOGICOS
3.3.2.P01 F01	MANTENIMIENTO PREVENTIVO DE EQUIPOS DE COMUNICACIONES E INFORMATICA
3.3.2.P01 F02	MANTENIMIENTO PREVENTIVO DE IMPRESORAS Y SCANNER
3.3.2.P01 F03	LISTA DE VERIFICACION MANTENIMIENTO PREVENTIVO
3.3.2.P02	MANTENIMIENTO CORRECTIVO DE EQUIPOS DE COMUNICACIONES E INFORMATICA
3.3.2.P02 F01	MANTENIMIENTO CORRECTIVO DE EQUIPOS DE COMUNICACIONES E INFORMATICA
3.3.2.P03	COPIA DE SEGURIDAD DEL SISTEMA DGH
3.3.2.P04	COPIA DE SEGURIDAD DEL SISTEMA SAIH
3.3.2.P05	INSTALACION DE LOS MODULOS DEL SISTEMA SAIH

3.3.2.P06	CREACION DE REPORTES DEL SISTEMA DGH
3.3.2.P07	INSTALACION Y CREACION DE USUARIOS DE DGH
3.3.2.P07 F01	RECEPCIÓN DE SERVICIO DE SISTEMAS
3.3.2.P08	RECUPERACIÓN DE DATOS DEL SISTEMA DGH
3.3.2.P09	BAJA DE SOFTWARE
3.3.2.P10	ENTREGA O CAMBIO DE EQUIPOS TECNOLOGICOS
3.3.2.P11	DILIGENCIAMIENTO DE LA HOJA DE VIDA DE LOS EQUIPOS TECNOLOGICOS
3.3.2.P12	ADMINISTRACIÓN DEL ANTIVIRUS
3.3.2.P13	CONTROL EN LA RED LAN E INTERNET POR UTM
3.3.2.P14	MANTENIMIENTO PREVENTIVO AL SISTEMA DGH
3.3.2.P15	REGISTRO DE USUARIOS Y ASIGNACIÓN DE PERMISOS EN EL SISTEMA DGH
3.3.2.P16	MANTENIMIENTO CORRECTIVO AL SISTEMA SAIH
3.3.2.P17	REGISTRO DE USUARIOS Y PERMISOS EN EL SISTEMA SAIH
3.3.2.P18	REGISTRO DE USUARIOS Y PERMISOS EN EL SISTEMA SGE
3.3.2.P19	ANALISIS Y DETECCION DE VARIACIONES EN LOS SISTEMAS DE INFORMACION
3.3.2.P19 F01	REGISTRO DE VARIACIONES EN LOS SISTEMAS DE INFORMACION
3.3.2.R01	ADMINISTRACION Y CONTROL DE LICENCIAS

12. Formatos y Registros

- Formato de Auditoria de Seguridad de Redes.
- Registro de Incidentes de Seguridad en Comunicaciones
- Acuerdos de Confidencialidad y No Divulgaciones.

13. Bibliografía

No.	DOCUMENTO
1	International Organization for Standardization. (2013). ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements. ISO.
2	Ministerio de Tecnologías de la Información y las Comunicaciones. (2016). Guía Metodológica de Pruebas de Efectividad. MinTIC.

14. Revisión y aprobación

ÍTEM	ELABORÓ	COORDINADOR	REVISÓ	APROBÓ
Nombre	Darwin Mahecha Niño	Jonathan Garcia Suarez	María Francey López	Pablo Mauricio Zambrano Román
Cargo	Calidad	Líder TIC	Coordinador de Calidad	Subgerente Administrativo
Fecha	Dic. 03 de 2024	Dic. 03 DE 2024	Dic. 03 de 2024	Dic. 03 de 2024

15. Control de Cambios al Documento

Fecha del Cambio	Versión Actual	Justificación del Cambio	Indique el ítem del Documento Donde se Requiere el Cambio	Versión Nueva	Nombre y Cargo de Quien Elaboro el Cambio	Nombre y Cargo de Quien Aprobó el Cambio