PLAN ESTRATEGICO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION P.E.S.I

Bello – Antioquia
Enero de 2024

1. INTRODUCCIÓN

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 computadoras e información contenida en el servidor, ordenadores, periféricos y accesorios, utilizados por los funcionarios de cada dependencia de la ESE Bellosalud, están expuestos a riesgo que pueden ser fuente de problemas. El Hardware, el Software, y están expuestos a diversos factores de riesgo humano y físicos.

De igual manera el Decreto 2106 de 2019, Por el cual se dictan normas para simplificar, suprimir y reformar trámites, procesos y procedimientos innecesarios existentes en la administración pública, en el parágrafo del artículo 16 indica que (…) Las autoridades deberán disponer de una estrategia de seguridad digital siguiendo los lineamientos que emita el Ministerio de Tecnologías de la Información y las Comunicaciones. (…)

2. OBJETIVOS

2.1 GENERAL

Garantizar la seguridad y el respaldo del sistema de información (bases de datos, información contable, documentos de Excel y Word, entre otros.) de la ESE Bellosalud mediante la aplicación del Plan de Contingencia Informático Institucional.

2.2 ESPECIFICOS

- ✓ Instruir a los funcionarios de la entidad a utilizar las herramientas tecnológicas para minimizar el riesgo de pérdida de información.
- ✓ Implementar políticas de buen manejo y seguridad de la información.
- ✓ 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, 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, esta 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. 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 perdida y 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.

El motivo o el motor para implementar medidas de protección, responden a la seguridad de la información, es el propio interés de la institución o persona que maneja los datos, porque la pérdida o modificación de ellos le puede causar un daño

(material o inmaterial). Por ejemplo, en una entidad bancaria la pérdida o la modificación errónea de la información, sea causada intencionalmente o simplemente por negligencia humana, de un récord de una cuenta bancaria, puede resultar en pérdidas económicas u otras consecuencias negativas para la empresa.

5. PROTECCIÓN DE DATOS

En el caso de la protección de datos, el objetivo de la protección no son los datos en sí, sino el contenido de la información sobre personas, para evitar el abuso de esta. El motivo o el motor para la implementación de medidas de protección, por parte de la institución o persona que maneja los datos, es la obligación jurídica o la simple ética personal, de evitar consecuencias negativas para las personas de las cuales se trata la información.

El objetivo del dominio de control de acceso consiste en limitar el acceso a la información y a las instalaciones con el fin de salvaguardar los activos de información.

Se debe realizar unas políticas de control de acceso, con sus respectivas normas y procedimientos que las implementen. Las recomendaciones para esta política son:

- Tener en cuenta para este fin la clasificación de la información, la legislación pertinente de acuerdo con las leyes de protección de datos.
- Implementar un procedimiento de gestión de derechos de acceso a los diferentes tipos de activos de información en los que se involucre a los dueños de los activos de información.
- El criterio fundamental a la hora de definir la política de control de acceso debería ser: “Permitir sólo lo que necesita conocer para realizar sus funciones, de lo contrario no se permite”
- Se debe realizar unas políticas de control de acceso a redes y servicios de red, con sus respectivas normas y procedimientos que las implementen. Las recomendaciones al respecto son:
- El acceso a redes o servicios de red debe justificarse en función de los activos a los que se necesita acceder, en la clasificación de los activos puede encontrar en qué redes o a que servicios se le debe permitir acceso para acceder al activo de información.
- Se debe incluir procedimientos para monitorear las redes, tráfico y quién tiene acceso de acuerdo con la política, y en caso de accesos no autorizados, considerarlos como un incidente de seguridad e iniciar inmediatamente una investigación de seguridad.
- Se debe implementar un procedimiento de gestión de acceso a usuarios. Este procedimiento incluye la creación, modificación y eliminación de usuarios.

Generalmente está asociado con el proceso de contratación y desvinculación. El procedimiento debe tener en cuenta la autorización al acceso de activos de información, redes y servicios, y estas autorizaciones deben ser avaladas por el dueño del activo de información y por el área de seguridad de la información como mínimo.

- Se debe revisar periódicamente todos los accesos a los activos de información, redes y servicios. En estas revisiones identificar y eliminar o deshabilitar permisos redundantes y obsoletos de acuerdo con las solicitudes de acceso.
- Se debe tener especial cuidado con usuarios con altos privilegios.
- Se debe habilitar logs de acceso a los sitios restringidos.
- Se debe realizar auditoría periódica a los permisos de acceso
- A nivel de aplicativos, durante su desarrollo, desde la etapa de diseño, se debe tener en cuenta: La posibilidad de restringir el acceso a la información de la aplicación, para esto utilizar roles, permitir auditar el acceso a información sensible y a operaciones sensibles dentro del aplicativo, entre otras.
- Utilizar técnicas de autenticación adecuadas para corroborar la identidad de un usuario.
- Durante el log-on se debe proteger de intentos de ingreso por fuerza bruta, evitar mensajes de ayuda en el log-on, utilizar contraseña protegida (que no se vea la contraseña al momento de ingresarla), llevar registro de intentos de log-on (exitosos y fallidos). No transmitir las contraseñas en texto plano.
- Se debe cerrar las sesiones por inactividad.

6. AMENAZAS Y VULNERABILIDADES

6.1 AMENAZAS

Una Amenaza es la posibilidad de ocurrencia de cualquier tipo de evento o acción que puede producir un daño (material o inmaterial) sobre los elementos de un sistema, en el caso de la seguridad informática y los elementos de información. La seguridad informática tiene como propósitos garantizar la confidencialidad, integridad, disponibilidad, autenticidad de los datos e informaciones, las amenazas y los consecuentes daños que puede causar un evento exitoso, también tiene relación con la confidencialidad, integridad, disponibilidad y autenticidad de los datos e informaciones.

Desde el punto de vista de la entidad que maneja los datos, existen amenazas de origen externo, por ejemplo, agresiones técnicas, naturales o humanas, también amenazas de origen interno, como la negligencia del propio personal o las condiciones técnicas, procesos operativos internos.

Generalmente se distingue y divide tres grupos:

1. **Criminalidad:** Son todas las acciones causadas por la intervención humana, que violan la ley y que están penalizadas por esta. Con criminalidad política se entiende todas las acciones dirigido desde el gobierno hacia la sociedad civil.
2. **Sucesos de origen físico:** son todos los eventos naturales y técnicos, así mismos eventos causados por la intervención humana.
3. **Negligencia y decisiones institucionales:** Son todas las acciones, decisiones u omisiones por parte de las personas que tienen poder e influencia sobre el sistema. Al mismo tiempo son las amenazas menos predecibles porque están directamente relacionado con el comportamiento humano.

Existen amenazas que difícilmente se dejan eliminar (virus de computadora) y por eso es la tarea de la gestión de riesgo de preverlas, implementar medidas de protección para evitar o minimizar los daños en caso de que se materialice.

6.2 VULNERABILIDADES

La Vulnerabilidad es la capacidad, las condiciones y características del mismo sistema (incluyendo la entidad que lo maneja), que lo hace susceptible a amenazas, con el resultado de sufrir algún daño. En otras palabras, es la capacidad y posibilidad de un sistema de responder o reaccionar a una amenaza o de recuperarse de un daño, las vulnerabilidades están en directa relación con las amenazas porque si no existe una amenaza, tampoco existe la vulnerabilidad o no tiene importancia, porque no puede ocasionar daño.

Dependiendo del contexto de la institución, se puede agrupar las vulnerabilidades por sus características: ambientales, físicas, económicas, sociales, educativas, institucionales y políticas.

7. CLASIFICACION Y FLUJO DE INFORMACION.

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.

7.1. SERVIDORES DE RED IMPLEMENTADOS EN LA ESE.

Servidores

1. ZEUS (192.168.17.100) Servidor de controlador de dominio y active directory y servidor de DNS.
2. ORION (192.168.17.101) Servidor de Base de datos SQL Server.
3. MARTE (192.168.17.102) Servidor de chat interno Openfire y spark, servidor de antivirus mcafee y servidor de rayos X.
4. Issabel (192.168.17.103) Servidor de telefonía IP CALLCENTER.
5. LABCORE (192.168.17.105) Servidor de laboratorio a cargo de medife.
6. VENUS (192.168.17.106) Servidor de correos electrónicos, servidor de pruebas de dinámica, servidor de base de datos de pruebas de dinámica, servidor de escritorio remoto.
7. Issabel (192.168.17.109) Servidor de telefonía IP PBX.

Dispositivos Nube Locales

1. NAS1 (192.168.17.110) Servidor de archivos o nube local.
2. NAS2 (192.168.17.111) Servidor de copia de seguridad basada en nube local, servidor de archivos y aplicativos de dinámica.
3. NAS01ZAMORA (192.168.18.245) servidor de archivos y aplicativos de dinámica.
4. NAS01FONTIDUEÑO (192.168.19.245) servidor de archivos y aplicativos de dinámica.
5. NAS01PLAYA RICA (192.168.20.245) servidor de archivos y aplicativos de dinámica.
6. NAS01MARUCHENGA (192.168.21.245) servidor de archivos y aplicativos de dinámica.
7. NAS01PARIS (192.168.22.245) servidor de archivos y aplicativos de dinámica.

8. NAS01SANFELIX (192.168.23.245) servidor de archivos y aplicativos de dinámica.
9. NAS01MIRADOR (192.168.24.245) servidor de archivos y aplicativos de dinámica.

8. ANALISIS DE RIESGO

Existen varios métodos de como valorar un riesgo y al final, todos tienen los mismos retos las variables son difíciles de precisar y en su mayoría son estimaciones y llegan casi a los mismos resultados y conclusiones.

En el ámbito de la Seguridad Informática, el método más usado es el Análisis de Riesgo. La valoración del riesgo basada en la fórmula matemática (Riesgo= Probabilidad de Amenaza * Magnitud de Daño.)

Para la presentación del resultado (riesgo) se usa una gráfica de dos dimensiones, en la cual, el eje-x (horizontal, abscisa) representa la “probabilidad de amenaza” y el eje-Y (vertical, ordenada) la “Magnitud de Daño”. La probabilidad de amenaza y magnitud de daño pueden tomar condiciones entre insignificante (1) y alta (4). En la práctica no es necesario asociar valores aritméticos a las condiciones de las variables, sin embargo, facilita el uso de herramientas técnicas como hojas de cálculo.

8.1. PROCEDIMIENTOS OPERACIONALES Y RESPONSABILIDADES

Para este procedimiento se debe:

- Tener procedimientos documentados de cada uno de los elementos de procesamiento de información, como servicios, aplicativos, dispositivos de red y de infraestructura. La documentación por cada elemento debería incluir como mínimo o Instalación y configuración de los sistemas o procedimiento de encendido y apagado o procedimiento de respaldo tanto de los datos como de la configuración
- Contar con un procedimiento de gestión de la capacidad. El principio fundamental consiste en monitorear todos los recursos de procesamiento y comunicación, tales como ancho de banda de los canales, memoria, capacidad de almacenamiento, capacidad de cálculo, entre otros, y alertar cuándo lleguen a valores críticos con el fin de gestionar la capacidad de cómputo, bien sea optimizando o adquiriendo más capacidad.

Contar con separación de ambientes, la norma se refiere a que el ambiente de desarrollo debe ser diferente al ambiente de producción. Cuando se refiere a ambientes, lo ideal sería que fuesen ambientes totalmente independientes. En lo posible, se debe procurar cinco ambientes como se describen a continuación:

- **Terceros:** cuando se desarrolla software por terceros y es necesario que tengan acceso a los sistemas de la ESE, es recomendable construir un ambiente independiente para el proveedor que no interfiera con la entidad ni afecte la seguridad de la misma. La información con la que se realiza estos desarrollos debe ser información de prueba, nunca con datos reales.
- **Desarrollo:** El ambiente de desarrollo es un ambiente diseñado para este fin no debe tener acceso directo a los sistemas de producción. Debería brindarles a los desarrolladores una infraestructura lo más similar posible a la que se tiene para producción. La información con la que se realiza estos desarrollos debe ser información de prueba, nunca con datos reales.
- **Pruebas y Calidad de Software:** Es un ambiente destinado para todas las pruebas de software: funcionales, no funcionales y pruebas de seguridad. Debería tener una infraestructura lo más similar posible a la que se tiene para producción. La información con la que se realiza estos desarrollos debe ser información de prueba, nunca con datos reales.
- **Producción:** Es el ambiente productivo, donde se realizan las operaciones reales de la entidad.
- **Contingencia:** Es el ambiente de respaldo que se analiza en detalle en la gestión de continuidad, debe ser lo suficientemente robusto para soportar los servicios mínimos requeridos por la ESE.

9. 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.

- **Recurso Humano**: corresponde a los servidores públicos y contratistas de la ESE que tengan acceso de una u otra manera a los activos de información de la Entidad
- **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.
- **Guía:** documento técnico que describe el conjunto de normas a seguir en los trabajos relacionados con los sistemas de información.
- **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.
- **Parte interesada**: (Stakeholder) Persona u organización que puede afectar a, ser afectada por o percibirse a sí misma como afectada por una decisión o actividad.
- **Política del SGSI**: Manifestación expresa de apoyo y compromiso de la alta dirección con respecto a la seguridad de la información.
- **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).

ALEXIS ALBERTO AGUDELO GOMEZ
Subgerente Administrativo y Financiero

SEGUIMIENTO, CONTROL Y MEJORA

Las acciones y actividades articuladas al plan de acción de acuerdo a lo estipulado en el decreto 612 de 2018 se encuentran diligenciadas en el formato establecido para tal fin.

MODIFICACIONES

Versión	Fecha	Razón
00	31/01/2021	Plan Estratégico de seguridad y privacidad de la información PESI
01	31/01/ 2022	Actualización para vigencia 2022
03	31/01/2023	Actualización para vigencia 2023
03	30/01/2024	Actualización para vigencia 2024

APROBACIÓN.

Elaboró	Revisó	Aprobó
Ingeniero de Sistemas	Subgerencia Administrativa y Financiera	Gerente