



Para la ESE Centro de Salud Santa
Isabel de Buena vista el Talento
Humano es su capital más valioso.

Plan de Seguridad y Privacidad de la Información.

ESE Centro de Salud Santa Isabel
de Buenavista

2024

Gerente:
Edith Aleida Ballesteros Peña

Elaborado: Hermes González Flórez

ESE CENTRO DE SALUD DE BUENAVISTA		
	PLAN ESTRATEGICO DE TALENTO HUMANO	CÓDIGO: 1.1.M01
	PROCESO DIRECCIONAMIENTO ESTRATEGICO	VERSIÓN: 01
		FECHA: Ene. 31 de 2022

TABLA DE CONTENIDO

INTRODUCCIÓN	3
OBJETIVO GENERAL.....	4
OBJETIVOS ESPECÍFICOS	4
ALCANCE Y RESPONSABILIDADES	4
SEGURIDAD DE LA INFORMACION Y PROTECCIÓN DE DATOS	5
PROTECCIÓN DE DATOS	5
AMENAZAS Y VULNERABILIDADES	6
AMENAZAS.....	6
VULNERABILIDADES	6
ANALISIS DE RIESGO	7
CLASIFICACION Y FLUJO DE INFORMACION.....	7
ANALISIS DE RIESGO	8
OBTENCION Y ALMACENAMIENTO DE COPIAS DE SEGURIDAD (BACKUPS)	9

ESE CENTRO DE SALUD DE BUENAVISTA		
	PLAN ESTRATEGICO DE TALENTO HUMANO	CÓDIGO: 1.1.M01
	PROCESO DIRECCIONAMIENTO ESTRATEGICO	VERSIÓN: 01
		FECHA: Ene. 31 de 2022

INTRODUCCIÓN

El plan de tratamiento de riesgos de Seguridad y Privacidad de la información, Seguridad Digital y Continuidad de la Operación, se basa en una orientación estratégica que requiere el desarrollo de una cultura de carácter preventivo, de manera que, al comprender el concepto de riesgo, así como el contexto, se planean acciones que reduzcan la afectación a la entidad en caso de materialización, adicional se busca desarrollar estrategias para la identificación, análisis, tratamiento, evaluación y monitoreo de dichos riesgos con mayor objetividad, dando a conocer aquellas situaciones que pueden comprometer el cumplimiento de los objetivos trazados en el Entorno TIC para el Desarrollo Digital, ciudadanos y hogares empoderados del Entorno Digital, Transformación Digital Sectorial y Territorial e Inclusión Social Digital.

Lo anterior dando cumplimiento a la normativa establecida por el estado colombiano, CONPES 3854 de 2016, Modelo de Seguridad y Privacidad de MINTIC y lo establecido en el decreto 1008 de 14 de junio 2018, adoptando las buenas prácticas y los lineamientos de los estándares ISO 27001:2013, ISO 31000:2018 y la guía para la administración del riesgo y el diseño de controles en entidades públicas - Riesgos de gestión, corrupción y seguridad digital - Versión 4 emitida por el DAFP.

ESE CENTRO DE SALUD DE BUENAVISTA		
	PLAN ESTRATEGICO DE TALENTO HUMANO	CÓDIGO: 1.1.M01
	PROCESO DIRECCIONAMIENTO ESTRATEGICO	VERSIÓN: 01
		FECHA: Ene. 31 de 2022

OBJETIVO GENERAL

Establecer los conceptos básicos y metodológicos para una adecuada administración de riesgos a partir de su identificación, manejo y seguimiento dentro del plan de seguridad y privacidad de la información.

OBJETIVOS ESPECÍFICOS

- Involucrar y comprometer a todos los funcionarios en la formulación e implementación de controles y acciones encaminadas a prevenir y administrar los riesgos.
- Establecer, mediante una adecuada administración del riesgo, una base confiable para la toma de decisiones y la planificación institucional.
- Definir y aplicar los lineamientos para tratar de manera integral los riesgos de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación a la que la ESE Santa Isabel pueda estar expuesta, y de esta manera alcanzar los objetivos, la misión y la visión institucional, protegiendo y preservando la integridad, confidencialidad, disponibilidad y autenticidad de la información.

ALCANCE Y RESPONSABILIDADES

Realizar una eficiente gestión de riesgos de Seguridad y Privacidad de la información, Seguridad Digital y Continuidad de la Operación, que permita integrar en los procesos de la entidad, buenas prácticas que contribuyan a la toma de decisiones y prevenir incidentes que puedan afectar el logro de los objetivos. Este plan, proporcionará una metodología establecida por la ESE SANTA ISABEL DE BUENAVISTA, para la Administración y Gestión de los Riesgos a nivel interno; orienta sobre las actividades a desarrollar desde la definición del contexto estratégico, la identificación de los riesgos, su análisis y valoración de las opciones de manejo que pueden requerir la formulación de acciones adicionales para garantizar una adecuada gestión del riesgo.

ESE CENTRO DE SALUD DE BUENAVISTA		
	PLAN ESTRATEGICO DE TALENTO HUMANO	CÓDIGO: 1.1.M01
	PROCESO DIRECCIONAMIENTO ESTRATEGICO	VERSIÓN: 01
		FECHA: Ene. 31 de 2022

SEGURIDAD DE LA INFORMACIÓN 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.

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

El motivo para implementar medidas de protección, que 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 los datos, le puede causar un daño (material o inmaterial).

PROTECCIÓN DE DATOS

En el caso de la Protección de Datos, el objetivo de la protección no son los datos en sí mismos, sino el contenido de la información sobre personas, para evitar el abuso de esta. Esta vez, el motivo o el motor para la implementación de medidas de protección, por parte de la ESE, es la obligación jurídica o la simple ética personal, de evitar consecuencias negativas para las personas de las cuales se trata la información. Pero una buena Gestión de Riesgos no es una tarea única sino un proceso dinámico y permanente que tiene que estar integrado en los procesos (cotidianos) de la estructura institucional, que debe incluir a todas y todos los funcionarios. Si estas características esenciales no están garantizadas, las medidas de protección implementadas no funcionarán y son una pérdida de recursos.

ESE CENTRO DE SALUD DE BUENAVISTA		
	PLAN ESTRATEGICO DE TALENTO HUMANO	CÓDIGO: 1.1.M01
	PROCESO DIRECCIONAMIENTO ESTRATEGICO	VERSIÓN: 01
		FECHA: Ene. 31 de 2022

AMENAZAS Y VULNERABILIDADES

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, los Elementos de Información.

Debido a que la Seguridad Informática tiene como propósitos de garantizar la confidencialidad, integridad, disponibilidad y autenticidad de los datos e informaciones, las amenazas y los consecuentes daños que puede causar un evento de estos, deben ser reducidas a cero.

Desde el punto de vista de la entidad que maneja los datos, existen dos tipos de amenazas:

- Amenazas de origen externo: se refiere a las agresiones técnicas (intentos de hackeo), naturales (inundaciones, terremotos, incendios) y humanas (robos, vandalismo).
- Amenazas de origen interno: se refiere a la negligencia del propio personal, a las condiciones técnicas (problemas eléctricos, falta de mantenimiento a discos duros y otros componentes de los equipos de cómputo) y a procesos operativos internos.

Existen amenazas que difícilmente se dejan eliminar (virus de computadora) y por eso es la tarea de la gestión de riesgo; preverlos, implementar medidas de protección para evitar o minimizar los daños causados por virus informáticos.

VULNERABILIDADES

La Vulnerabilidad es la condición y características del sistema mismo (incluyendo la entidad que lo maneja), que lo hace susceptible a amenazas, con el riesgo de sufrir algún daño.

La capacidad y posibilidad de un sistema de responder o reaccionar a una amenaza para evitar un daño o de recuperarse de un daño ya causado, se debe tener bien documentada en todo plan de seguridad y privacidad de la información.

Las vulnerabilidades están en directa interrelación con las amenazas porque si no existe una amenaza, tampoco existe la vulnerabilidad o no tiene importancia, porque no se puede ocasionar un daño.

ESE CENTRO DE SALUD DE BUENAVISTA		
	PLAN ESTRATEGICO DE TALENTO HUMANO	CÓDIGO: 1.1.M01
	PROCESO DIRECCIONAMIENTO ESTRATEGICO	VERSIÓN: 01
		FECHA: Ene. 31 de 2022

ANALISIS DE RIESGO

El primer paso en la Gestión de Riesgo, es el análisis de riesgo que tiene como propósito determinar los componentes de un sistema que requieren protección, sus vulnerabilidades que los debilitan y las amenazas que lo ponen en peligro, con el fin de valorar su grado de riesgo.

Evitar: es eliminar la probabilidad de ocurrencia o disminuir totalmente el impacto, lo que requiere la eliminación de la actividad o fuente de riesgo, eliminar la exposición y su expresión máxima es dejar una actividad. Por ejemplo, para evitar pérdida de documentación se prohíbe el ingreso a un área.

Prevenir: corresponde al área de planeación, esto es, planear estrategias conducentes a que el evento no ocurra o que disminuya su probabilidad. Un ejemplo de ello son las inspecciones el mantenimiento preventivo, las políticas de seguridad o las revisiones periódicas a los procesos

Reducir o mitigar: corresponde a la protección en el momento en que se presenta el riesgo se encuentra en esta categoría los planes de emergencia, planes de contingencia y copias de respaldo.

Dispersar: es dividir una actividad en diferentes componentes operativos, de manera que las actividades no se concentren en un mismo sitio o bajo una sola responsabilidad. Este es el caso de los contratos de suministro de partes, la ubicación de nodos, plantas alternas, equipos paralelos, contratar obras por tramos

Compartir: es involucrar a un tercero para que responda en todo o en parte por el riesgo que genera una actividad. Dentro de los mecanismos de transferencia se encuentran los siguientes: contratos de seguro, transferencia explícita por medio de cláusulas contractuales, derivados financieros.

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, sensible 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.

ESE CENTRO DE SALUD DE BUENAVISTA		
	PLAN ESTRATEGICO DE TALENTO HUMANO	CÓDIGO: 1.1.M01
	PROCESO DIRECCIONAMIENTO ESTRATEGICO	VERSIÓN: 01
		FECHA: Ene. 31 de 2022

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.

ANALISIS DE RIESGO

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:

$$\text{Riesgo} = \text{Probabilidad de Amenaza} \times \text{Magnitud de Daño.}$$

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 del daño”. La probabilidad de amenaza y la magnitud del daño pueden tomar condiciones entre Insignificante y Alta.

Se habla de un Impacto, cuando un ataque exitoso para el delincuente, perjudicó la confidencialidad, integridad, disponibilidad y autenticidad de los datos e informaciones, estimar la Magnitud de Daño generalmente es una tarea muy compleja. La manera más fácil es expresar el daño de manera cualitativa, lo que significa que aparte del daño económico, también se considera otros valores como daños materiales, daños a la imagen de la empresa, daños emocionales, entre otros. Expresarlo de manera cuantitativa, es decir calcular todos los componentes en un solo daño económico, resulta en un ejercicio aún más complejo y extenso.

Quando hablamos de un impacto?	Como valorar la Magnitud de Daño?
<ul style="list-style-type: none"> * Se pierde la Información / conocimiento. * Terceros tienen acceso a la información / conocimiento. * Información ha sido manipulada o está siendo manipulada 	<p>Consideración sobre las consecuencias de un impacto. ¿Quién sufrirá el daño?</p> <ul style="list-style-type: none"> * Incumplimiento de confidencialidad (interna y externa) * Incumplimiento de obligaciones * Costo de recuperación

ESE CENTRO DE SALUD DE BUENAVISTA		
	PLAN ESTRATEGICO DE TALENTO HUMANO	CÓDIGO: 1.1.M01
	PROCESO DIRECCIONAMIENTO ESTRATEGICO	VERSIÓN: 01
		FECHA: Ene. 31 de 2022

OBTENCION Y ALMACENAMIENTO DE COPIAS DE SEGURIDAD (BACKUPS)

Se debe contar con procedimientos para la obtención de las copias de seguridad de todos los elementos de software necesarios para asegurar la correcta ejecución de los sistemas en la ESE Centro de Salud, se debe implementar el sistema de almacenamiento realizando un protocolo de implementación y seguimiento.

ESE CENTRO DE SALUD DE BUENAVISTA

	PLAN ESTRATEGICO DE TALENTO HUMANO	CÓDIGO: 1.1.M01
	PROCESO DIRECCIONAMIENTO ESTRATEGICO	VERSIÓN: 01
		FECHA: Ene. 31 de 2022

DESCRIPCIÓN DEL PLAN

ACTIVIDAD	TAREA A DESARROLLAR PARA EL PLAN	FECHA DE INICIO	FECHA FINAL	RESPONSABLE DEL CUMPLIMIENTO Y SEGUIMIENTO	PRESUPUESTO PLANIFICADO	SEGUIMIENTO
Realizar el manual de políticas de seguridad y privacidad de la información	Elaboración de documento	1/01/2024	31/12/2024	Designado por Gerencia	\$ 0	Mensual
Crear políticas relacionadas con el cumplimiento del Modelo de Seguridad y Privacidad de la Información	Documento con políticas	1/01/2024	31/12/2024	Designado por Gerencia	\$ 0	Mensual
Crear los procedimientos relacionadas con el cumplimiento del Modelo de seguridad y privacidad de la información	Documento con procedimientos a seguir para cada caso	1/01/2024	31/12/2024	Designado por Gerencia	\$ 0	Mensual
Realizar campañas y/o sesiones de socialización y sensibilización de las políticas de seguridad y privacidad de la información	Socialización de las políticas y procedimientos con los empleados de la ESE	1/01/2024	31/12/2024	Designado por Gerencia	\$ 0	Mensual
Desarrollar el inventario de activos de información de TI	Además de las hojas de vida de los equipos de computo, crear documento con documentación sobre el software usado en la institución	1/01/2024	31/12/2024	Designado por Gerencia	\$ 0	Mensual
Implementar la Ley 1581:2012 sobre protección de datos personales	Creación de formatos	1/01/2024	31/12/2024	Designado por Gerencia	\$ 0	Mensual
Elaborar la matriz de riesgos de seguridad de la información	Elaboración de documento	1/01/2024	31/12/2024	Designado por Gerencia	\$ 0	Mensual
Elaborar el plan de tratamiento de riesgos de seguridad de la información	Elaboración de documento	1/01/2024	31/12/2024	Designado por Gerencia	\$ 0	Mensual

ESE CENTRO DE SALUD DE BUENAVISTA		
	PLAN ESTRATEGICO DE TALENTO HUMANO	CÓDIGO: 1.1.M01
	PROCESO DIRECCIONAMIENTO ESTRATEGICO	VERSIÓN: 01
		FECHA: Ene. 31 de 2022

9. CONTROL DOCUMENTAL

ITEM	ELABORÓ	REVISÓ	APROBÓ
Nombre	Hermes González Flórez	Jesica Rincón Quiñonez	Edith Aleida Ballesteros Peña
Cargo	Asesor (Ing. de Sistemas)	Asesor Calidad Y Control Interno	Gerente
Fecha	26/01/2024	31/01/2024	31/01/2024

VERSIÓN	FECHA	RAZÓN
1	Ene. 31 de 2023	Definición inicial del documento