TABLA DE CONTENIDO

TABLA DE TABLAS

Pág.

INTRODUCCIÓN

El uso de las tecnologías de la información y la comunicación es esencial para el progreso y éxito de países, instituciones y empresas. La información que se maneja en estos ámbitos es un activo cada vez más valioso y puede determinar el éxito o fracaso de una organización. Por lo tanto, es crucial utilizar herramientas y procesos que aseguren, respalden y mantengan la información de manera óptima y redundante.

Sin embargo, muchas empresas subestiman la importancia de la seguridad informática y no prestan suficiente atención a los riesgos actuales, como las amenazas internas, como los errores humanos, y las amenazas externas, como los virus. Esta falta de inversión en capital humano y recursos económicos para prevenir daños o pérdidas de información resulta en datos poco confiables, integridad comprometida y falta de disponibilidad para la empresa. En muchos casos, esto lleva a la paralización de las operaciones, causando pérdidas significativas de tiempo y dinero, factores cruciales para el desarrollo de cualquier organización.

Para hacer frente a estos desafíos, las empresas desarrollan el Plan Estratégico de Seguridad y Privacidad de la Información (PESI), que tiene como objetivo reducir o abordar las vulnerabilidades y riesgos relacionados con la seguridad de la información. Este plan se convierte en una parte fundamental de las actividades estratégicas de las organizaciones para garantizar un entorno seguro y confiable para el manejo de la información y así respaldar su crecimiento y desarrollo.

ALCANCE

El propósito de este documento es proporcionar un marco de trabajo que permita a la empresa mantener su información segura frente a diversas amenazas. Para lograr esto, se propone la creación de un programa estratégico de seguridad de información que reduzca los riesgos a los que la organización está expuesta, tanto en sus datos como en su infraestructura.

El programa se inicia con la identificación y planteamiento de proyectos de tecnologías de la información que ayuden a contrarrestar los efectos de la falta de seguridad informática. A continuación, se busca aprovechar y utilizar de manera efectiva los recursos disponibles para llevar a cabo estos proyectos. Finalmente, se lleva a cabo la implementación y puesta en marcha de los proyectos propuestos.

Este programa estratégico también incluye evaluaciones de seguridad y un análisis exhaustivo de los riesgos presentes. Esto permite desarrollar políticas de seguridad informática que se integren de manera concreta dentro del marco general del programa. Al combinar todos estos elementos, la empresa podrá mantener una concienciación constante sobre la seguridad de su información y tomar medidas proactivas para protegerse de posibles amenazas.

1. DEFINICIONES

Con el fin de entender el tema desarrollado dentro de este programa es necesario conocer ciertos términos que serán usados durante el transcurso de todo el documento para su conocimiento y entendimiento.

Factores de riesgos: Manifestaciones o características medibles u observables de un proceso que indican la presencia de riesgo o tienden a aumentar la exposición, pueden ser interna o externa a la entidad.

Impacto: Es la medición y valoración del daño que podría producir a la empresa un incidente de seguridad. La valoración global se obtendrá sumando el coste de reposición de los daños tangibles y la estimación, siempre subjetiva, de los daños intangibles.

Riesgo: Proximidad o posibilidad de un daño, peligro, etc. Cada uno de los imprevistos, hechos desafortunados, etc., que puede cubrir un seguro.

Seguridad: Cualidad o estado de seguro. Garantía o conjunto de garantías que se da a alguien sobre el cumplimiento de algo. Se dice también de todos aquellos objetos, dispositivos, medidas, etc., que contribuyen a hacer más seguro el funcionamiento o el uso de una cosa: cierre de seguridad, cinturón de seguridad.

Seguridad física: Consiste en la aplicación de barreras físicas y procedimientos de control, como medidas de prevención ante amenazas a los recursos e información confidencial que puedan interrumpir procesamiento de información.

Seguridad lógica: Consiste en la aplicación de barreras y procedimientos para mantener la seguridad en el uso de software, la protección de los datos, procesos y programas, así como la del acceso ordenado y autorizado de los usuarios a la información.

Seguridad de las redes: Es la capacidad de las redes para resistir, con un determinado nivel de confianza, todos los accidentes o acciones malintencionadas, que pongan en peligro la disponibilidad, autenticidad, integridad y confidencialidad de los datos

almacenados o transmitidos y de los correspondientes servicios que dichas redes ofrecen o hacen accesibles y que son tan costosos como los ataques intencionados.

Seguridad Informática: Son técnicas desarrolladas para proteger los equipos informáticos individuales y conectados en una red frente a daños accidentales o intencionados.

Vulnerabilidad: Cualquier debilidad en los Sistemas de Información que pueda permitir a las amenazas causarles daños y producir pérdidas.

2. DIRECCIONAMIENTO ESTRATÉGICO

2.1. Misión

Somos un Instituto Público de servicios educativos en formación para el trabajo, que contribuye a mejorar la competitividad y la calidad de vida hacia el desarrollo humano y socio-económico del Municipio de Yumbo.

2.2. Visión

Constituirnos en Instituto Técnico Superior con formación para el trabajo y Agencia Pública de Gestión y Colocación de Empleo reconocido a nivel regional por su competitividad, pertinencia, Calidad Educativa y gestión de la empleabilidad, que se adapta a las necesidades y expectativas de nuestros grupos de valor, con personal íntegro y ambientes modernos.

2.3. Principios Éticos

Los principios se refieren a las ideas fundamentales sobre las que se basa el pensamiento que precede la conducta, desde los cuales se funda el sistema de valores al que la persona o los grupos se adscriben. Estos se presentan como postulados que el individuo y el colectivo asumen como patrón que orienta su conducta y que no permiten la negociación. La empresa se reconoce y se actúa sobre los siguientes principios éticos:

2.4. Valores Empresariales

Los valores empresariales que regirán la actuación de la organización, todos los servidores públicos y particulares que ejercen funciones de la organización en general están enmarcados por el código de integridad y son los siguientes:

- **Honestidad:** Los servidores públicos y particulares que ejercen funciones y cualquiera actividad para la entidad actuarán con rectitud, honradez, veracidad en todos y cada uno de los actos de la vida, favoreciendo siempre el interés general.

- **Respeto:** Los servidores públicos y particulares que ejercen funciones y cualquiera actividad para la entidad reconocerán, valoraran y trataran de manera digna a todas las personas, con sus virtudes y defectos, sin importar su labor, su procedencia, títulos o cualquier otra condición.

- **Compromiso**: Los servidores públicos y particulares que ejercen funciones y cualquiera actividad para la entidad serán conscientes de la importancia del rol que como servidores públicos y de la disposición permanente para comprender y resolver las necesidades de las personas con las que se relacionan en las labores cotidianas, buscando siempre mejorar su bienestar.

- **Diligencia:** Los servidores públicos y particulares que ejercen funciones y cualquiera actividad para la entidad cumplirán con los deberes, funciones y responsabilidades asignadas a mi cargo de la mejor manera posible, con atención, prontitud, destreza y eficiencia, para así optimizar el uso de los recursos del Estado.

- **Justicia:** Los servidores públicos y particulares que ejercen funciones y cualquiera actividad para la entidad actuaran con imparcialidad garantizando los derechos de las personas, con equidad, igualdad y sin discriminación.

- **Cordialidad:** Genero una relación personal a partir de la humanización fundamentada en el buen trato, el buen lenguaje y los buenos modales hacia los demás.

- **Motivación:** Reconozco y transmito la fuerza interior que me permite ser líder y buen empleado cumpliendo los objetivos institucionales con efectividad.

3. IMPORTANCIA DE LA SEGURIDAD DE INFORMACIÓN

La información es la sangre de todas las organizaciones y sin ella la empresa dejaría de funcionar, principalmente si hablamos de empresas altamente automatizadas por lo que su seguridad sigue siendo un punto pendiente y por tanto el factor más determinante por el cual fracasan.

Es fundamental comprender que, a pesar de considerar nuestra institución como segura, el creciente uso de nuevas tecnologías para gestionar información nos expone a un mayor número y variedad de amenazas. En el competitivo entorno actual, es vital que las entidades aseguren la confidencialidad, integridad y disponibilidad de su información corporativa clave.

La seguridad informática debe ser el resultado de una colaboración entre los responsables de la seguridad de la información, quienes deben implementar las medidas disponibles, y los usuarios, quienes deben ser conscientes de los riesgos asociados con ciertos usos de los sistemas y recursos. Cada vez que se enfrentan a problemas de seguridad, se pierde tiempo de producción y el consumo de recursos durante la recuperación de la actividad normal, lo que en muchos casos es irreparable.

Sin embargo, gran parte de esta concienciación recae en los responsables de seguridad de la información, respaldados de manera explícita y activa por la Dirección. Es crucial informar no solo sobre las principales amenazas en cada momento, sino también sobre las acciones que deben tomarse para evitarlas, estableciendo procedimientos efectivos que complementen las medidas técnicas implementadas por el equipo de informática.

Por lo tanto, en este nuevo entorno, las empresas deben prepararse no solo para prevenir el riesgo de comprometer sus operaciones comerciales debido a una falla de seguridad, sino también para establecer medidas que reduzcan los problemas de seguridad potenciales.

El objetivo de este documento es presentar un marco de trabajo para el establecimiento, implementación, operación, monitoreo, revisión y mejora continua del Sistema de Gestión de Seguridad y Privacidad de la información del IMETY. Con esta iniciativa, buscamos fortalecer la seguridad y privacidad de nuestros datos, protegiendo nuestros recursos y garantizando la confianza de nuestros clientes y socios en nuestro manejo de la información.

4. OBJETIVOS

4.1. Objetivo general

Establecer el PESI a través de un marco de trabajo orientado a diferentes proyectos que permitan establecer, implementar, operar, monitorear, revisar y una mejora continua en el sistema de Gestión de Seguridad y Privacidad de la Información en la empresa.

4.2. Objetivos específicos

- Presentar los proyectos a realizar dentro del alcance del programa, teniendo en cuenta, alcance, tiempo y presupuesto.
- Alinear los proyectos con el programa y objetivos estratégicos de la empresa.
- Asociar los objetivos de cada proyecto a dar solución a los riesgos expuestos en la matriz de riesgos de seguridad informática de la empresa.
- Desarrollar los proyectos dentro los tiempos y lineamientos establecidos por la empresa.

5. MARCO DE TRABAJO DE PROYECTOS

El programa estratégico de seguridad de la información se desarrolla siguiendo los lineamientos dados por los siguientes documentos:

- ISO 27001
- Autoevaluación MSPI
- Análisis de vulnerabilidades y riesgos de TI de la empresa.
- Programa de tratamiento de Riesgos
- Artículo 6 - Ley 1581 de 2012: Tratamiento de datos sensibles. Se prohíbe el Tratamiento de datos sensibles.
- Artículo 17 - Ley 1581 de 2012: Deberes de los responsables del Tratamiento. Los responsables del Tratamiento deberán cumplir los deberes, sin perjuicio de las demás disposiciones previstas en la presente ley y en otras que rijan su actividad.

- Artículo 18 - Ley 1581 de 2012: Deberes de los Encargados del Tratamiento. Los Encargados del Tratamiento deberán cumplir los deberes, sin perjuicio de las demás disposiciones previstas en la presente ley y en otras que rijan su actividad.
- Articulo 13 - Ley 1712 de 2014: Registros de Activos de Información. Todo sujeto obligado deberá crear y mantener actualizado el Registro de Activos de Información.
- Articulo 17 - Ley 1712 de 2014: Sistemas de información. Para asegurar que los sistemas de información electrónica sean efectivamente una herramienta para promover el acceso a la información pública

Con la información recolectada por los documentos anteriores se define según la prioridad y las buenas prácticas de seguridad informática, los proyectos alienados a dar cumplimiento a las políticas y estándares nacionales en materia de TI. Se define un plazo de ejecución para la vigencia 2024, teniendo en cuenta el alcance, tiempo, riesgo y presupuesto.

6. PROYECTOS ESTRATÉGICOS

Tabla 1: Proyectos Estratégicos

Nombre	Implementación de sistema de gestión de seguridad y privacidad de la información.
Prioridad	1
Descripción	Implementar un sistema integral de gestión de la seguridad y privacidad de la información, mediante el seguimiento de las actividades presentadas en la norma ISO 27001 y el MSPI.
Actividades del Proyecto	1. Lista de chequeo de actividades ISO 27001. 2. Lista de chequeo de actividades MSPI. 3. Seguimiento programa de tratamiento de Riesgos. 4. Implementación de programa de cierre de brechas. 5. Capacitación de seguridad informática (Sensibilización). 6. Creación de comité de seguridad y privacidad de la información. 7. Definición de procesos de seguridad y privacidad de la información.

Nombre	Implementación de sistema de gestión de seguridad y privacidad de la información.
	8. Auditoría externa de seguridad informática. 9. Actualización de los activos de información y bases de datos personales. 10. Pruebas periódicas de vulnerabilidades y ethical hacking. 11. Definir procesos de fortalecimiento del sistema de gestión de seguridad y privacidad de la información.
Objetivos del Proyecto	• Realizar acciones para proteger, preservar y gestionar los activos de información, bases de datos y tecnologías dentro de la empresa con el fin de mantener la integridad y confidencialidad de la información. • Definir controles periódicos para la prevención y mitigación de riesgos de seguridad de la información. • Disponer de medidas para atender los incidentes y eventos de seguridad informática. • Fortalecer la cultura de la seguridad informática en la entidad a través de los diferentes planes, proyectos, programas y capacitaciones de seguridad informática
Tiempo estimado de ejecución	11 meses.

7. PROGRAMACIÓN 2024

A continuación, se muestra una propuesta de programación para la ejecución de los proyectos y actividades del PESI, el tiempo de ejecución de las actividades es de 1 año:

Tabla 2: Programación 2024

	PROGRAMACIÓN
1	Implementar un sistema integral de gestión de la seguridad y privacidad de la información basado en la norma ISO 27001 y el MSPI.

8. ACTUALIZACIÓN DEL PESI

Este programa estratégico se podrá actualizar dependiendo de los cambios en la estratégica organizacional de la institución, cambios o daños significativos en la

infraestructura tecnológica de la empresa, incidentes de seguridad o privacidad de la información que tengan un impacto general muy alto, hay que tener en cuenta que las modificaciones de este programa solo podrán ser autorizadas con el visto bueno de la dirección, el personal de informática y el personal de planeación estratégica de la institución.

9. REFERENCIAS

M. Hernández, "Diseño de un plan estratégico de seguridad de información en una empresa del sector comercial" (Tesis, Instituto de Ciencias Matemáticas, Escuela Superior Politécnica del Litoral, 2006).

Echenique García José Antonio, Auditoria en Informática (2da Edición, Mc. Graw Hill, 2001), pp. 194-241.

Laudon Kenneth C. y Laudon Jane P, Administración de los Sistemas de Información, Organización y Tecnología (3ra Edición, México, Prentice Hall Hispanoamericana S.A., 1994), pp. 702-706.

Lucena López Manuel José, Criptografía y Seguridad en Computadoras (2da Edición, Universidad de Jaen, 1999), pp. 30-138.

Norton Peter, Introducción a la Computación (1ra Edición, México, Mc Graw Hill), pp. 50-53.

Simson Garfinkel y Spafford Gene, Seguridad y Comercio en el Web (México, Mc. Graw Hill, 1999), pp. 8-13.

Simson Gar Finkel, y Spafford Gene, Seguridad Práctica en UNIX e Internet (2da Edición, Mc. Graw Hill, 1999), pp.360-366.

REVISO: INGMART	**CARGO:** CONTRATISTA	**FIRMA:**
APROBO: RUBEN DARIO MILLAN	**CARGO:** DIRECTOR	**FIRMA:**

ANEXOS

Anexo A. Control de Cambios

Versión	Fecha (dd/mm/aaaa)	Revisado por:	Aprobado por:	Descripción de la actualización
01	17/01/2019	Manuel Alberto Torres	Carlos Arturo Tello Becerra	Creación del Plan
02	28/06/2019	Christian Valencia	Carlos Arturo Tello Becerra	Actualización del Plan, en donde se modifica el objetivo, alcance, justificación, seguimiento y evaluación y la mejora continua.
03	30/01/2020	Ruben Barreto / Johanna Orejuela	Jaime Sánchez Lenis	Actualización del Plan. Se incluye la política y el cronograma de implementación para la vigencia 2020.
04	27/01/2020	Jhon Jairo Ortiz	Jaime Sánchez Lenis	Se actualiza la información referente a la política de seguridad y privacidad de la información, seguridad digital y continuidad del servicio del Instituto Municipal de Educación para el Trabajo y el Desarrollo Humano de Yumbo – IMETY y el cronograma de implementación para la vigencia 2021.
05	26/11/2021	Ruben Barreto	Jaime Sánchez Lenis	Actualización del Plan. Se incluye la gestión de aplicativos de operación de la entidad y el usuario administrador de los mismos, para la vigencia 2021.
06	24/01/2022	Claudia Vélez Arias Ruben Barreto	Jaime Sánchez Lenis	Cambios de actividades y fechas
07	31/01/2023	Ruben Barreto	Ruben Dario Millán	Implementar le MSPI en la entidad de acuerdo a la actividad del negocio, según Mintic y se cambio fecha de las actividades.
08	01/11/2023	Jose Cristian Valencia	Ruben Dario Millán	Actualización del Plan. Se incluye la gestión de aplicativos de operación de la entidad y el usuario administrador de los mismos, para la vigencia 2024.