PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

ESE SANTA ISABEL

BUENAVISTA – BOYACÁ

Enero 2023

TABLA DE CONTENIDO

Contenido

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.

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.

SEGURIDAD DE LA INFORMACIÒN 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, justificación 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.

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.

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 o el motor 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). Entonces en referencia al ejercicio con el banco, la pérdida o la modificación errónea, sea causado intencionalmente o simplemente por negligencia humana, de algún récord de una cuenta bancaria, puede resultar en pérdidas económicas u otras consecuencias negativas para la ESE

PROTECCIÓN DE DATOS

En el caso de la Protección de Datos, el objetivo de la protección no son los datos en sí mismo, 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 -¡¡la falla el eslabón más débil de la cadena!!- y que requiere el reconocimiento y apoyo de las directivas. Sin estas

Características esenciales no están garantizadas, las medidas de protección implementadas no funcionarán y son una pérdida de recursos.

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 exitoso, también hay que ver en 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 como por ejemplo las agresiones técnicas, naturales o humanos, sino 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

- Criminalidad: Son todas las acciones, causado por la intervención humana, que violan la ley y que están penadas por esta. Con criminalidad política se entiende todas las acciones dirigido desde el gobierno hacia la sociedad civil.

- Sucesos de origen físico: Son todos los eventos naturales y técnicos, sino también eventos indirectamente causados por la intervención humana.

- 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 realice una amenaza.

VULNERABILIDADES

La Vulnerabilidad es la capacidad, las condiciones y características del sistema mismo (incluyendo la entidad que lo maneja), que lo hace susceptible a amenazas, con el resultado de sufrir algún daño. En otras palabras, es la capacitad y posibilidad de un sistema de responder o reaccionar a una amenaza o de recuperarse de un daño.

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.

Dependiendo del contexto de la institución, se puede agrupar las vulnerabilidades en grupos característicos: Ambiental, Física, Económica, Social, Educativo, Institucional y Política.

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 perdida 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 continencia equipos de protección personal, ambiental, de acceso mantener 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 explicita 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, 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.

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 x 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 y Alta (4). En la práctica no es necesario asociar valores aritméticos a las condiciones de las variables.

Cuando hablamos de un impacto?	Como valorar la Magnitud de Daño?
• Se pierde la Información / conocimiento. • Terceros tienen acceso a la información/conocimiento. • Información ha sido manipulada o está	• Consideración sobre las consecuencias de un impacto. - ¿Quién sufrirá el daño? - Incumplimiento de confidencialidad (interna y externa) - Incumplimiento de obligación - Costo de recuperación (imagen, emocional, recursos,

Se habla de un Impacto, cuando un ataque exitoso 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, imagen,

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.

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 Puesto de Salud, se debe implementar el sistema de almacenamiento realizando un protocolo de implementación y seguimiento.

Plan de Seguridad y Privacidad de la Información						
9. DESCRIPCIÓN DEL PLAN						
ACTIVIDAD	**TAREA A DESARROLLAR PARA EL PLAN**	**FECHA INICIO**	**FECHA FINALIZACIÓN**	**RESPONSABLE DEL CUMPLIMIENTO Y SEGUIMIENTO**	**PRESUPUESTO PLANIFICADO**	**SEGUIMIENTO**
realizar el manual de políticas de seguridad y privacidad de la información	Diagnostico	1/08/2023	31/03/2023	Designado por la alta dirección	$0,00	Mensual
Crear políticas relacionadas con el cumplimiento del Modelo de Seguridad y Privacidad de la Información	Elaborar la documentación asociada a las políticas de seguridad de la información del MSPI	1/02/2021	31/03/2023	Designado por la alta dirección	$0,00	Mensual
Crear los procedimientos relacionadas con el	Elaborar la documentación			Designado		

cumplimiento del Modelo de seguridad y privacidad de la información	asociada a los procedimientos, guías e instructivos de seguridad de la información del MSPI	1/02/2021	31/03/2023	por la alta dirección	$0,00	Mensual

*

Realizar campañas y/o sesiones de socialización y sensibilización de las políticas de seguridad y privacidad de la información	Realizar la socialización y sensibilización a la comunidad sobre las políticas de seguridad de la información	1/03/2023	30/04/2023	Designado por Gerencia	$0,00	Mensual
Desarrollar el inventario de activos de información de TI	Desarrollar el inventario de activos de información de TI	01/05/2023	31/05/2023	Designado por gerencia	$0,00	Mensual

Implementar la Ley 1581:2012 sobre protección de datos personales	Elaborar políticas de protección de datos	01/08/2023	31/12/2023	Designado por gerencia	$0,00	Mensual
	Elaborar formatos para la autorización de datos personales	1/08/2023				
	Realizar la socialización sobre la Ley 1581:2012	1/08/2023				
Elaborar la matriz de riesgos de seguridad de la información	realizar el levantamiento de riesgos de seguridad de la información	1/08/2023	11/07/2023		$0,00	Mensual

Elaborar el plan de tratamiento de riesgos de seguridad de la información	Elaborar y revisar del plan de tratamiento de riesgos de seguridad	1/08/2023	11/07/2023	Líder de Seguridad de la Información	$0,00	Mensual