EMPRESA SOCIAL DEL ESTADO
HOSPITAL REGIONAL DE CHIQUINQUIRÁ
DEPARTAMENTO DE BOYACÁ

CUMPLIMIENTO DE LOS REQUISITOS LEGALES DE TI

CHIQUINQUIRÁ, DICIEMBRE DE 2024

1. Tabla de Contenido

2. Introducción

El presente protocolo tiene como objetivo establecer los lineamientos necesarios para garantizar el cumplimiento de los requisitos legales, contractuales y de seguridad de la información en la ESE Hospital Regional de Chiquinquirá. Este documento es de aplicación obligatoria para todos los funcionarios y áreas que manejen información sensible, sistemas de información y procesos relacionados con la seguridad de la información.

La necesidad de este protocolo surge de la importancia de proteger la información crítica de la organización, cumplir con las normativas legales y contractuales, y asegurar que los sistemas de información operen de acuerdo con las políticas y procedimientos establecidos. Este protocolo aplica a todas las áreas del hospital, incluyendo sus sedes y servicios externos, y está alineado con los requisitos de la norma ISO/IEC 27001:2013, específicamente en el Anexo A.18 (Cumplimiento).

3. Identificación

PROCESO	**GESTION DE RECURSOS LOGISTICOS**
SUBPROCESO	Tecnologías de la Información y las Comunicaciones
OBJETIVO GENERAL	Establecer y mantener un sistema de gestión que garantice el cumplimiento de los requisitos legales, contractuales y de seguridad de la información en la ESE Hospital Regional de Chiquinquirá.
OBJETIVOS ESPECÍFICOS	➢ Identificar y documentar los requisitos legales, reglamentarios y contractuales aplicables. ➢ Implementar controles para proteger la información y los registros de la organización. ➢ Realizar revisiones periódicas para asegurar el cumplimiento con las políticas y normativas de seguridad.
ALCANCE	Este protocolo aplica a todas las áreas y servicios de la ESE Hospital Regional de Chiquinquirá, incluyendo sus sedes y servicios y cubre todos los sistemas de información y procesos relacionados con la seguridad de la información.

4. Definiciones y Conceptos

Cumplimiento Legal: Conformidad con las leyes, regulaciones y normativas aplicables a la organización.

Cumplimiento Contractual: Adherencia a los acuerdos y cláusulas establecidos en los contratos con terceros.

Seguridad de la Información: Protección de la información contra accesos no autorizados, modificaciones, destrucción o divulgación.

Control Criptográfico: Uso de técnicas de cifrado para proteger la confidencialidad e integridad de la información.

5. Generalidades

El protocolo se basa en los requisitos establecidos en la norma ISO/IEC 27001:2013, específicamente en el Anexo A.18, que aborda el cumplimiento de los requisitos

legales, contractuales y de seguridad de la información. Se deben considerar las siguientes políticas y procedimientos:

- **Identificación de Requisitos Legales y Contractuales:** Se deben identificar y documentar todos los requisitos legales, reglamentarios y contractuales aplicables a la organización.
- **Protección de Registros:** Los registros deben protegerse contra pérdida, destrucción, falsificación y acceso no autorizado.
- **Privacidad de Datos Personales:** Se deben implementar controles para garantizar la privacidad y protección de los datos personales, de acuerdo con la legislación aplicable.
- **Uso de Controles Criptográficos:** Se deben utilizar controles criptográficos para proteger la información sensible, en cumplimiento con las normativas vigentes.

6. Materiales e Insumos Requeridos

- Software de cifrado y controles criptográficos.
- Formatos para la revisión y auditoria de cumplimiento

7. Roles y responsabilidades

ROL	RESPONSABILIDAD
Líder de TI	Supervisar y garantizar el cumplimiento de los requisitos legales y contractuales.
Ingeniero TI	Implementar y mantener los controles criptográficos y de seguridad de la información.
Lideres y Coordinadores de Procesos	Asegurar que los registros y datos personales estén protegidos según las normativas.
Calidad	Realizar revisiones periódicas para verificar el cumplimiento con las políticas.

8. Contenido del Protocolo de Gestión de Continuidad del Negocio

8.1 Identificación de Requisitos Legales y Contractuales (A.18.1.1)

Objetivo: Identificar y documentar todos los requisitos legales, reglamentarios y contractuales aplicables a la organización.

Actividades:

1. **Recopilación de Requisitos:**
   - Realizar un inventario de las leyes, regulaciones y normativas aplicables al sector salud y a la gestión de la información (por ejemplo, Ley de Protección de Datos Personales, normativas de salud, Política de Gobierno Digital, etc.).
   - Revisar los contratos con proveedores, clientes y terceros para identificar cláusulas relacionadas con la seguridad de la información.
2. **Documentación:**
   - Crear un registro centralizado que incluya todos los requisitos identificados, clasificados por tipo (legales, contractuales, reglamentarios).
   - Asignar un responsable para mantener este registro actualizado.
3. **Comunicación:**
   - Informar a todas las áreas de la organización sobre los requisitos aplicables y su responsabilidad en el cumplimiento.
   - Capacitar al personal en los aspectos relevantes de las normativas identificadas.

8.2 Protección de Registros (A.18.1.3)

Objetivo: Proteger los registros de la organización contra pérdida, destrucción, falsificación, acceso no autorizado y liberación no autorizada.

Actividades:

1. **Clasificación de Registros:**
   - Identificar los registros críticos de la organización (historiales médicos, registros financieros, contratos, etc.).
   - Clasificar los registros según su nivel de confidencialidad y criticidad.
2. **Implementación de Controles:**

- Establecer controles de acceso para garantizar que solo el personal autorizado pueda acceder a los registros.
- Implementar medidas de respaldo y recuperación para prevenir la pérdida de registros.
- Utilizar sistemas de cifrado para proteger los registros electrónicos.

3. **Procedimientos de Retención y Disposición:**
   - Definir políticas de retención de registros, alineadas con los requisitos legales y contractuales.
   - Establecer procedimientos seguros para la disposición de registros que ya no sean necesarios (por ejemplo, destrucción física o borrado seguro).

8.3 Privacidad y Protección de Datos Personales (A.18.1.4)

Objetivo: Asegurar la privacidad y protección de los datos personales, de acuerdo con la legislación aplicable.

Actividades:

1. **Identificación de Datos Personales:**
   - Identificar los datos personales que maneja la organización (por ejemplo, datos de pacientes, empleados, proveedores).
   - Clasificar los datos según su sensibilidad y nivel de protección requerido.
2. **Implementación de Controles:**
   - Establecer controles de acceso basados en roles para limitar el acceso a los datos personales.
   - Utilizar técnicas de cifrado para proteger los datos personales en tránsito y en reposo.
   - Implementar medidas de anonimización o pseudonimización cuando sea necesario.
3. **Capacitación y Concientización:**
   - Capacitar al personal en la protección de datos personales y en el cumplimiento de las normativas aplicables (por ejemplo, Ley de Protección de Datos).

- Realizar campañas de concientización sobre la importancia de la privacidad y la protección de datos.

8.4 Uso de Controles Criptográficos (A.18.1.5)

Objetivo: Utilizar controles criptográficos para proteger la información sensible, en cumplimiento con las normativas vigentes.

Actividades:

1. **Selección de Controles Criptográficos:**
   - Identificar los tipos de información que requieren protección criptográfica (por ejemplo, datos personales, registros médicos, comunicaciones confidenciales).
   - Seleccionar algoritmos y protocolos de cifrado que cumplan con los estándares internacionales y las normativas locales.
2. **Implementación de Controles:**
   - Configurar sistemas de cifrado para proteger la información en tránsito (por ejemplo, correos electrónicos, transferencias de datos).
   - Implementar soluciones de cifrado para proteger la información almacenada en dispositivos y servidores.
   - Establecer políticas para la gestión segura de claves criptográficas (generación, almacenamiento, rotación y destrucción).
3. **Monitoreo y Auditoría:**
   - Realizar revisiones periódicas para verificar que los controles criptográficos estén funcionando correctamente.
   - Auditar el cumplimiento de las políticas de cifrado y la gestión de claves.

8.5 Revisiones de Seguridad de la Información (A.18.2)

Objetivo: Asegurar que la seguridad de la información se implemente y opere de acuerdo con las políticas y procedimientos organizacionales.

Actividades:

1. **Revisión Independiente (A.18.2.1):**

   - Designar un equipo independiente (interno o externo) para realizar revisiones periódicas del sistema de gestión de seguridad de la información (SGSI).
   - Evaluar la eficacia de los controles implementados y la conformidad con las políticas y normativas.

2. **Revisión de Cumplimiento con Políticas y Normas (A.18.2.2):**

   - Realizar revisiones periódicas para verificar que los procesos y procedimientos de información cumplan con las políticas y normas de seguridad.
   - Documentar los hallazgos y establecer planes de acción para corregir las no conformidades identificadas.

3. **Revisión del Cumplimiento Técnico (A.18.2.3):**

   - Realizar pruebas técnicas para verificar que los sistemas de información cumplan con las políticas y normas de seguridad.
   - Utilizar herramientas de auditoría técnica para identificar vulnerabilidades y brechas de seguridad.

8.6 Plan de Acción y Mejora Continua

Objetivo: Establecer un plan de acción para corregir no conformidades y mejorar continuamente el sistema de gestión de seguridad de la información.

Actividades:

1. **Identificación de No Conformidades:**

   - Documentar todas las no conformidades identificadas durante las revisiones y auditorías.
   - Clasificar las no conformidades según su gravedad y prioridad.

2. **Implementación de Acciones Correctivas:**

   - Desarrollar planes de acción para corregir las no conformidades identificadas.

- Asignar responsables y plazos para la implementación de las acciones correctivas.

3. **Seguimiento y Evaluación:**

- Realizar seguimiento a la implementación de las acciones correctivas.
- Evaluar la eficacia de las acciones implementadas y realizar ajustes si es necesario.

9. Recomendaciones

- Realizar revisiones periódicas para asegurar el cumplimiento con las políticas y normativas.
- Capacitar al personal en temas de seguridad de la información y cumplimiento legal.
- Mantener actualizada la documentación relacionada con los requisitos legales y contractuales.

10. Herramienta y Metodología de Evaluación

Lista de verificación de cumplimiento y realizar auditorías internas trimestrales para verificar el cumplimiento con los requisitos legales, contractuales y de seguridad de la información.

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 Revisión de Cumplimiento.
- Registro de Auditorías Internas.

13. Bibliografía

No.	DOCUMENTO
1	International Organization for Standardization. (2013). ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements. ISO.

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