Vigilado Supersalud

ESE BelloSalud
Juntos construimos vidas saludables

Plan de Seguridad y Privacidad de la Información

Vigilado Supersalud

TABLA DE CONTENIDO

1. INTRODUCCION 3
2. OBJETIVO 3
2.1. Objetivo General 3
2.2. Objetivos Específicos 4
4. DEFINICIONES 4
5. MARCO LEGAL 6
6. ARTICULACION MIPG CON PESI 7
6.1. Articulación del PESI con el Plan de Desarrollo Institucional 8
7. SEGURIDAD DE LA INFORMACION Y PROTECCIÓN DE DATOS 9
8. PROTECCIÓN DE DATOS 9
9. AMENAZAS Y VULNERABILIDADES 10
9.1. Amenazas Comunes 10
9.2. Vulnerabilidades Críticas 10
10. CLASIFICACIÓN Y FLUJO DE INFORMACIÓN 11
11. MATRIZ DE RIESGOS 11
12. PROYECTOS ESTRATÉGICOS 12
13. CONTROL DE CAMBIOS 13

1. INTRODUCCION

En una época donde la información de la salud de las persona ha tenido grandes transformaciones hacia el entorno digital, y ha dejado de ser una prioridad técnica para convertirse en un pilar ético y operativo fundamental, la seguridad y privacidad de esta son uno de los más relevantes y principales objetivos de la entidades encargadas de la prestación de servicios en salud, al ser uno de los más críticos y sensibles, donde se debe entender que dichas entidades tienen la obligación de dar el tratamiento y gestión adecuada a los datos clínicos, cuya protección no solo garantiza la privacidad del paciente, sino que también asegura la continuidad de servicios vitales donde el acceso oportuno a la información puede marcar la diferencia entre la vida y la muerte.

El presente documento describe el Plan de Seguridad y Privacidad de la Información (PESI) de la Empresa Social del Estado Bellosalud, alineado con los objetivos, metas, procesos, procedimientos y estructura de la Entidad. En concordancia con la política de Gobierno Digital del Ministerio de Tecnologías de la Información y las Comunicaciones (MINTIC) en el marco del Modelo Integrado de Planeación y Gestión – MIPG, conforme con lo establecido en el Decreto 612 2018, para prestar servicios de confianza, generando protección de la información de los ciudadanos, gestionando los riesgos y los incidentes de seguridad digital.

El sistema de redes de comunicación, y la información contenida en servidores, PC´s, periféricos y demás accesorios tecnológicos, que se utilizan en los diferentes procesos que realizan los funcionarios en cada dependencia de la ESE Bellosalud, permanecen expuestos a múltiples riesgos, los cuales pueden ser potencialmente catastróficos y llevar al robo, secuestro, modificación, o pérdida total de la información de la entidad, incluyendo la de los pacientes que es información crítica y sensible.

2. OBJETIVO

2.1. Objetivo General

Garantizar la confidencialidad, integridad y disponibilidad de los activos de información de la ESE Bellosalud mediante el fortalecimiento y la aplicación de procesos, procedimientos, buenas prácticas, y en general cumplimiento de las políticas de seguridad y privacidad de la información establecidas como eje central para la protección y uso adecuado de los datos de la entidad, mitigando **riesgos**

cibernéticos y asegurando el cumplimiento de la normativa vigente en protección de datos personales para el periodo 2026.

2.2. Objetivos Específicos

- ✓ Implementar políticas de buen manejo y seguridad de la información.
- ✓ Sensibilizar e instruir al personal, en buenas prácticas de seguridad digital y privacidad de los datos, fomentando una cultura de prevención frente a amenazas como el phishing y la ingeniería social.
- ✓ Facilitar de manera integral la gestión de los riesgos de seguridad y privacidad de la información, seguridad digital y continuidad de la operación de los servicios.
- ✓ Mitigar el impacto de los incidentes de seguridad y privacidad de la información y de seguridad digital, de forma efectiva, eficaz y eficiente
- ✓ Establecer los mecanismos de aseguramiento físico y digital, para fortalecer la confidencialidad, integridad, disponibilidad, autenticidad, privacidad y no repudio de la información de la ESE Bellosalud.
- ✓ Dar cumplimiento a los requisitos legales y normativos en materia de seguridad y privacidad de la información y de seguridad digital y protección de la información personal.

3. ALCANCE

Aplica a todos los niveles de la ESE Bellosalud, a todos sus funcionarios, contratistas, proveedores, operadores y 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, entidades relacionadas que accedan, ya sea interna o externamente a cualquier tipo de información, independientemente de su ubicación. Así mismo, está lo dispuesto en este documento y su implementación aplica a toda la información creada, procesada o utilizada por la ESE Bellosalud, sin importar el medio, formato, presentación o lugar en el cual se encuentre.

4. DEFINICIONES

Activos de Información: Se refiere a cualquier información o elemento que tiene valor estratégico para los procesos de negocio de la ESE Bellosalud

Datos: Corresponde a los elementos básicos de la información física o digital que se generen, recojan, gestionan, transmiten y destruyen en la ESE Bellosalud.

Sistemas de Información: Conjunto de aplicaciones que se utiliza para la gestión de la información

Tecnología: Corresponde al hardware y software empleado para gestionar la información y las comunicaciones - Seguridad de la Información: 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 del Estado, y de los servicios que prestan al ciudadano2

Análisis de Riesgo: Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo. (ISO/IEC 27000).

Confidencialidad: La información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados, Contratistas: Entenderemos por contratista aquella persona natural o jurídica que ha celebrado un contrato de prestación de servicios o productos con una entidad.

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.

Disponibilidad: Acceso y utilización de la información y los sistemas de tratamiento de la misma por parte de los individuos, entidades o procesos autorizados cuando lo requieran.

Integridad: Mantenimiento de la exactitud y completitud de la información y sus métodos de proceso.

Norma: Principio que se impone o se adopta para dirigir la conducta o la correcta realización de una acción o el correcto desarrollo de una actividad.

Política: Es la orientación o directriz que debe ser divulgada, entendida y acatada por todos los miembros de la entidad.

Privacidad de datos: La privacidad de datos, también llamada protección de datos, es el aspecto de la tecnología de la información (TI) que se ocupa de la capacidad que una organización o individuo tiene para determinar qué datos en un sistema informático pueden ser compartidos con terceros

Procedimiento: Los procedimientos constituyen la descripción detallada de la manera como se implanta una política.

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).

Rol: Papel, función que alguien o algo desempeña.

Seguridad de la información: Preservación de la confidencialidad, integridad, y disponibilidad de la información. (ISO/IEC 27000).

5. MARCO LEGAL

Decreto 612 de 2018 – Integración de los planes institucionales

Este decreto es la base principal para exigir el PESI en las entidades públicas del país.

Establece que el Plan de Seguridad y Privacidad de la Información y el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información deben integrarse al Plan de Acción institucional de manera.

Política de Gobierno Digital (Decreto 1008 de 2018 y Decreto 767 de 2022)

La Política de Gobierno Digital obliga a las entidades públicas a gestionar la seguridad y privacidad de la información como habilitador transversal de la transformación digital, orientando que la seguridad se incorpore en procesos, trámites, servicios y sistemas institucionales.

Modelo de Seguridad y Privacidad de la Información – MSPI

El MSPI es el marco técnico que define cómo implementar los principios de seguridad de la información en las entidades públicas.

Es emitido por el Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC.

Resolución 500 de 2021 (MinTIC)

Establece los lineamientos y estándares para la estrategia de seguridad digital, la adopción del MSPI y la forma en que la seguridad de la información debe integrarse al Plan de Seguridad y Privacidad de la Información (que a su vez se integra al Plan de Acción por Decreto 612).

Decreto 1078 de 2015 (DUR-TIC) — Reglamento del sector TIC que da el marco general de la política de Gobierno Digital.

Decreto 2106 de 2019 — Obligación de implementar estrategia de seguridad digital para trámites digitales.

Lineamientos de gestión de riesgos y controles (Guía para administración de riesgos de seguridad y privacidad).

6. ARTICULACION MIPG CON PESI

El Plan Estratégico de Seguridad de la Información – PESI de la E.S.E. Bellosalud se constituye en un instrumento estratégico que garantiza la protección de la información institucional y la continuidad de los servicios tecnológicos que soportan la prestación de los servicios de salud. Su implementación no es un ejercicio aislado de carácter técnico, sino un componente transversal que fortalece la gestión institucional, el control interno y la generación de valor público.

En este sentido, el PESI se articula de manera directa con el Modelo Integrado de Planeación y Gestión – MIPG y con las líneas estratégicas del Plan de Desarrollo Institucional, asegurando que la seguridad de la información sea un habilitador de la eficiencia, la transparencia y la calidad del servicio.

El PESI contribuye al fortalecimiento de varias dimensiones del MIPG, así:

Dimensión Talento Humano

El PESI promueve la cultura de seguridad de la información mediante:

Sensibilización y capacitación a funcionarios sobre buenas prácticas digitales.

Fortalecimiento de competencias en manejo seguro de la información clínica y administrativa.

Responsabilidad individual en el uso de sistemas y protección de datos.

Dimensión Direccionamiento Estratégico y Planeación

Integra la gestión de riesgos de seguridad de la información a la planeación institucional.

Asegura que las decisiones tecnológicas incluyan criterios de seguridad y privacidad desde su diseño.

Dimensión Gestión con Valores para Resultados

Reduce riesgos que puedan afectar la continuidad de los servicios de salud.

Protege la integridad de la información clínica, garantizando atención segura al usuario.

Dimensión Evaluación de Resultados

Permite hacer seguimiento a incidentes de seguridad, vulnerabilidades y niveles de cumplimiento.

Genera información para la toma de decisiones y mejora continua en materia de seguridad digital.

Dimensión Información y Comunicación

Garantiza la calidad, disponibilidad, integridad y confidencialidad de la información institucional.

Fortalece la confianza de usuarios, funcionarios y entes de control en el manejo de los datos.

Dimensión Gestión del Conocimiento e Innovación

Protege los activos de información que constituyen la memoria institucional.

Asegura que la transformación digital se realice de manera segura y sostenible.

Dimensión Control Interno

Implementa controles tecnológicos y administrativos para mitigar riesgos.

Fortalece la trazabilidad, auditoría y control de accesos a la información.

6.1. Articulación del PESI con el Plan de Desarrollo Institucional

El PESI es un habilitador estratégico para el cumplimiento de las metas del Plan de Desarrollo de la E.S.E. Bellosalud, al brindar un entorno digital seguro que respalda tanto los procesos asistenciales como administrativos.

Estratégica del Plan de Desarrollo	Aporte del PESI
Mejoramiento de la prestación de servicios de salud	Protección de la historia clínica, disponibilidad de sistemas asistenciales, continuidad de los servicios tecnológicos.
Fortalecimiento de la gestión administrativa y financiera	Seguridad de la información financiera y contable, control de accesos a sistemas administrativos.
Transparencia y buen gobierno	Trazabilidad de la información, reducción de riesgos de fraude, protección de datos personales.

Estratégica del Plan de Desarrollo	Aporte del PESI
Modernización institucional	Implementación de buenas prácticas de seguridad digital en nuevos sistemas y servicios en la nube.
Humanización y confianza del usuario	Protección de datos sensibles de los pacientes, fortaleciendo la confianza en la institución.

De esta manera, el PESI permite que la transformación digital de la E.S.E. Bellosalud se realice bajo principios de seguridad, confidencialidad, integridad y disponibilidad de la información, contribuyendo al fortalecimiento del MIPG, al cumplimiento de la Política de Gobierno Digital y al logro de las metas estratégicas del Plan de Desarrollo Institucional.

7. SEGURIDAD DE LA INFORMACION Y PROTECCIÓN DE DATOS

En la seguridad informática se debe distinguir dos propósitos de protección, la seguridad de la información y la protección de datos. Se debe distinguir entre los dos, porque forman la base y dan la razón, justificado en la selección de los elementos de información que requieren una atención especial dentro del marco de la Seguridad Informática y normalmente también dan el motivo y la obligación para su protección.

Sin embargo, hay que destacar que, aunque se diferencia entre la seguridad de la información y la protección de datos como motivo u obligación de las actividades de seguridad, las medidas de protección aplicadas normalmente serán las mismas.

En la seguridad de la información el objetivo de la protección son los datos mismos y trata de evitar su pérdida o modificación no autorizada. Esta debe garantizar en primer lugar la confidencialidad, integridad y disponibilidad de los datos, sin embargo, existen más requisitos, por ejemplo, la autenticidad, entre otros.

8. PROTECCIÓN DE DATOS

En la seguridad informática se debe distinguir dos propósitos de protección, la seguridad de la información y la protección de datos. Se debe distinguir entre los dos, porque forman la base y dan la razón, justificado en la selección de los elementos de información que requieren una atención especial dentro del marco de la Seguridad Informática y normalmente también dan el motivo y la obligación para su protección.

Sin embargo, hay que destacar que, aunque se diferencia entre la seguridad de la información y la protección de datos como motivo u obligación de las actividades de seguridad, las medidas de protección aplicadas normalmente serán las mismas.

En la seguridad de la información el objetivo de la protección son los datos mismos y trata de evitar su pérdida o modificación no autorizada. Esta debe garantizar en primer lugar la confidencialidad, integridad y disponibilidad de los datos, sin embargo, existen más requisitos, por ejemplo, la autenticidad, entre otros.

9. AMENAZAS Y VULNERABILIDADES

La seguridad de la información se basa en entender que una vulnerabilidad es una debilidad propia de los sistemas en la entidad, mientras que una amenaza es el factor externo que intenta aprovechar dicha vulnerabilidad.

9.1. Amenazas Comunes

Son los peligros potenciales que pueden comprometer los datos. Se dividen en varias categorías:

Malware: generalmente es software malicioso como virus, troyanos y muy especialmente el ransomware, este último cuyo objetivo es el secuestro datos para solicitar a su propietario, un rescate por los mismos.

Ingeniería Social: Son tácticas de manipulación como el Phishing, donde se suplanta una identidad confiable buscando robar credenciales de autenticación a cualquier sistema al que ingrese la víctima.

Ataques de Red: Incluyen la denegación de servicio (DoS/DDoS) para hace inaccesibles los sistemas y los ataques de intermediario (MitM) para interceptar tráfico en la red.

Amenazas Internas: Son acciones (accidentales o intencionales) de empleados o personas que cuentan con acceso legítimo a los sistemas.

9.2. Vulnerabilidades Críticas

Son las brechas o fallos que les facilita a los delincuentes, el éxito de un ataque:

Humanas: Son consideradas a menudo el eslabón más débil, como por ejemplo el uso de contraseñas débiles o la falta de capacitación en ciberseguridad.

De Software: Errores y debilidad en la protección del código de los programas, que facilita a los delincuentes el acceso a estos y les permite generar procesos como la inyección SQL, que trata de inyectar código malicioso para que en ciertos campos del aplicativo se pueda obtener acceso la base de datos asociada al mismo y poder manipular información confidencial.

De Configuración: Suele suceder con servidores o equipos en red mal configurados, falta de cifrado o ausencia de algún tipo de autenticación segura como lo es la autenticación multifactor.

Físicas: Falta de control de acceso a los servidores físicos o al robo de hardware.

10. CLASIFICACIÓN Y FLUJO DE INFORMACIÓN

La clasificación de datos tiene el propósito de garantizar la protección de datos (personales) y significa definir, dependiendo del tipo o grupo de personas internas y externas, los diferentes niveles de autorización de acceso a los datos e informaciones.

Considerando el contexto de nuestra misión institucional, tenemos que definir los niveles de clasificación como, por ejemplo: confidencial, privado, sensitivo y público. Cada nivel define por lo menos el tipo de persona que tiene derecho de acceder a los datos, el grado y mecanismo de autenticación. Una vez clasificada la información, tenemos que verificar los diferentes flujos existentes de información internos y externos, para saber quiénes tienen acceso a qué información y datos.

Clasificar los datos y analizar el flujo de la información a nivel interno y externo es importante, porque ambas cosas influyen directamente en el resultado del análisis de riesgo y las consecuentes medidas de protección. Porque solo si sabemos quiénes tienen acceso a qué datos y su respectiva clasificación, podemos determinar el riesgo de los datos, al sufrir un daño causado por un acceso no autorizado.

11. MATRIZ DE RIESGOS

Activo de Información	Amenaza	Vulnerabilidad	Riesgo	Nivel de Riesgo	Controles Existentes	Acciones de Tratamiento	Responsable
Historia Clínica Electrónica	Acceso no autorizado	Contraseñas débiles	Divulgación de datos sensibles	Alto	Usuarios y contraseñas	Implementar doble factor de autenticación	Líder TI
Servidor ERP	Falla eléctrica	No hay UPS suficiente	Interrupción del servicio financiero	Alto	Planta eléctrica	Adquirir UPS y pruebas de respaldo	Subgerencia Administrativa.
Base de datos de pacientes	Malware	Equipos sin actualización	Pérdida o alteración de datos	Alto	Antivirus básico	Implementar política de parches y EDR	Sistemas

Activo de Información	Amenaza	Vulnerabilidad	Riesgo	Nivel de Riesgo	Controles Existentes	Acciones de Tratamiento	Responsable
Equipos de admisiones	Robo	Falta de control físico	Pérdida de información	Medio	Claves de acceso	Cifrado de disco y anclaje físico	TI
Red institucional	Ataque externo	Firewall desactualizado	Caída de servicios	Alto	Firewall perimetral	Actualizar firmware y monitoreo	Proveedor TI

12. PROYECTOS ESTRATÉGICOS

Para el año 2026 se tiene proyectado para el área de las TI las siguientes actividades:

Instalación o actualización de antivirus: Proceso de implementar un software especializado para detectar, prevenir y eliminar programas maliciosos (malware). El antivirus actúa como un escudo en segundo plano, escaneando archivos y descargas en tiempo real para evitar que virus, troyanos o spyware comprometan los equipos y la información que en estos se encuentra.

Este no solo limpia los equipos de amenazas, su función principal es ser proactivo, bloqueando dichas amenazas antes de que se ejecuten.

Creación y optimización de políticas de seguridad de la información: Hace referencia al diseño de un documento formal e institucional, que dicta las reglas y procedimientos de la entidad para proteger sus activos de información. La optimización implica actualizar estas reglas constantemente para adaptarse a nuevas amenazas o cambios tecnológicos.

Gestión para la protección de datos: Es el enfoque estratégico para garantizar que la información (especialmente los datos personales y sensibles) no sea robada ni utilizada de forma indebida. Incluye herramientas para supervisar quién accede a la información y evitar fugas accidentales o intencionales.
Se centra en cumplir con normativas legales y proteger la privacidad de usuarios y clientes.

Gestión de riesgos de seguridad informática: Es el proceso continuo de identificar, evaluar y minimizar las amenazas potenciales antes de que causen daño en los sistemas de la entidad, en lugar de esperar a que algo falle, se analizan las vulnerabilidades del sistema y se decide qué medidas tomar para reducir la probabilidad de un incidente.

No busca eliminar el riesgo por completo (eso es imposible), sino mantenerlo bajo control bajo niveles aceptables para el negocio.

CESAR AUGUSTO ARANGO SERNA
Gerente

ELIANA MARCELA RAMIREZ AYALA
Subgerente Administrativa y Financiera

13. CONTROL DE CAMBIOS

DESCRIPCIÓN	FECHA
Elabora: Ingeniero Sistemas	Enero 2026
Revisa: Profesional Universitario MIPG	Enero 2026
Aprueba: Comité De Gestión y Desempeño	Enero 2026

CONTROL DE ACTUALIZACIONES			
Versión	**Fecha**	**Ítem Modificado**	**Descripción del cambio**
01	Enero 2021	Elaboración del Plan	Se crea el Documento del Plan
01	Enero 2022	Se actualiza de acuerdo a la norma y vigencia	Actualización de las actividades, normatividad y formato
01	Enero 2023	Se actualiza de acuerdo a la norma y vigencia	Actualización de la normatividad y plan de acción
01	Enero 2024	Se actualiza de acuerdo a la norma y vigencia	Actualización de las actividades y plan de acción
01	Enero 2025	Se actualiza de acuerdo a la norma y vigencia	Se actualiza de acuerdo a los resultados del año anterior
01	Enero 2026	Se actualiza de acuerdo a la norma y vigencia	Se actualiza normatividad y actividades