Empresa Social Del Estado Hospital San Vicente De Paul

Municipio De Caldas- Antioquia

Plan de Seguridad y Privacidad de la Información

Contiene:

- Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información

2021

Elaborado por

Diana Isabel Posada Villada

Líder de Sistemas

Aprobado por

José David Vélez González

Gerente

Caldas- Antioquia

Enero – 2021

Índice

1. Introducción 3
2. Objetivos 3
   2.2 Objetivo General 3
   2.2 Objetivos Específicos 4
3. Marco legal 5
4. Alcance 5
5. Responsables 6
6. Definiciones 6
7. Desarrollo 14
   7.1 Metodología 14
   7.2 Estructura 14
   7.3 Descripción del plan 14
8. Bibliografía 15
9. Control de cambios 16
10. Anexos 16

1. Introducción

La ESE San Vicente de Paul de Caldas como Entidad Gubernamental está en la obligación de cumplir con la política de gobierno digital impuesta en el decreto No. 1008 del 14 de junio 2018 que tiene como foco el principio donde se tiene como prioridad la seguridad de la información, el cual dice textualmente: “Este principio busca crear condiciones de uso confiable en el entorno digital, mediante un enfoque basado en la gestión de riesgos, preservando la confidencialidad, integridad y disponibilidad de la información de las entidades estatales, y de los servicios que prestan al ciudadano”.

Para la realización del documento se tomará como base los lineamientos de seguridad de la información establecidos por la política de seguridad digital de junio de 2018. La ESE Hospital San Vicente de Paul de Caldas Antioquia se guiará bajo los lineamientos normativos de la NTC/ISO 27001:2013; que proporciona un esquema para la gestión de riesgos y las mejores prácticas, buscando mejorar el desempeño y la capacidad de prestar un servicio que responsa a las necesidades y expectativas de las partes interesadas.

2. Objetivos

2.2 Objetivo General

Definir un Plan estratégico de Seguridad de la Información (PESI) y plan de tratamiento de riesgos de seguridad y privacidad de la Información (MSPI) liderados por la Dirección de Informática de la ESE Hospital San Vicente de Paul de Caldas Antioquia, durante la vigencia 2021, que responda a las necesidades de preservar la confidencialidad, la integridad y la disponibilidad sobre los activos de información.

2.2 Objetivos Específicos

2.2.1 Comunicar e implementar la Estrategia de Seguridad de la Información.

2.2.2 Calificar el nivel de madurez en la gestión de la seguridad de la información.

2.2.3 Implementar y apropiar el Modelo de Privacidad y Seguridad de la Información MPSI, con el objetivo de proteger la información y los sistemas de información, de acceso, uso, divulgación, interrupción o destrucción no autorizada.

2.2.4 Hacer uso eficiente de los recursos de TI (Humano, Físico, Financiero, Tecnológico, etc.) para garantizar la continuidad en la prestación de los servicios.

2.2.5 Definir las responsabilidades relacionadas con el manejo de la seguridad.

2.2.6 Establecer una metodología de gestión de seguridad de la información clara y estructurada.

2.2.7 Reducir el riesgo de pérdida, robo o corrupción de información.

2.2.8 Garantizar que los usuarios tengan acceso a la información a través de medidas de seguridad que garanticen la confidencialidad, integridad y disponibilidad de esta.

2.2.9 Cumplir con la legislación vigente sobre información personal, propiedad intelectual y otras.

2.2.10 Optimizar la seguridad de la información con base en la gestión de procesos.

3. Marco legal

Título de la norma o documento	Descripción
Constitución política de Colombia	Constitución política de Colombia 1991
Ley 80 de 1983	Estatuto general de contratación de administración pública
Ordenanza Plan Departamental de Desarrollo de Antioquia 2016-2019	Plan departamental de desarrollo de Antioquia 2016-2019
Ley 594 de 2000	Ley de archivos – gestión documental
Ley 1581 de 2012	Ley de protección de datos personales
Ley 1712 de 2014	Ley de transparencia
Ley 1150 de 2007	Disposiciones generales sobre contratación con recursos públicos
Ley 1273 de 2009	Protección de la información y de los datos
Ley 1341 de 2009	Principios y conceptos sobre la sociedad de la información y las comunicaciones TIC, se crea la agencia nacional de espectro y se dictan otras disposiciones
Ley 23 de 1982	Derechos de autor
Decreto 1008 de 2018	Lineamientos generales de la estrategia de Gobierno Digital
Directiva Presidencial 04 de 2012 – cero papeles	Eficiencia administrativa y lineamientos de la política de cero papeles en la administración pública
Decreto 1078 de 2015 – reglamento TIC	Reglamento del sector de las tecnologías de la información y comunicaciones
Ley 1266 de 2008	Habeas data
Ley 1928 de 2018	Convenio sobre la ciberdelincuencia
Ley 527 de 1999	Acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones.
CONPES 3584	Política de seguridad digital
CONPES 3701	Lineamientos de política para ciberseguridad y ciberdefensa
CONPES 3854	Política Nacional de Seguridad Digital

4. Alcance

El Plan estratégico de Seguridad de la Información (PESI) y plan de tratamiento de riesgos de seguridad y privacidad de la Información (MSPI) aplica a todos los procesos de la institución los cuales manejen, procesen o interactúen con información institucional.

La institución acorde con su naturaleza jurídica, misión y visión, encontró aplicables todos los requisitos de la NTC/ISO 27001:2013 y todos los controles del Anexo A.

5. Responsables

Líder de Sistemas
Gerente

6. Definiciones

- **Acción Correctiva:** Acción para eliminar la causa de una no conformidad y prevenir su repetición. Va más allá de la simple corrección.

- **Acción preventiva:** Medida de tipo proactivo orientada a prevenir potenciales no conformidades.

- **Aceptación del riesgo:** Decisión informada de asumir un riesgo concreto.

- **Activo:** En relación con seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de esta (sistemas, soportes, edificios, personas, etc.) que tengan valor para la organización.

- **Alcance:** Ámbito de la organización que queda sometido al SGSI.

- **Amenaza:** Causa potencial de un incidente no deseado, puede provocar daños a un sistema o a la organización.

- **Análisis de riesgos:** Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo

- **Autenticidad**: Propiedad de que una entidad es lo que afirma ser.

- **CIA: Véase:** CID. Acrónimo inglés de Confidentiality, Integrity y Availability, las dimensiones básicas de la seguridad de la información.

- **CID: (inglés: CIA).** Acrónimo español de Confidencialidad, Integridad y Disponibilidad, las dimensiones básicas de la seguridad de la información.

- **COBIT:** Control Objectives for Information and related Technology. Publicados y mantenidos por ISACA. Su misión es investigar, desarrollar, publicar y promover un conjunto de objetivos de control de tecnología de información rectores, actualizados, internacional y generalmente aceptados para ser empleados por gerentes de empresas y auditores.

- **Compromiso de la Dirección:** (inglés: Management commitment). Alineamiento firme de la Dirección de la organización con el establecimiento, implementación, operación, monitorización, revisión, mantenimiento y mejora del SGSI. La versión de 2013 de ISO 27001 lo engloba bajo la cláusula de Liderazgo.

- **Confidencialidad:** (inglés: Confidentiality). Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados. 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.

- **Control correctivo:** Control que corrige un riesgo, error, omisión o acto deliberado antes de que produzca pérdidas relevantes. Supone que la amenaza ya se ha materializado pero que se corrige.
- **Control detectivo:** Control que detecta la aparición de un riesgo, error, omisión o acto deliberado. Supone que la amenaza ya se ha materializado, pero por sí mismo no la corrige.

- **Control disuasorio:** Control que reduce la posibilidad de materialización de una amenaza, p.ej., por medio de avisos o de medidas que llevan al atacante a desistir de su intención.

- **Control preventivo:** Control que evita que se produzca un riesgo, error, omisión o acto deliberado. Impide que una amenaza llegue siquiera a materializarse.

- **Corrección:** Acción para eliminar una No Conformidad detectada. Si lo que se elimina es la causa de la no conformidad, véase acción correctiva.

- **Cuadro de Mando Integral:** es un modelo de gestión que traduce la estrategia en objetivos relacionados entre sí, medidos a través de indicadores y ligados a unos planes de acción que permiten alinear el comportamiento de los miembros de la organización con la estrategia de la empresa.

- **Declaración de aplicabilidad:** SOA Documento que enumera los controles aplicados por el 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.

- **Desastre:** Cualquier evento accidental, natural o malintencionado que interrumpe las operaciones o servicios habituales de una organización durante el tiempo suficiente como para verse la misma afectada de manera significativa.

- **Directiva o directriz:** Una descripción que clarifica qué debería ser hecho y cómo, con el propósito de alcanzar los objetivos establecidos en las políticas. Disponibilidad: (inglés: Availability). Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada.

- **Estimación de riesgos:** Proceso de comparar los resultados del análisis de riesgos con los criterios de riesgo para determinar si el riesgo y/o su magnitud es aceptable o tolerable.

- **Evaluación de riesgos:** Proceso global de identificación, análisis y estimación de riesgos. Evidencia objetiva: Información, registro o declaración de hechos, cualitativa o cuantitativa, verificable y basada en observación, medida o test, sobre aspectos relacionados con la confidencialidad, integridad o disponibilidad de un proceso o servicio o con la existencia e implementación de un elemento del sistema de gestión de seguridad de la información.

- **Gestión de claves**: Controles referidos a la gestión de claves criptográficas.

- **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.

- **Gestión de riesgos:** Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo. Se compone de la evaluación y el tratamiento de riesgos.

- **Identificación de riesgos:** (inglés: Risk identification). Proceso de encontrar, reconocer y describir riesgos.

- I**ncidente de seguridad de la información:** (inglés: Information security incident). Evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

- **Integridad:** Propiedad de la información relativa a su exactitud y completitud.

- **Inventario de activos:** Lista de todos aquellos recursos (físicos, de información, software, documentos, servicios, personas, intangibles, etc.) dentro del alcance del SGSI, que tengan valor para la organización y necesiten por tanto ser protegidos de potenciales riesgos.

- **ISO:** Organización Internacional de Normalización, con sede en Ginebra (Suiza). Es una agrupación de entidades nacionales de normalización cuyo objetivo es establecer, promocionar y gestionar estándares (normas).

- **ISO 17799:** Código de buenas prácticas en gestión de la seguridad de la información adoptado por ISO transcribiendo la primera parte de BS7799. Dio lugar a ISO 27002, por cambio de nomenclatura, el 1 de Julio de 2007. Ya no está en vigor.

- **ISO 19011:** "Guidelines for auditing management systems". Norma con directrices para la auditoría de sistemas de gestión. Guía de utilidad para el desarrollo, ejecución y mejora del programa de auditoría interna de un SGSI.

- **ISO/IEC 27001:** Norma que establece los requisitos para un sistema de gestión de la seguridad de la información (SGSI). Primera publicación en 2005; segunda edición en 2013. Es la norma en base a la cual se certifican los SGSI a nivel mundial.

- **ISO/IEC 27002:** Código de buenas prácticas en gestión de la seguridad de la información. Primera publicación en 2005; segunda edición en 2013. No es certificable.

- **ITIL**: IT Infrastructure Library. Un marco de gestión de los servicios de tecnologías de la información.

- **NIST: (**National Institute of Standards and Technology), Agencia de la Administración de Tecnología del Departamento de Comercio de los Estados Unidos. La misión de este instituto es promover la innovación y la competencia

industrial en Estados Unidos mediante avances en metrología, normas y tecnología de forma que mejoren la estabilidad económica y la calidad de vida.

- **No conformidad**: (inglés: Nonconformity). Incumplimiento de un requisito. No repudio: Según [CCN-STIC-405:2006]: El no repudio o irrenunciabilidad es un servicio de seguridad que permite probar la participación de las partes en una comunicación. Según [OSI ISO-7498-2]: Servicio de seguridad que previene que un emisor niegue haber remitido un mensaje (cuando realmente lo ha emitido) y que un receptor niegue su recepción (cuando realmente lo ha recibido).

- **Parte interesada:** (inglés: Interested party / Stakeholder). Persona u organización que puede afectar a, ser afectada por o percibirse a sí misma como afectada por una decisión o actividad.

- **PDCA**: Plan-Do-Check-Act. Modelo de proceso basado en un ciclo continuo de las actividades de planificar (establecer el SGSI), realizar (implementar y operar el SGSI), verificar (monitorizar y revisar el SGSI) y actuar (mantener y mejorar el SGSI). La actual versión de ISO 27001 ya no lo menciona directamente, pero sus cláusulas pueden verse como alineadas con él.

- **Plan de Continuidad del Negocio:** (inglés: Bussines Continuity Plan). Plan orientado a permitir la continuación de las principales funciones del negocio en el caso de un evento imprevisto que las ponga en peligro.

- **Plan de tratamiento de riesgos:** (inglés: Risk treatment plan). Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma.

- **Política de escritorio despejado:**(inglés: Clear desk policy). La política de la empresa que indica a los empleados que deben dejar su área de trabajo libre de cualquier tipo de informaciones susceptibles de mal uso en su ausencia.

- **Proceso:** (inglés: Process). Conjunto de actividades interrelacionadas o interactuantes que transforman unas entradas en salidas. Propietario del riesgo: (inglés: Risk owner). Persona o entidad con responsabilidad y autoridad para gestionar un riesgo.

- **Recursos de tratamiento de información:** (inglés: Information processing facilities). Cualquier sistema, servicio o infraestructura de tratamiento de información o ubicaciones físicas utilizadas para su alojamiento.

- **Riesgo:** (inglés: Risk). 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.

- **Riesgo residual:** (inglés: Residual risk). El riesgo que permanece tras el tratamiento del riesgo.

- **Segregación de tareas**: (inglés: Segregation Of Duties - SOD). Reparto de tareas sensibles entre distintos empleados para reducir el riesgo de un mal uso de los sistemas e informaciones deliberado o por negligencia. Seguridad de la información: (inglés: Information Security). Preservación de la confidencialidad, integridad y disponibilidad de la información.

- **Selección de controles:** (inglés: Control selection). Proceso de elección de los controles que aseguren la reducción de los riesgos a un nivel aceptable. SGSI: (inglés: ISMS). Véase: Sistema de Gestión de la Seguridad de la Información.

- **Sistema de Gestión de la Seguridad de la Información:** (inglés: Information Security Management System). Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión del riesgo y de mejora continua.

- **SoA:** Acrónimo inglés de Statement of Applicability. Véase: Declaración de aplicabilidad.

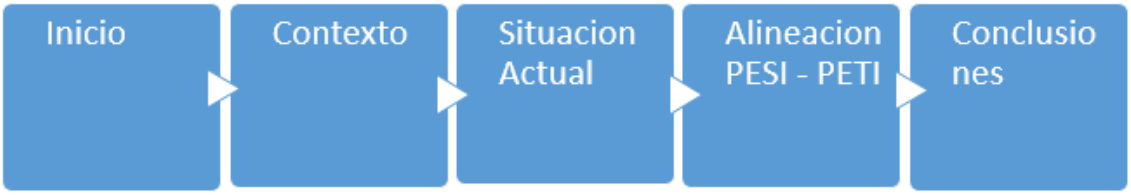
- **Tratamiento de riesgos:** (inglés: Risk Treatment). Proceso de modificar el riesgo, mediante la implementación de controles.

- **Trazabilidad:** (inglés: Accountability). Según [CESID:1997]: Cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a un individuo o entidad.
- **Vulnerabilidad:** (inglés: Vulnerability). Debilidad de un activo o control que puede ser explotada por una o más amenazas.

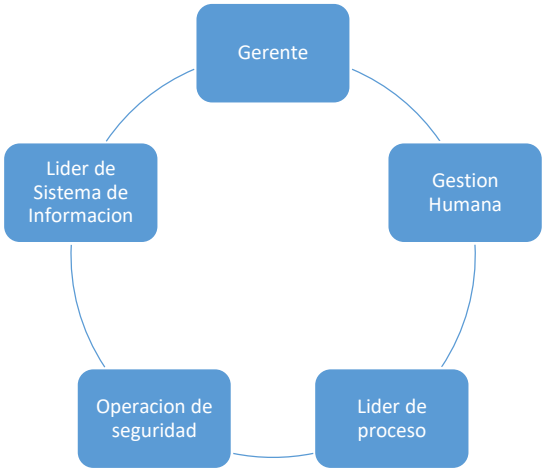
7. Desarrollo

7.1 Metodología

La metodología utilizada para el desarrollo del PESI se muestra a continuación:



7.2 Estructura



7.3 Descripción del plan

Se tiene planeada la realización de la fase de diagnóstico, buscando identificar el estado actual de la organización con respecto a los requerimientos del Modelo de Seguridad y Privacidad de la Información.

Para la realización de dicha fase, se tienen las siguientes actividades planteadas:

- Diagnóstico para determinar el estado actual de la gestión de seguridad y privacidad de la información al interior de la ESE.
- Análisis para determinar el nivel de madurez de los controles de seguridad de la información.
- Identificación el avance de la implementación del ciclo de operación al interior de la entidad.
- Identificación del nivel de cumplimiento con la legislación vigente relacionada con protección de datos personales.
- Identificación del uso de buenas prácticas en ciberseguridad.

Las actividades serán realizadas de acuerdo con la herramienta de diagnóstico MSPI suministrada por MINTIC y la metodología de pruebas de efectividad.

Después de tener el resultado del diagnóstico inicial y se haya determinado el nivel de madurez de la ESE, se procede al desarrollo de la fase de Planificación.

Los resultados asociados a la fase de Diagnostico previas a la implementación serán revisados y socializados en la entidad.

8. Bibliografía

Fortalecimiento de la tecnología de la información. Ministerio de Tecnología de la Información. Disponible en: https://www.mintic.gov.co/gestionti/615/w3-propertyvalue-7275.html?_noredirect=1

9. Control de cambios

Versión	**Descripción del cambio** (Indique si es creación o actualización del documento)	**Justificación**	**Fecha**
01	Creación	Plan de Seguridad y Privacidad de la Información	29 de Enero de 2021

10. Anexos

N/A