EMPRESA SOCIAL DEL ESTADO

PASTO SALUD E.S.E

NIT.900091143-9

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

VERSIÓN 8.0

SAN JUAN DE PASTO
2024

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION
PASTO SALUD E.S.E.

ACTUALIZO

WILLIAM MONTENEGRO GUEVARA
Jefe Oficina Asesora de Comunicaciones y Sistemas

SAN JUAN DE PASTO
2024

TABLA DE CONTENIDO

RESOLUCIÓN No. 0079 -
(. 2024)

"Por la cual se adopta el Plan de Seguridad y Privacidad de la Información de la Empresa Social del Estado Pasto Salud ESE para la vigencia 2024"

EL GERENTE

En uso de sus atribuciones legales y en especial a la conferidas por el Acuerdo No. 004 del 2006 emanado del Concejo Municipal de Pasto, Ley 1753 de 2015 y Decreto 1083 del 2015 y,

CONSIDERANDO:

Que mediante el Decreto 612 del 4 de abril del 2018, se fijan directrices para la integración de los planes institucionales y estratégicos del Plan de Acción por parte de las entidades del Estado, en su artículo 1, adiciona entre otros el artículo 2.2.22.3.14 al capítulo 3 del Título 22 del parte 2 del Decreto 1083 del 2015. Único Reglamentario del Sector de Función Pública, la cual dispone que las entidades de Estado, de acuerdo con el ámbito de aplicación del Modelo Integrado de Planeación y Gestión, deberán integrar los planes institucionales y estratégicos, entre ellos el Plan Anual

Que el artículo 2 del Decreto Presidencial 612 del 4 de abril de 2018 señala que las entidades del Estado de manera progresiva deberán integrar los planes institucionales y estratégicos y publícalos en la página web de la entidad.

Que mediante el Decreto 1008 de 14 de junio de 2018 se establece que la seguridad y privacidad de la información, es uno de los habilitadores transversales de la nueva Política de Gobierno Digital.

Que mediante Acta No 001-2024 del Comité Institucional de Gestión y Desempeño del día 25 de enero de 2024 se presentó, se revisó y se aprobó el Plan de Seguridad y Privacidad de la Información de la Empresa Social del Estado Pasto Salud ESE para la vigencia 2023, el cual se pretende adoptar mediante el presente acto administrativo.

En mérito de lo expuesto,

RESUELVE:

ARTÍCULO PRIMERO. - Adoptar el Plan de Seguridad y Privacidad de la Información de la Empresa Social del Estado Pasto Salud ESE para la vigencia 2024", documento que hace parte integral de la presente resolución.

ARTÍCULO SEGUNDO. - El Plan de Seguridad y Privacidad de la Información tiene como objetivo principal gestionarlos riesgos de seguridad y privacidad de la información, a través de la metodología establecida, facilitando la identificación del riesgo, las oportunidades, el análisis, la valoración e implementación de políticas, así como el seguimiento y monitoreo permanente enfocado a su cumplimiento y mejoramiento continuo.

ARTÍCULO TERCERO. - Publíquese el presente acto administrativo en la página web de la Empresa Social del Estado Pasto Salud ESE para la vigencia 2024".

EMPRESA SOCIAL DEL ESTADO PASTO SALUD E S E

RESOLUCIONES

VERSIÓN	PROCESO/SERVICIO	CODIGO	NUM
6.0	GESTION DE SISTEMAS DE INFORMACION	GSI-R	062

OFICINA DE COMUNICACIONES Y SISTEMAS

ARTÍCULO CUARTO. - La presente resolución rige a partir de la fecha de su expedición y deroga las disposiciones contrarias a este.

PUBLÍQUESE Y CÚMPLASE

SEBASTIAN GRANJA ORDOÑEZ
Gerente (E).

Proyectó: WILLIAM RICARDO MONTENEGRO GUEVARA / Profesional Universitario

CONTROL DE CAMBIOS

E: Elaboración del documento
M: Modificación del documento
X: Eliminación del documento

Versión	CONTROL DE CAMBIOS	INFORMACION DE CAMBIOS					Acto Administrativo de Adopción
		E	M	X	Actividades o Justificación del cambio	Elaboró / Actualizó	
8.0	Actualización Plan de Seguridad y Privacidad de la Información.		X		**Justificación**: Se realiza actualización plan vigencia 2024	Equipo Oficina Asesora de Comunicaciones y Sistemas/William Montenegro Guevara. Jefe Oficina Asesora de Comunicaciones y Sistemas	Resolución 060-28-01-2021
7.0	Actualización Plan de Seguridad y Privacidad de la Información.		X		**Justificación**: Se realiza ajuste a la política de Seguridad de la Información, Se ingresó un objetivo específico, se modificó el Modelo y Operación del Sistema de Seguridad de la Información.	Equipo Oficina Asesora de Comunicaciones y Sistemas/William Montenegro Guevara. Jefe Oficina Asesora de Comunicaciones y Sistemas	Resolución 060-28-01-2021
6.0	Elaboración y aprobación del Plan de Seguridad y Privacidad de la Información.	X			**Justificación** La alta gerencia de la Empresa Social del Estado Pasto Salud, para dar cumplimiento a lo establecido en el componente de seguridad y privacidad de la información de la estrategia de gobierno digital. , elabora el Modelo de Seguridad y Privacidad de la Información. Solicitudes del decreto 612 de 2018 y Decreto 1078 de 2015.	Equipo Oficina Asesora de Comunicaciones y Sistemas/William Montenegro Guevara. Jefe Oficina Asesora de Comunicaciones y Sistemas	Resolución 092 del 29 de enero de 2020

INTRODUCCIÓN

La empresa Social del Estado Pasto Salud E.S.E, siguiendo las directrices en materia de seguridad digital y de la información de acuerdo, al Decreto 1078 de 2015 modificado por el Decreto 1008 de 2018, en el artículo 2.2.9.1.1.3. Principios. Define la seguridad de la información como principio de la Política de Gobierno Digital, de igual manera en el artículo 2.2.9.1.2.1 define la estructura de los Elementos de la Política de Gobierno Digital a través de componentes y habilitadores transversales los cuales son los elementos fundamentales de Seguridad de la Información, Arquitectura y Servicios Ciudadanos Digitales, que permiten el desarrollo de los anteriores componentes y el logro de los propósitos de la Política de Gobierno Digital. Teniendo en cuenta lo anterior, se formula el Plan de Seguridad y privacidad de la información al interior de la Empresa Social del Estado Pasto Salud E.S.E.

1. OBJETIVO GENERAL

Proteger los activos de información, así como el uso adecuado de los recursos y gestión del riesgo, con el fin de preservar la disponibilidad, integridad y confidencialidad de la información.

1.1. OBJETIVOS ESPECÍFICOS

- Identificar, clasificar, y gestionar los activos de la información de la empresa
- Apropiar al talento humano de la política de seguridad y privacidad de la información y su aplicación.
- Fortalecer los mecanismos de respaldo de la información física como digital para su preservación y conservación.

2. ALCANCE

Aplica a todas las sedes de Pasto Salud E.S.E, a todos sus grupos de interés y aquellas personas o terceros que en razón del cumplimiento de sus funciones y las de Pasto Salud E.S.E generen, compartan, utilicen, recolecten, procesen, intercambien o consulten su información, sin importar el medio, formato o presentación o lugar en el cual se encuentre.

Así como a los Entes de Control, Entidades relacionadas que accedan, ya sea interna o externamente a cualquier archivo de información, independientemente de su ubicación.

3. POLÍTICA DE SEGURIDAD DE LA INFORMACION

La Empresa Social del Estado Pasto Salud E.S.E, mediante la adopción e implementación del Modelo de Seguridad y Privacidad de la Información enmarcado en el Sistema de Gestión de Seguridad de la información, administra, protege, preserva la confidencialidad, integridad, disponibilidad, autenticidad y no repudio de la información en todos los procesos organizacionales, mediante una gestión integral de riesgos y la implementación de controles físicos y digitales previniendo así incidentes y dando cumplimiento a los requisitos legales y reglamentarios, orientados a la mejora continua y al alto desempeño del Sistema de Gestión de Seguridad de la Información.

4. MARCO LEGAL

Ley 1273 de 5 de enero 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 23 de 1982: Sobre derechos de autor

ISO IEC 27001-2013: Estándares internacionales sobre tecnología de la información, técnicas de seguridad, Administración de seguridad de la información, los cuales proporcionan un marco de gestión de la seguridad de la información, utilizable por cualquier tipo de empresa.

ISO IEC 27002-2013: Es un estándar para la seguridad de la información.

Ley Estatutaria 1266 de 2008, Por la cual se dictan las disposiciones generales de 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 y se dictan otras disposiciones. Para conocer más de esta Ley,

Ley 1581 de 2012, la cual se dictan disposiciones generales para la Protección de Datos Personales. Para conocer más de esta Ley

5. GLOSARIO

Entiéndanse para el presente documento los siguientes términos:

Política: Son instrucciones mandatorios que indican la intención de la alta gerencia respecto a la operación de la organización respecto a un asunto determinado.

Recurso Informático: Elementos informáticos (base de datos, sistemas operacionales, redes, equipos de cómputo, sistemas de información y comunicaciones) que facilitan servicios informáticos.

Información: Puede existir en muchas formas. Puede estar impresa en papel, almacenada electrónicamente, transmitida por correo electrónico o utilizando medios magnéticos, presentada en imágenes, o expuesta en una conversación. Cualquiera sea la forma que adquiere la información, o los medios por los cuales se distribuye o almacena, siempre debe ser protegida en forma adecuada.

Usuarios Terceros: Todas aquellas personas naturales o jurídicas, que no son funcionarios o contratistas de Pasto Salud ESE, pero que por las actividades que realizan en la Entidad, deban tener acceso a recursos Informáticos.

Ataque cibernético: intento de penetración de un sistema informático por parte de un usuario no deseado ni autorizado a accederlo, por lo general con intenciones insanas y perjudiciales.

Brecha de seguridad: deficiencia de algún recurso informático o telemático que pone en riesgo los servicios de información o expone la información en sí misma, sea o no protegida por reserva legal.

Criptografía de llave publica: es el arte o ciencia de cifrar y descifrar información utilizando técnicas matemáticas que hagan posible el intercambio de mensajes de manera que sólo puedan ser leídos por las personas a quienes van dirigidos.

Cifrar: quiere decir transformar un mensaje en un documento no legible, y el proceso contrario se llama `descodificar" o `descifrar". Los sistemas de ciframiento se llaman `sistemas criptográficos".

Certificado Digital: es un bloque de caracteres que acompaña a un documento y que certifica quién es su autor (autenticación) y que no haya existido ninguna manipulación de los datos (integridad). Para firmar, el firmante emisor utiliza una clave secreta que le vincula al documento. La validez de la firma podrá ser comprobada por cualquier persona que disponga de la clave pública del autor.

Controles sobre la seguridad: representan los procedimientos de control interno establecidos por Pasto Salud E.S.E. para asegurar que el uso de las tecnologías de información alcance sus objetivos. En un concepto moderno y basado en los lineamientos

que define la reingeniería organizacional, los controles generales se han direccionado al control de los procesos informáticos.

Procesos informáticos: son los procesos que tienen relación directa con los servicios que se prestan a los usuarios de los sistemas de información y sus tecnologías relacionadas, procesos que consisten en tomar un insumo, agregarle valor y generar un producto que satisface a un cliente interno o externo.

Amenaza: es el conjunto de los peligros a los que están expuestos los sistemas de información y sus recursos tecnológicos relacionados, los que pueden ser de tipo accidental o intencional.

Amenaza Accidental: cuando no existe un deliberado intento de perjudicar a la organización.

Amenaza Intencional: su móvil es perjudicar a la organización u obtener beneficios en favor de quien comete la acción.

Confidencialidad: asegurar que los sistemas de información y sus recursos relacionados sean solo accedidos por los funcionarios o contratistas de Pasto Salud E.S.E, basados en la necesidad de saber o de hacer de sus cargos.

Integridad: exactitud y plenitud de los sistemas de información y sus recursos relacionados, limitando la gestión sobre los mismos a personas autorizados y programas de aplicación aprobados y autorizados, protegiéndolos contra pérdida, destrucción o modificaciones accidentales o intencionales.

Disponibilidad: Asegurar que los usuarios autorizados tienen acceso a los sistemas de información y sus recursos relacionados, en tiempo y forma, cuando sean requeridos.

Privacidad: Evitar que trascienda a terceras personas información de Pasto Salud E.S.E., referida a individuos, protegiendo a los mismos contra la divulgación indebida de su información personal y protegiendo la responsabilidad de la empresa sobre este tipo de divulgaciones.

TI: Tecnología de la Información.

Hacker: Usuario de computadores especializado en penetrar en las bases de datos de sistemas informáticos estatales con el fin de obtener información secreta y en algunos casos provocar daños.

Spam: Se llama spam, al correo basura o a los mensajes no solicitados, no deseados o de remitente desconocido.

Keylogger: Es un tipo de software o un dispositivo hardware específico que se encarga de registrar las pulsaciones que se realizan en el teclado, para posteriormente memorizarlas en un fichero o enviarlas a través de internet.

Sniffer: El sniffer es un software que permite capturar tramas de la red. Generalmente utilizado con fines maliciosos para capturar textos de emails, chats, datos personales, contraseñas, etc.

Phishing: El phishing es un tipo de engaño creado por hackers malintencionados, con el objetivo de obtener información importante como números de tarjetas de crédito, claves, datos de cuentas bancarias, etc.

6. MODELO Y OPERACIÓN DEL SISTEMA DE SEGURIDAD DE LA INFORMACIÓN – SGSI

7. PERSONAL DE SEGURIDAD DE LA INFORMACION

Las funciones del personal de seguridad de la información son asumidas por los profesionales Universitarios Sistemas de la Oficina asesora de Comunicaciones y Sistemas de Pasto Salud E.S.E.

8. PLAN DE IMPLEMENTACIÓN DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

El plan de implementación para el componente de seguridad y privacidad de la información, comprende las siguientes actividades, cronograma y recursos asignados.

EMPRESA SOCIAL DEL ESTADO PASTO SALUD E.S.E NIT.900091143-9	FORMULACIÓN PLAN OPERATIVO ANUAL			
	VERSIÓN	PROCESO/SERVICIO	CÓDIGO	NUM
	7.0	DIRECCIONAMIENTO ESTRATÉGICO	DE-POA	033

SEDE	SEDE ADMINISTRATIVA
FACTOR	GESTIÓN D ELA TECNOLOGÍA
PERSPECTIVA	PROCESOS INTERNOS
OBJETIVO ESTRATÉGICO	Mejorar continuamente los procesos d ela organizaciòn, haciendo especial ènfasis en los ejes de acreditaciòn: seguridad del paciente, humanizaciòn d ela atenciòn, gestiòn del riesgo, gestiòn de la tecnologia, gestiòn clinica centralizada en el paciente, responsabilidad social empresarial y transformaciòn cultural.
PROCESO	GESTION DE SISTEMAS DE INFORMACION
OBJETIVO	Identificar, clasificar, y gestionar los activos de la información de la empresa
VIGENCIA	**2024**

No.	**ESTRATEGIA**	**INDICADOR**		**META**
		NOMBRE DEL INDICADOR	**FORMULA**	
	Implementaciòn de controles y fortalecer el uso de buenas prácticas de las polìtcas de seguridad informàtica	Activos de la información, Esquema de Publicación e índice de clasificación actualizados	NA	>=90%
			NA	

PLAN DE ACCIÓN PARA EL LOGRO DE LA META			
No.	ACTIVIDAD	MEDIO DE VERIFICACIÓN	RESPONSABLE
1	Planificar las actividades para la actualización y consolidación de los activos de la información.	. Acta de reunión equipo Oficina asesora de Comunicaciones y sistemas / Archivo y correspondencia	Jefe Oficina Asesora de Comunicaciones y Sistemas
2	Actualizar, consolidar y publicar los activos de la información.	Activos de la información publicados en la página web link de transparencia	Jefe Oficina Asesora de Comunicaciones y Sistemas
3	Hacer seguimiento a la matrices de activos de la informaciòn.	Informe de revisiòn de activos de la informaciòn	Jefe Oficina Asesora de Comunicaciones y Sistemas
4	Identificación de oportunidades de mejora frente a resultados no esperados	Análisis de Causa Plan de mejora	Jefe Oficina Asesora de Comunicaciones y Sistemas

Nota: Si requiere mas filas, favor insertar.

NOMBRES Y APELLIDOS (Responsable de la formulación y ejecución del Plan Operativo Anual)	**CARGO**
HARVEY ALEXIS VALLEJO NARVAEZ	**JEFE**

VIGILADO Supersalud

EMPRESA SOCIAL DEL ESTADO PASTO SALUD E.S.E NIT 900091143-9	FORMULACIÓN PLAN OPERATIVO ANUAL			
	VERSIÓN	PROCESO/SERVICIO	CÓDIGO	NUM
	7.0	DIRECCIONAMIENTO ESTRATÉGICO	DE-POA	033

SEDE	SEDE ADMINISTRATIVA
FACTOR	GESTION D ELA TECNOLOGIA
PERSPECTIVA	PROCESOS INTERNOS
OBJETIVO ESTRATÉGICO	Mejorar continuamente los procesos d ela organizaciòn, haciendo especial èn fasis en los ejes de acreditaciòn: seguridad del paciente, humanizaciòn d ela atenciòn, gestiòn del riesgo, gestiòn de la tecnologia, gestiòn clinica centralizada en el paciente, responsabilidad social empresarial y transformaciòn cultural.
PROCESO	GESTION DE SISTEMAS DE INFORMACION
OBJETIVO ESPECÍFICO	Apropiar al talento humano de la política de seguridad y privacidad de la información y su aplicación.
VIGENCIA	**2024**

No.	**ESTRATEGIA**	**INDICADOR**		**META**
		NOMBRE DEL INDICADOR	**FORMULA**	
	Implementaciòn de controles y fortalecer el uso de buenas pràcticas de las politcas de seguridad informàtica	Apropiaciòn del talento humano de la política de seguridad y privacidad de la información.	No de capacitaciones realizadas / Total de capacitaciones programadas	>=90%

PLAN DE ACCIÓN PARA EL LOGRO DE LA META

No.	ACTIVIDAD	MEDIO DE VERIFICACIÓN	RESPONSABLE
1	Planificar las temáticas de capacitación de seguridad de la información en el Plan Institucional de Capacitaciones PIC	Plan Institucional de capacitaciones PIC.	Jefe Oficina Asesora de Comunicaciones y Sistemas
2	Elaborar cronograma de control y seguimiento a la política de seguridad de la información.	Informe al seguimiento de la seguridad de la información. Listas de chequeo	Jefe Oficina Asesora de Comunicaciones y Sistemas
5	Ejecutar el plan de capacitaciones de seguridad de la información	Piezas Gráficas Plataforma moodel Reunión Virtual Registro asistencia a Capacitación	Jefe Oficina Asesora de Comunicaciones y Sistemas
6	Realizar control y seguimiento de seguridad de la información a las sedes Priorizadas	Informe de seguimiento a las visitas realizadas a las sedes seleccionadas	Jefe Oficina Asesora de Comunicaciones y Sistemas

Nota: SI requiere mas filas, favor insertar.

NOMBRES Y APELLIDOS (Responsable de la formulación y ejecución del Plan Operativo Anual)	CARGO
HARVEY ALEXIS VALLEJO NARVAEZ	JEFE

VIGILADO Supersalud

EMPRESA SOCIAL DEL ESTADO PASTO SALUD E.S.E NIT.900091143-9	FORMULACIÓN PLAN OPERATIVO ANUAL			
	VERSIÓN	PROCESO/SERVICIO	CÓDIGO	NUM
	7.0	DIRECCIONAMIENTO ESTRATÉGICO	DE-POA	033

SEDE	SEDE ADMINISTRATIVA
FACTOR ESTRATÉGICO	GESTIÒN D ELA TECNOLOGÌA
PERSPECTIVA	PROCESOS INTERNOS
OBJETIVO ESTRATÉGICO	Mejorar continuamente los procesos d ela organizaciòn, haciendo especial èn fasis en los ejes de acreditaciòn: seguridad del paciente, humanizaciòn d ela atenciòn, gestiòn del riesgo, gestiòn de la tecnologìa, gestiòn clìnica centralizada en el paciente, responsabilidad social empresarial y transformaciòn cultural.
PROCESO	GESTION DE SISTEMAS DE INFORMACION
OBJETIVO ESPECÍFICO	Fortalecer los mecanismos de detección y tratamiento de incidentes de seguridad, así como los de respaldo de la información física como digital para asegurar su preservación y conservación.
VIGENCIA	**2024**

No.	**ESTRATEGIA**	**INDICADOR**		**META**
		NOMBRE DEL INDICADOR	**FORMULA**	
	Implementaciòn de controles y fortalecer el uso de buenas pràcticas de las politcas de seguridad informàtica	Copias de Seguridad	No de Backups realizados / No de Backups programados	>=100%

PLAN DE ACCIÓN PARA EL LOGRO DE LA META

No.	ACTIVIDAD	MEDIO DE VERIFICACIÓN	RESPONSABLE
1	Planificación de la programación de Backups de las bases de datos	Programación de backups en el Sql Server Análisis de Causa Plan de mejora	Jefe Oficina Asesora de Comunicaciones y Sistemas
2	Ejecución del programa de backups para las bases de datos	Bitácora de Jobs SQL Server de la programación de backups y la ejecución.	Jefe Oficina Asesora de Comunicaciones y Sistemas
3	Evaluación continua y sistemática de los resultados de ejecución de las copias de respaldo(backups) para las bases de datos	Indicador sistema de información MilPS	Jefe Oficina Asesora de Comunicaciones y Sistemas
4	Evaluación continua y sistemática de los resultados de Incidentes de Seguridad Informática frente a ciber amenazas sobre	Indicador sistema de información MilPS	Jefe Oficina Asesora de Comunicaciones y Sistemas
5			

Nota: Si requiere mas filas, favor insertar.

NOMBRES Y APELLIDOS (Responsable de la formulación y ejecución del Plan Operativo Anual)	**CARGO**

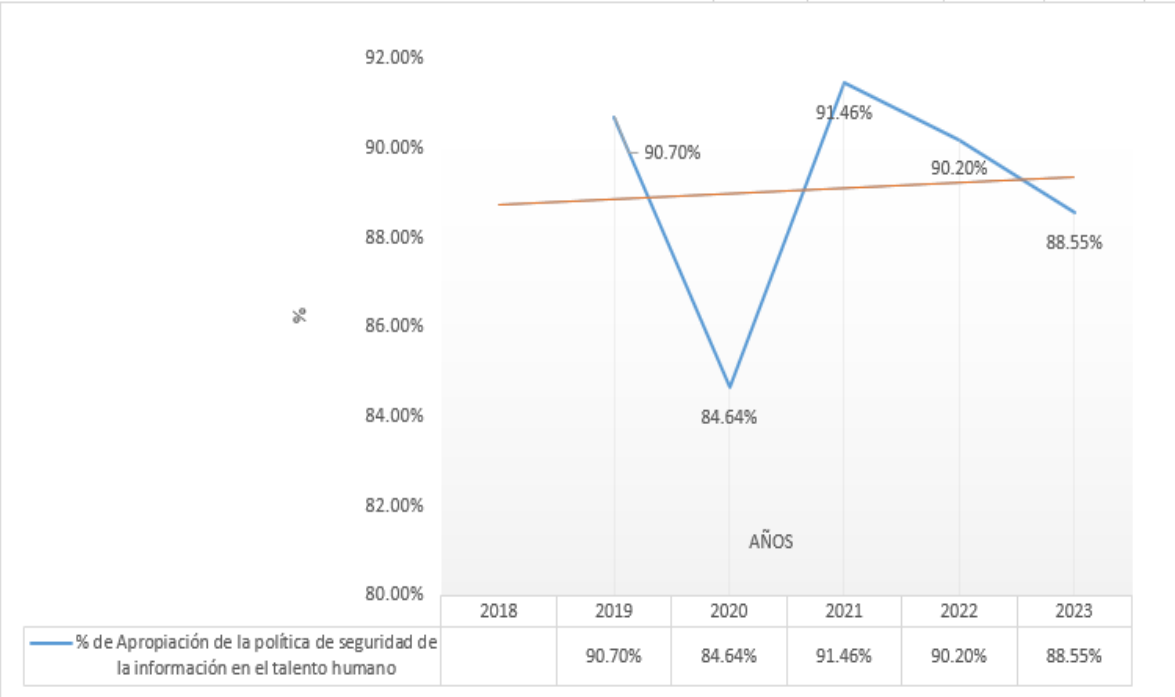
9. ANÁLISIS Y EVALUACIÓN DE RESULTADOS

RESULTADOS SEGURIDAD DE LA INFORMACIÓN

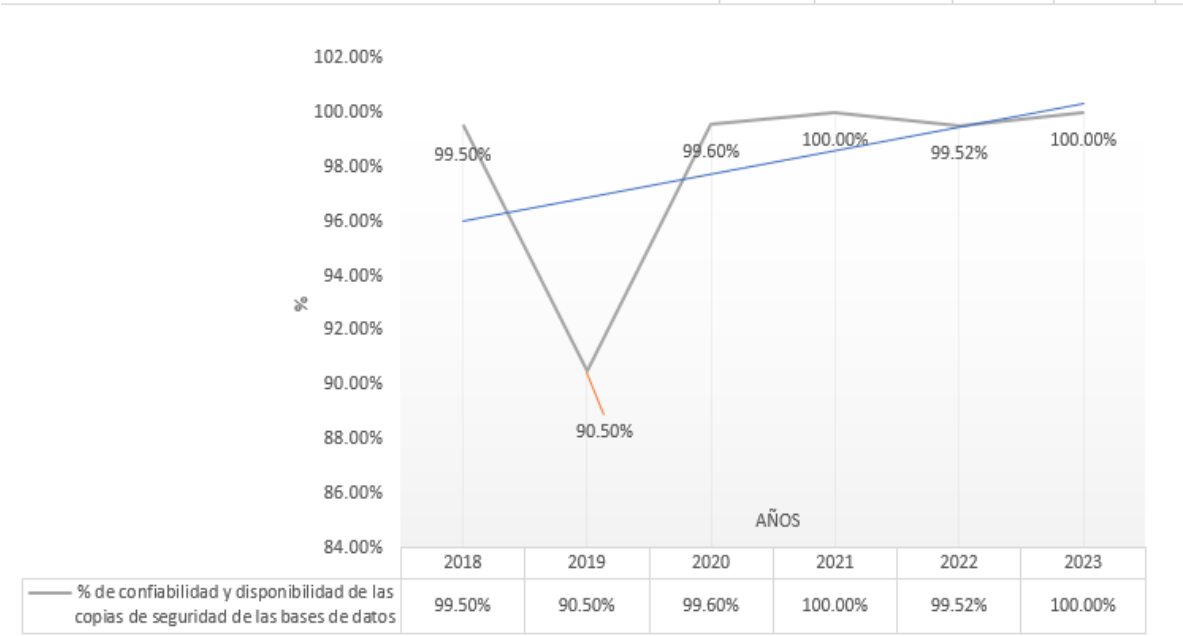
Análisis:

% de Apropiación de la Política de Seguridad de la Información en el Talento Humano: La meta de apropiación de la política de seguridad de la información en el talento humano es del 90%. Los resultados muestran cierta variabilidad, con el nivel más bajo en 2018 (90.70%) y una tendencia ascendente en 2023 (88.55%).

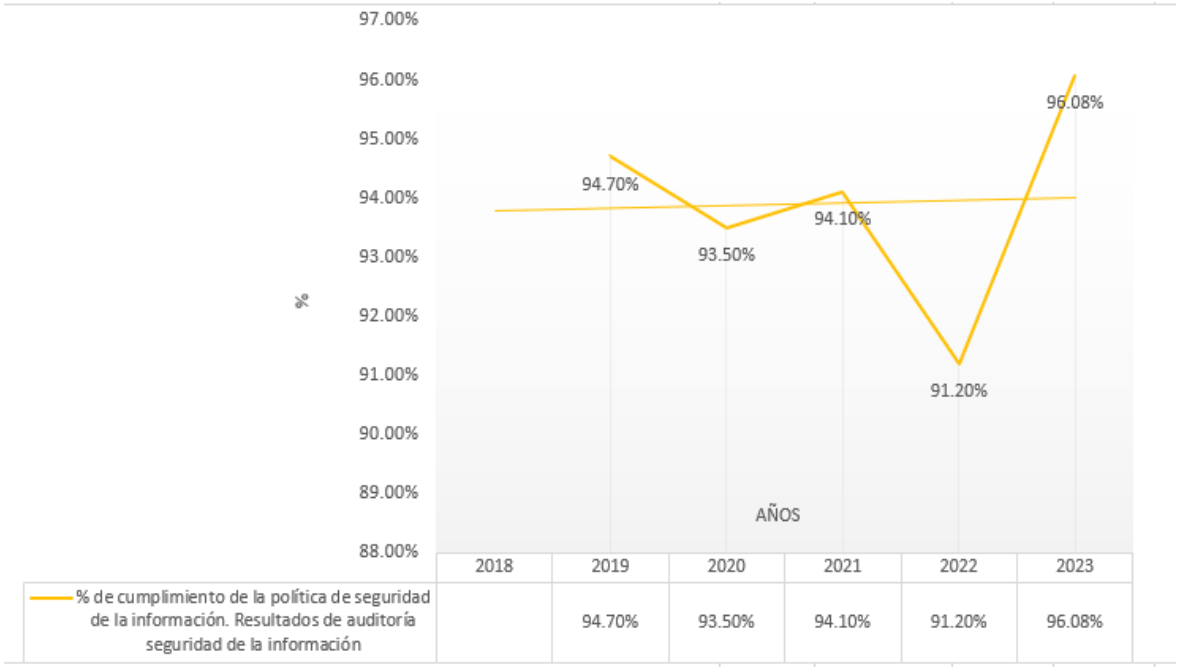
Se recomienda implementar estrategias para mejorar la conciencia y apropiación de la política entre el personal.



% de Confiabilidad y Disponibilidad de Copias de Seguridad: La meta establecida para el porcentaje de confiabilidad y disponibilidad de las copias de seguridad es del 99%. En el período analizado, los resultados fluctúan, alcanzando el nivel más bajo en 2019 con 90.50%, pero mejorando en 2023 con un 100.00%. Las razones por las cuales se han presentado porcentajes por debajo del 100% obedecen a perdida de copias diferenciales que se pueden presentar por consecuencia de fallas técnicas muy esporádicas en el hardware donde se generan los backups. Estas pérdidas no ponen en riesgo la pérdida total de la información.



% de Cumplimiento de la Política de Seguridad de la Información: La meta de cumplimiento de la política de seguridad de la información es del 90%. A lo largo de los años, los resultados varían, alcanzando su punto más alto en 2023 con un 96.08%. Se sugiere continuar fortaleciendo la implementación de la política para mantener y mejorar los niveles de cumplimiento.

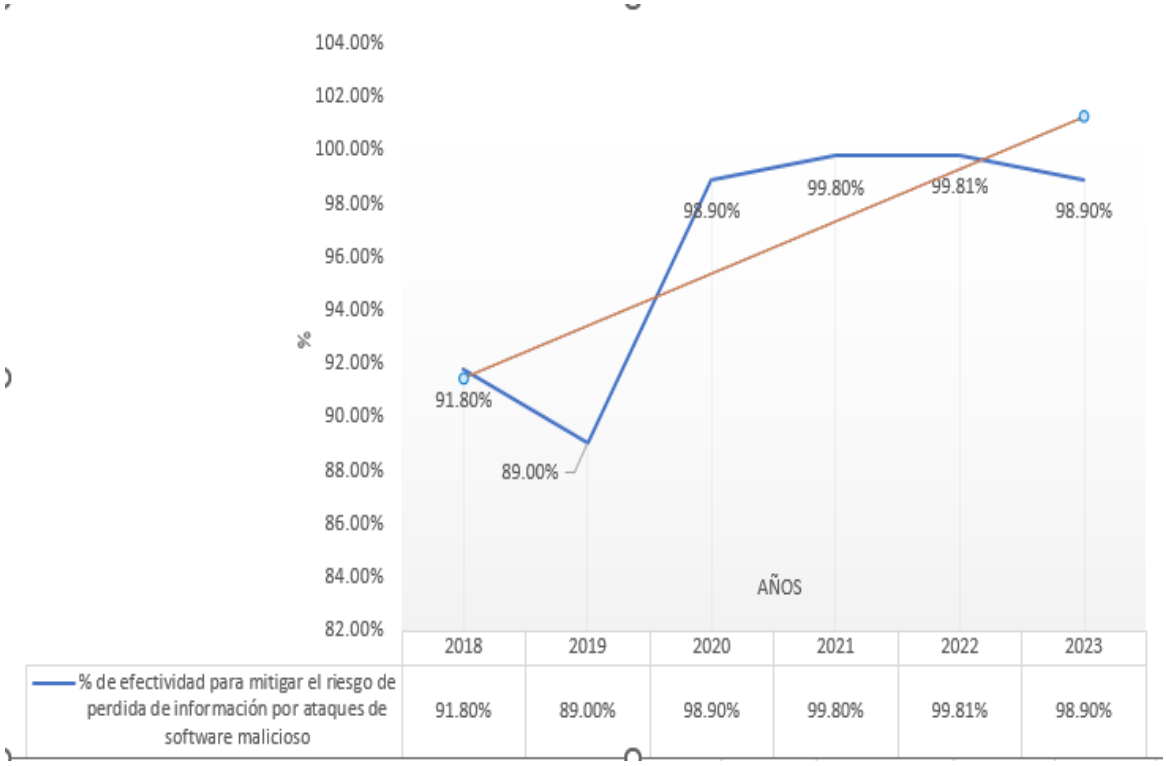


% de Efectividad para Mitigar el Riesgo de Pérdida de Información: La meta establecida es del 95%, indicando el nivel deseado de efectividad en la mitigación de riesgos de pérdida de información por ataques de software malicioso.

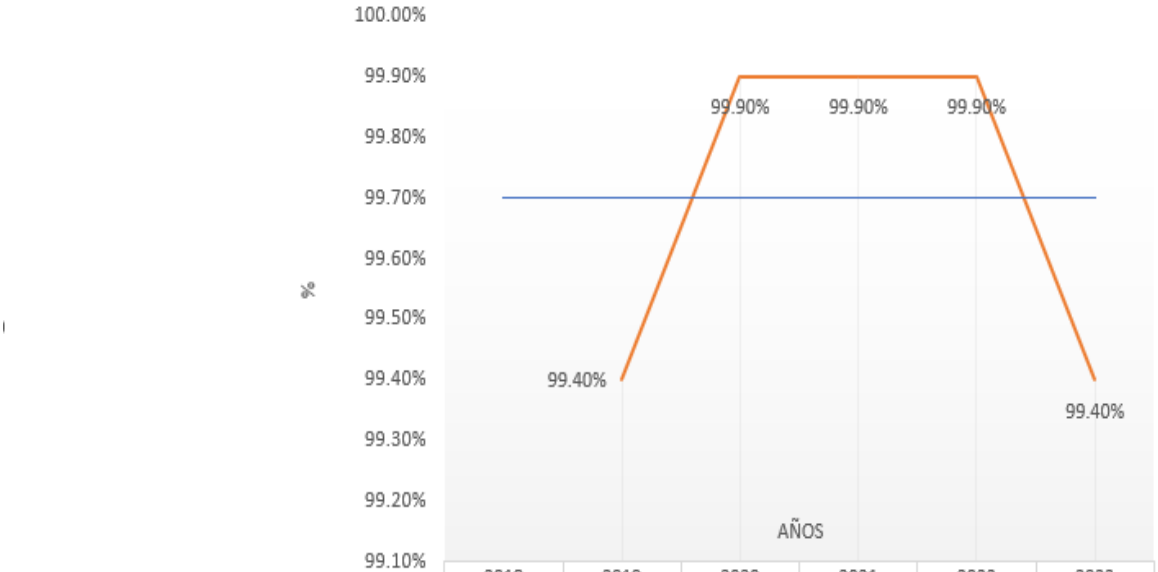
Los resultados han mostrado variaciones a lo largo de los años:

- En 2018, el resultado fue del 91.80%, indicando una efectividad por debajo de la meta.
- En 2019, hubo una disminución adicional a 89.00%, mostrando una baja efectividad.
- En 2020, se observa una mejora significativa alcanzando un 98.90%.
- En 2021 y 2022, la efectividad continúa mejorando, llegando al 99.80% y 99.81%, respectivamente.
- En 2023, hay una ligera disminución a 98.90%.

A partir del año 2019 se adquirió un nuevo antivirus Sophos el cual ha permitido mejorar la efectividad en la mitigación del riesgo.



% de Disponibilidad del Servicio de Conectividad: La meta establecida para el porcentaje de disponibilidad del servicio de conectividad es del 99%. Los resultados muestran niveles superiores al 99% en todos los años, indicando un desempeño consistente y cumplimiento de la meta.



	2018	2019	2020	2021	2022	2023
% porcentaje de disponibilidad del servicio de conectividad		99.40%	99.90%	99.90%	99.90%	99.40%

BIBLIOGRAFÍA

- Constitución Política de Colombia. Artículo 15.
- Ley 44 de 1993. Por la cual se modifica y adiciona la Ley 23 de 1982 y se modifica la Ley 29 de 1944 y Decisión Andina 351 de 2015 (Derechos de autor).
- Ley 527 de 1999. Por la cual se define y reglamenta el 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.
- Ley 594 de 2000. Por medio de la cual se expide la Ley General de Archivos.
- Ley 850 de 2003. Por medio de la cual se reglamentan las veedurías ciudadanas
- Ley 1266 de 2008. Por la cual se dictan las 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 y se dictan otras disposiciones.
- Ley 1221 del 2008. Por la cual se establecen normas para promover y regular el Teletrabajo y se dictan otras disposiciones.
- 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.
- Decreto 886 de 2014. Por el cual se reglamenta el Registro Nacional de Bases de Datos.
- Decreto 1008 del 2018. Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones.
- Resolución 2999 del 2008. Por el cual se adoptan las políticas de seguridad para el manejo de la información y se dictan otras normas para el uso y administración de los bienes y servicios informáticos del Ministerio TIC.
- Resolución 2007 de 2018. Por la cual se actualiza la política de tratamiento de datos personales del Ministerio/Fondo TIC.
- CONPES 3701 de 2011. Lineamientos de Política para Ciberseguridad y Ciberdefensa.
- CONPES 3854 de 2016. Política Nacional de Seguridad digital

Fin del documento.

ACTUALIZADO POR:

WILLIAM MONTENEGRO GUEVARA
Profesional Universitario

REVISADO POR:

HARVEY ALEXIS VALLEJO NARVAEZ
Jefe Oficina Asesora de Comunicaciones y Sistemas

APROBADO POR:

SEBASTIAN GRANJA ORDOÑEZ
Gerente (E)