PROCESO GESTIÓN DE SISTEMAS INFORMÁTICOS

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Hospital San Juan Bautista E.S.E
Chaparral – Tolima

Dependencia: Gestión de Recursos Financieros y Físicos

Vigencia 2021

TABLA DE CONTENIDO

1. OBJETIVO

Describir las actividades del plan de Seguridad y Privacidad de la información del Hospital San Juan Bautista E.S.E. basados en los lineamientos de buenas prácticas de tratamiento de la información y modelo de seguridad del Ministerio de las TIC´s.

2. ALCANCE

El plan de Seguridad y Privacidad de la Información se aplica a todos los procesos y funcionarios, Contratistas, terceros que tienen relación alguna o hacen parte del hospital San Juan Bautista E.S.E.

3. TERMINOS Y 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/IEC27000).

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.

Archivo: Conjunto de documentos, sea cual fuere su fecha, forma y soporte material, acumulados en un proceso natural por una persona o entidad pública o privada, en el transcurso de su gestión, conservados respetando aquel orden para servir como testimonio e información a la persona o institución que los produce y a los ciudadanos, o como fuentes de la historia. También se puede entender como la institución que está al servicio de la Gestión administrativa, la información, la investigación y la cultura. (Ley 594 de 2000, art 3)

Amenazas: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000).

Análisis de Riesgo: Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo. (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).

Autorización: Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales (Ley 1581 de 2012, art 3)

Bases de Datos Personales: Conjunto organizado de datos personales que sea objeto de Tratamiento (Ley 1581 de 2012, art 3).

Ciberseguridad: Capacidad del Estado para minimizar el nivel de riesgo al que están expuestos los ciudadanos, ante amenazas o incidentes de naturaleza cibernética. (CONPES 3701).

Ciberespacio: Es el ambiente tanto físico como virtual compuesto por computadores, sistemas computacionales, programas computacionales (software), redes de telecomunicaciones, datos e información que es utilizado para la interacción entre usuarios. (Resolución CRC 2258 de 2009).

Control: Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.

Datos Abiertos: Son todos aquellos datos primarios o sin procesar, que se encuentran en formatos estándar e interoperables que facilitan su acceso y reutilización, los cuales están bajo la custodia de las entidades públicas o privadas que cumplen con funciones públicas y que son puestos a disposición de cualquier ciudadano, de forma libre y sin restricciones, con el fin de que terceros puedan reutilizarlos y crear servicios derivados de los mismos (Ley 1712 de 2014, art 6)

Datos Personales: Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. (Ley 1581 de 2012, art 3).

Datos Personales Públicos: Es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva. (Decreto 1377 de 2013, art 3)

Datos Personales Privados: Es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular. (Ley 1581 de 2012, art 3 literal h).

Datos Personales Mixtos: Para efectos de esta guía es la información que contiene datos personales públicos junto con datos privados o sensibles.

Datos Personales Sensibles: Se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos. (Decreto 1377 de 2013, art 3)

Declaración de aplicabilidad: Documento que enumera los controles aplicados por el Sistema de Gestión de Seguridad de la Información – SGSI, de la organización tras el resultado de los procesos de evaluación y tratamiento de riesgos y su justificación, así como la justificación de las exclusiones de controles del anexo A de ISO 27001. (ISO/IEC 27000).

Derecho a la Intimidad: Derecho fundamental cuyo núcleo esencial lo constituye la existencia goce de una órbita reservada en cada persona, exenta de la intervención del poder del Estado o de las intromisiones arbitrarias de la sociedad, que le permite a dicho individuo el pleno desarrollo de su vida personal, espiritual y cultural (Jurisprudencia Corte Constitucional).

Encargado del Tratamiento de Datos: Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del responsable del Tratamiento. (Ley 1581 de 2012, art 3)

Gestión de incidentes de seguridad de la información: Procesos para Detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información. (ISO/IEC 27000).

Información Pública Clasificada: Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una

persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6)

Información Pública Reservada: Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6)

Ley de Habeas Data: Se refiere a la Ley Estatutaria 1266 de 2008.

4. MARCO NORMATIVO

- Anexo 1 - Resolución 3564 de 2015 - Reglamenta aspectos relacionados con la Ley de Transparencia y Acceso a la Información Pública.
- Decreto Reglamentario Único 1081 de 2015 - Reglamento sobre la gestión de la información pública.
- Título 9 - Decreto 1078 de 2015 - Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
- Ley 1712 de 2014 - Ley de Transparencia y acceso a la información pública.
- Ley 57 de 1985 -Publicidad de los actos y documentos oficiales.
- Ley 594 de 2000 - Ley General de Archivos.
- Título 9 - Decreto 1078 de 2015 - Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
- Título 9 - Decreto 1078 de 2015 - Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
- Ley Estatutaria 1757 de 2015 - Promoción y protección del derecho a la participación democrática.
- Ley estatutaria 1618 de 2013: Ejercicio pleno de las personas con discapacidad.
- Ley 1437 de 2011: Código de Procedimiento Administrativo y de lo Contencioso Administrativo.
- Acuerdo 03 de 2015 del Archivo General de la Nación Lineamientos generales sobre la gestión de documentos electrónicos.
- Decreto 019 de 2012 - Suprimir o reformar regulaciones, procedimientos y trámites innecesarios existentes en la Administración Pública.
- Decreto 2364 de 2012 - Firma electrónica.

- Ley 962 de 2005 - Racionalización de trámites y procedimientos administrativos procedimientos administrativos.

- Decreto 1747 de 2000 - Entidades de certificación, los certificados y las firmas digitales.

- Ley 527 de 1999 - Ley de Comercio Electrónico.

- Decreto Ley 2150 de 1995 - Suprimen y reforman regulaciones, procedimientos o trámites innecesarios existentes en la Administración Pública.

- Ley Estatutaria 1581 de 2012 - Protección de datos personales.

- Ley 1266 de 2008 - Disposiciones generales de habeas data y se regula el manejo de la información.

5. POLITICA DE TRATAMIENTO DE LA INFORMACION

El HOSPITAL SAN JUAN BAUTISTA E.S.E., en cumplimiento de la ley estatutaria 1581 de 2012 y su decreto reglamentario 1377 de 2013, sobre la privacidad y protección de datos personales en Colombia, asegura el manejo adecuado de la información que obtenga, registra, use, transmita y actualice mediante la autorización previa, expresa y voluntaria del titular de la información y actúa como responsable del tratamiento y custodia de los datos personales que por virtud de sus funciones y competencias legales establecidas le han sido suministradas a la entidad, con los cuales tiene, ha tenido o espera tener algún tipo de relación, cualquiera sea su naturaleza (Civil, Comercial y/o Laboral etc.), incluyendo pero sin limitarse, los grupos de interés (usuarios directos, usuarios indirectos, terceros relacionados y entidades externas).

En virtud de los procesos misionales y administrativos del Hospital San Juan Bautista E.S.E, enmarcados en los modelos de atención tratamientos médicos, se compromete que la información recolectada, almacenada, usada, transferida o eliminada tendrá los procesos adecuados y documentados con las descripciones de acuerdo a las finalidades para las cuales la información es recolectada y una explicación sobre la necesidad de recolectar los datos en cada caso que establezca la ley y normatividad vigente.

6. OBJETIVOS DEL SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION

- Adoptar Modelo de Seguridad y Privacidad de la información MSPI de acuerdo con los lineamientos de la Política de Gobierno Digital para la implementación del Sistema de Gestión de Seguridad de la Información SGSI.
- Implementar el SGSI y fortalecer los controles de protección de los activos de la información.
- Minimizar los riesgos de seguridad de la información mediante la ejecución de las políticas de seguridad.
- Garantizar la Seguridad, Confidencialidad y Disponibilidad de la información de acuerdo con el SGSI y normas vigentes que lo reglamente.
- Prevenir y controlar los incidentes de seguridad de la información.
- Construir una cultura en seguridad de la información en los procesos misionales, administrativos y financieros de la E.S.E.

- Mejorar continuamente el SGSI, mediante las acciones de mejoras y lecciones aprendidas en la ejecución de la política de gobierno digital.

7. ALCANCE DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE INFORMACIÓN – SGSI

Aplicable a todos los activos de información, talento humano de los procesos misionales, técnicos, administrativos, Financieros de Apoyo y demás, verificando y ajustándolo a la Institución, comprende las políticas, procedimientos y controles para la preservación de confidencialidad, integridad y disponibilidad de la información, en concordancia con la declaración de aplicabilidad avalada por el Comité de Seguridad de la Información o política de tratamiento de datos.

8. COMITÉ DE SEGURIDAD DE LA INFORMACIÓN

Teniendo en cuenta que el Modelo Integrado de Planeación y Gestión MPIG, permite la integración de todos los procesos, planes y orientación de Misional y de apoyo de la Institución se nombra como integrantes del Comité De Seguridad de la Información a los integrantes del Comité de gestión y Desempeño, sus integrantes son las personas que tienen los siguientes cargos:

- Gerente o su delegado, quien lo presidirá.
- Profesional Universitario del área Financiera.
- Profesional Universitario área de Personal.
- Coordinador Área Asistencial.
- Coordinador Área de Sistemas de Información.
- Coordinador área de Calidad.
- Contador.
- Asesor Jurídico.
- Asesor de planeación.
- Invitados: Control Interno; quien tendrán voz, pero no voto.

Las funciones del Comité de Seguridad de la Información son:

- Impulsar la implementación del Sistema de Gestión de Seguridad de la Información SGSI en la E.S.E.
- Realizar el seguimiento y/o verificación de la implementación de los requisitos, controles e indicadores del Sistema de Gestión de Seguridad de la Información SGSI de los procesos institucionales de la E.S.E.
- Supervisar la integración del Sistema de Gestión de Seguridad de la Información - SGSI con el Sistema Integrado de Gestión de la Información.
- Aprobar las medidas y Políticas de Seguridad de la Información y sus modificaciones, en relación con los activos de la información para la presidencia de la República.
- Adoptar las medidas y acciones a que haya lugar, de conformidad con los resultados de los diagnósticos de la seguridad de la información para la E.S.E, con el fin de tomar y establecer las medidas necesarias.
- Establecer mecanismos necesarios para prevenir situaciones de riesgo o incidentes de seguridad física o virtual que puedan generar pérdidas patrimoniales o afectar los recursos de Información de la entidad.
- Aprobar el uso de metodologías específicas para garantizar confiabilidad, disponibilidad e integridad de la seguridad de la información.
- Revisar y aprobar los proyectos de seguridad de la información y servir de facilitadores para su implementación.

- Recomendar la investigación de los incidentes de seguridad de la información ante las instancias necesarias cuando haya lugar a ello.
- Evaluar los planes de acción para mitigar y/o eliminar riesgos en seguridad de la información.
- Alinear sus acciones y decisiones a la normatividad vigente en materia de tecnologías y seguridad de la información.
- Las demás funciones inherentes a la naturaleza del Comité.

9. ACTIVIDADES DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Las actividades a realizar se definen de acuerdo al instrumento de Evaluación del Modelo de Seguridad y Privacidad de la Información MSPI de MINTIC en su componente de Planificación e Implementación y serán aplicadas a la vigencia 2021 de acuerdo con el Plan de Acción Institucional.

Nombre	Descripción	Calculo	Meta	Frec. Medición
AD.1. POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	Hace referencia a prácticas de Ciberseguridad NIST de las áreas Administrativas.	Número de Actividades del Ítem / Numero de actividades Realizadas	30%	Semestral
A2. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	Hace referencia a prácticas de Ciberseguridad NIST de las áreas Administrativas.	Número de Actividades del Ítem / Numero de actividades Realizadas	30%	Semestral
AD.3. SEGURIDAD DE LOS RECURSOS HUMANOS	Hace referencia a prácticas de Ciberseguridad NIST de las áreas Administrativas.	Número de Actividades del Ítem / Numero de actividades Realizadas	30%	Semestral
AD.4. GESTIÓN DE ACTIVOS	Hace referencia a prácticas de Ciberseguridad NIST de las áreas Administrativas.	Número de Actividades del Ítem / Numero de actividades Realizadas	30%	Semestral
T.1. CONTROL DE ACCESO	Hace referencia a prácticas de Ciberseguridad NIST de las áreas Técnicas.	Número de Actividades del Ítem / Numero de actividades Realizadas.	40%	Semestral
T.3. SEGURIDAD FÍSICA Y DEL ENTORNO	Hace referencia a prácticas de Ciberseguridad NIST de las áreas Técnicas.	Número de Actividades del Ítem / Numero de actividades Realizadas.	40%	Semestral

T.4. SEGURIDAD DE LAS OPERACIONES	Hace referencia a prácticas de Ciberseguridad NIST de las áreas Técnicas.	Número de Actividades del Ítem / Numero de actividades Realizadas.	40%	Semestral

10. REQUISITOS TÉCNICOS

- Norma Técnica Colombiana NTC/ISO 27001:2013 Sistemas de gestión de la seguridad de la información.
- Modelo de Seguridad y Privacidad de la Información, Ministerio de Tecnologías y Sistemas de Información.

11. DOCUMENTOS ASOCIADOS

CÓDIGO	TITULO
PE-PE-MIPG-PL6	Plan Estratégico de Tecnologías de la Información - PETI
PE-PE-MIPG-PL7	Plan de Tratamiento de Riesgo de Seguridad y Privacidad de la Información.
Articles-5482 MINTIC	Instrumento Evaluación MSPI MINTIC
PA-GSI-ARI-M1 (V1)	Manual Políticas de Seguridad y Privacidad

12. BITÁCORA DE ACTUALIZACIÓN

Número	Fecha Aprobación	Ítem Alterado	Motivo	Realizado por
01	06-06-2018	Todas	Aprobación inicial	Técnico Administrativo Sistemas
02	28-01-2019	Todas	Actualización	Técnico Administrativo Sistemas
03	23-01-2012	6. Objetivos Del Sistema De Gestión De Seguridad De La Información 9. Actividades De Seguridad Y Privacidad De La Información	Actualización	Técnico Administrativo Sistemas
04		9. Actividades De Seguridad Y Privacidad De La Información	Actualización	Técnico Administrativo Sistemas