CONTENIDO

INTRODUCCION

La ESE Hospital Regional Manuela Beltrán Socorro en cumplimiento del marco legal Colombiano relacionado con la protección, seguridad y confidencialidad de la información, en especial el decreto 612 del 2018; además de la iniciativa propia de la empresa de diseñar un marco de referencia para proteger sus activos de información consciente de la vital importancia de los mismos para su funcionamiento, construye el presente Plan de Seguridad y Privacidad de la Información.

1. OBJETIVO DEL PLAN

Definir el conjunto de acciones necesarias para Diseñar, desarrollar e implementar de manera integral, la gestión de los riesgos de seguridad y privacidad de la información, con el objetivo de proteger los activos de información de la institución y garantizar la continuidad del funcionamiento de la plataforma informática.

1.1 Objetivos Específicos

- Disminuir la probabilidad de ocurrencia e impacto de los incidentes de Seguridad y Privacidad de la Información de forma efectiva.
- Establecer los mecanismos de aseguramiento físico y digital, para fortalecer la confidencialidad, integridad, disponibilidad, autenticidad, y privacidad de la información de la ESE Hospital Regional Manuela Beltrán Socorro.
- Asegurar y hacer uso eficiente y seguro de los recursos de Tecnologías de Información y Comunicaciones, así como aquellos equipos biomédicos que almacena información referente a los servicios prestados, con el fin de garantizar la continuidad de la prestación de los servicios.
- Dar cumplimiento a los requisitos legales y normativos en materia de Seguridad y Privacidad de la Información, Seguridad Digital y protección de la información personal.
- Minimizar el riesgo de vulnerabilidad de la información en el desarrollo de los procesos.
- Mantener la confianza de sus clientes internos y externos.
- Asegurar la continuidad de funcionamiento de la plataforma informática
- Cumplir con la legislación nacional e institucional sobre seguridad de la información
- Garantizar la disponibilidad de la información para la eficiente toma de decisiones.
- Fortalecer la cultura de la seguridad de la información a nivel de clientes internos y externos.
- Proteger los activos tecnológicos y apoyar su desarrollo.

2. ALCANCE

Aplica a todos los niveles asistenciales y administrativos de la ESE Hospital Regional Manuela Beltrán Socorro, sus funcionarios, contratistas, proveedores, usuarios, docentes, estudiantes que realicen prácticas, pasantías o trabajos de grado, bajo el marco de un contrato y/o convenio académico y cooperantes, adicionalmente todas aquellas personas o terceros que en razón del cumplimiento de sus funciones y las de la ESE compartan, utilicen, recolecten, procesen, intercambien o consulten su información, así como a los Entes de Control, que accedan ya sea interna, remotamente o vía internet a cualquier tipo de información, independientemente de su ubicación. Así mismo, esta lo dispuesto en este documento y su implementación aplica a toda la información creada, procesada o utilizada por la ESE Hospital Regional Manuela Beltrán Socorro, sin importar el medio, formato, presentación o lugar en el cual se encuentre.

3. DEFINICIONES

Acceso a la Información Pública: *Derecho fundamental consistente en la facultad que* tienen todas las personas de conocer sobre la existencia y acceder a la información pública en posesión o bajo control de sujetos obligados. (Ley 1712 de 2014, art 4)
Activo: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas…) que tenga valor para la organización. (ISO/IEC 27000).
Activo de Información: En relación con la privacidad de la información, se refiere al activo que contiene información pública que el sujeto obligado genere, obtenga, adquiera, transforme o controle en su calidad de tal.
Amenaza: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000).
Auditoría: Proceso sistemático, independiente y documentado para obtener evidencias de auditoria y obviamente para determinar el grado en el que se cumplen los criterios de auditoria. (ISO/IEC 27000).
Antivirus: Software de seguridad que protege un equipo de virus, normalmente a través de la detección en tiempo real y también mediante análisis del sistema, que pone en cuarentena y elimina los virus. El antivirus debe ser parte de una estrategia de seguridad estándar de múltiples niveles.
Ataques Web: Es un ataque que se comete contra una aplicación cliente y se origina desde un lugar en la Web, ya sea desde sitios legítimos atacados o sitios maliciosos que han sido creados para atacar intencionalmente a los usuarios de ésta.
Contraseña: Cadena exclusiva de caracteres que introduce un usuario como código de identificación para restringir el acceso a equipos y archivos confidenciales. El sistema compara el código con una lista de contraseñas y usuarios autorizados
Confidencialidad: Propiedad que determina que la información está disponible ni sea revelada a quien no esté autorizado (2.13 ISO 27000)
Disponibilidad: Propiedad que la información sea accesible y utilizable por solicitud de los autorizados (2.10 ISO 27000) • Integridad: Propiedad de salvaguardar la exactitud y el estado completo de los activos (2.36 ISO 27000).
Encriptación: La encriptación es un método de cifrado o codificación de datos para evitar que los usuarios no autorizados lean o manipulen los datos. Sólo los individuos con acceso a una contraseña o clave pueden descifrar y utilizar los datos.
Firewall: Es una aplicación de seguridad física y/o lógica diseñada para bloquear las conexiones en determinados puertos del sistema, independientemente de si el tráfico es benigno o maligno. Un firewall debería formar parte de una estrategia de seguridad estándar de múltiples niveles.
Malware: Es la descripción general de un programa informático que tiene efectos no deseados o maliciosos. Incluye virus, gusanos, troyanos y puertas traseras.
Plan de tratamiento de Gestión de Riesgos: Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma. (ISO/IEC 27000).
Privacidad: En el contexto de este documento, por privacidad se entiende el derecho que tienen todos los titulares de la información en relación con la información que involucre datos personales y la información clasificada que estos hayan entregado o esté

en poder de la entidad en el marco de las funciones que a ella le compete realizar y que generan en las entidades destinatarias del Manual de GEL la correlativa obligación
Procedimiento: Sucesión cronológica de acciones concatenadas entre sí, para la realización de una actividad o tarea específica dentro del ámbito de los controles de Seguridad de la Información.
Riesgo: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).
Seguridad de la información: Preservación de la confidencialidad, integridad, y disponibilidad de la información. (ISO/IEC 27000).
Sistema de detección de intrusos: Es un servicio que monitorea y analiza los eventos del sistema para encontrar y proporcionar en tiempo real o casi real advertencias de intentos de acceso a los recursos del sistema de manera no autorizada. Es la detección de ataques o intentos de intrusión, que consiste en revisar registros u otra información disponible en la red.
Virus: Programa informático escrito para alterar la forma como funciona una computadora, sin permiso o conocimiento del usuario.
Vulnerabilidad: Es un estado viciado en un sistema informático (o conjunto de sistemas) que afecta las propiedades de confidencialidad, integridad y disponibilidad de los sistemas.

4. DOCUMENTOS DE REFERENCIA

Decreto 1078 de 2015 – MINISTERIO DE LAS TECNOLOGIAS DE LA INFORMACION Y COMUNICACIONES
Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.

NTC / ISO 27001:2013 - ICONTEC
Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información (SGSI). Requisitos.

NTC/ISO 27002:2013- ICONTEC
Tecnología de la información. Técnicas de seguridad. Código de Práctica para controles de seguridad de la información.

Ley 1266 de 2008
“Por la cual se dictan disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países”.

Ley 1273 de 2009
“Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.”

Ley 1581 de 2012
“Por la cual se dictan disposiciones generales para la protección de datos personales.”

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.”

Ley 1978 de 2019
“Por la cual se moderniza el sector de las Tecnologías de la Información y las Comunicaciones TIC, se distribuyen competencias, se crea un regulador único y se dictan otras disposiciones.”

Resolución 232 del 2015 – ESE Hospital Regional Manuela Beltrán Socorro
Por medio de la cual se adopta ley de protección de datos para usuarios de la ESE Hospital Regional Manuela Beltrán Socorro.
Resolución 355 del 2016 – ESE Hospital Regional Manuela Beltrán Socorro
Por medio de la cual se adopta la Política de Comunicaciones de la ESE Hospital Regional Manuela Beltrán Socorro.
Resolución 095 del 2018 – ESE Hospital Regional Manuela Beltrán Socorro

Por medio del cual se aprueba y expide la política para la Definición de políticas y niveles de acceso a la plataforma Informática de la ESE Hospital Regional Manuela Beltrán Socorro.

Resolución 045 del 2019 – ESE Hospital Regional Manuela Beltrán Socorro

Por medio del cual se aprueba el plan de gestión de riesgos plataforma informática de la ESE Hospital Regional Manuela Beltrán Socorro.

Resolución 166 del 2020 – ESE Hospital Regional Manuela Beltrán Socorro

Por medio del cual se establece la política de seguridad y privacidad de la información en la E.S.E Hospital Regional Manuela Beltrán Socorro.

Acuerdo 028 del 2009 – ESE Hospital Regional Manuela Beltrán Socorro

Por medio del cual se establece el Reglamento sobre las políticas para el uso de los servicios de Tecnologías de la Información y Comunicación ofrecidos por la E.S.E Hospital Regional Manuela Beltrán Socorro.

Acuerdo 007 del 2015 – ESE Hospital Regional Manuela Beltrán Socorro

Por medio del cual se realizan modificaciones al acuerdo 028 del 2009.

5. POLITICAS

En el Artículo 6 de la resolución 166 del 2020, ya se tienen definidas las políticas básicas para la seguridad y privacidad de la información, las cuáles se mencionan a continuación:

"La E.S.E. Hospital Regional Manuela Beltrán ha decidido definir, implementar, operar y mejorar de forma continua un Sistema de Gestión de Seguridad de la Información, soportado en lineamientos claros alineados a las necesidades del negocio, y a los requerimientos regulatorios que le aplican a su naturaleza.

- Las responsabilidades frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de los empleados, contratistas o terceros.
- La ESE Hospital Regional Manuela Beltrán protegerá la información generada, procesada o resguardada por los procesos de negocio y activos de información que hacen parte de los mismos.
- La ESE Hospital Regional Manuela Beltrán protegerá la información creada, procesada, transmitida o resguardada por sus procesos de negocio, con el fin de minimizar impactos financieros, operativos o legales debido a un uso incorrecto de esta. Para ello es fundamental la aplicación de controles de acuerdo con la clasificación de la información de su propiedad o en custodia.
- La ESE Hospital Regional Manuela Beltrán protegerá su información de las amenazas originadas por parte del personal.
- La ESE Hospital Regional Manuela Beltrán protegerá las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.
- La ESE Hospital Regional Manuela Beltrán controlará la operación de sus procesos de negocio garantizando la seguridad de los recursos tecnológicos y las redes de datos.
- La ESE Hospital Regional Manuela Beltrán implementará control de acceso a la información, sistemas y recursos de red.
- La ESE Hospital Regional Manuela Beltrán garantizará que la seguridad sea parte integral del ciclo de vida de los sistemas de información.
- La ESE Hospital Regional Manuela Beltrán garantizará a través de una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información una mejora efectiva de su modelo de seguridad.
- La ESE Hospital Regional Manuela Beltrán garantizará la disponibilidad de sus procesos de negocio y la continuidad de su operación basada en el impacto que pueden generar los eventos.
- La ESE Hospital Regional Manuela Beltrán Socorro garantizará el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas."

6. ACTIVIDADES A DESARROLLAR

6.1. FASE I: ANÁLISIS DE BRECHA

Actualización del plan de Gestión de Riesgos Informáticos.

Elaborar el análisis GAP (análisis de brecha) frente a la norma ISO 27000 y el Modelo de seguridad y privacidad de la información MSPI de la ESE Hospital Regional Manuela Beltrán Socorro.

6.2. FASE II: ESTABLECIMIENTO DEL SGSI

Diseñar políticas y procedimientos de seguridad conforme la estructura propuesta por la norma ISO 27000 alineados al Sistema Integrado de Gestión de la Entidad.

Realizar jornadas de capacitación y sensibilización sobre seguridad informática.

Determinar la estructura y ubicación en el organigrama institucional de la función de seguridad de la información ajustada al contexto interno de la ESE Hospital Regional Manuela Beltrán Socorro y teniendo en cuenta sus necesidades.

Fortalecimiento de la infraestructura tecnológica de seguridad digital.

Implementar formalmente el proceso de gestión de incidentes del SGSI

Crear, definir e implementar los indicadores (métricas) adecuados para medir la madurez, eficiencia, eficacia, implantación o impacto de controles de seguridad de la información Se deberá tener como referencia la norma ISO 27004:2016

6.3. CRONOGRAMA DESARROLLO

	Producto	Fecha Inicio	Fecha Final
Fase 1	Actualización Plan de Gestión de Riesgos	01/01/2023	30/06/2023
	Análisis GAP	01/03/2023	31/12/2023
Fase 2	Diseñar políticas y procedimientos de seguridad conforme la estructura propuesta por la norma ISO 27000 alineados al Sistema Integrado de Gestión de la Entidad. Realizar jornadas de capacitación y sensibilización sobre seguridad informática. Determinar la estructura y ubicación en el organigrama institucional de la función de	01/01/2023	31/12/2024

	seguridad de la información ajustada al contexto interno de la ESE Hospital Regional Manuela Beltrán Socorro y teniendo en cuenta sus necesidades. Fortalecimiento de la infraestructura tecnológica de seguridad digital. Implementar formalmente el proceso de gestión de incidentes del SGSI Crear, definir e implementar los indicadores (métricas) adecuados para medir la madurez, eficiencia, eficacia, implantación o impacto de controles de seguridad de la información Se deberá tener como referencia la norma ISO 27004:2016		