PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DE LA EMPRESA DE SERVICIOS PÚBLICOS DE PAMPLONA EMPOPAMPLONA S.A E.S.P.

TABLA DE CONTENIDO.

INTRODUCCIÓN

El “Plan de Privacidad y Seguridad de la Información” contempla actividades encaminadas a salvaguardar la información. Incluye definir el alcance, identificar procesos y servicios, evaluar activos, clasificar activos de información, determinar dependencias, identificar amenazas y vulnerabilidades, evaluar impactos y probabilidades de amenazas y establecer controles para el tratamiento de riesgos.

Este plan es crucial para garantizar la protección de la información al abordar los riesgos de seguridad y las preocupaciones de privacidad dentro de una organización o entidad.

OBJETIVO.

Garantizar la protección de datos contra amenazas externas e internas, asegurar la confidencialidad e integridad de la información, prevenir acciones no autorizadas como uso, divulgación, distorsión, alteración, investigación y destrucción de la información, y establecer controles para mitigar riesgos.

Además, el objetivo busca mantener la integridad, disponibilidad, privacidad, control, y autenticidad de la información manejada, así como proteger los datos confidenciales del acceso no autorizado, garantizando que solo personas autorizadas tengan acceso a la información sensible.

ALCANCE

El plan de seguridad y privacidad de la información abarca una serie de actividades esenciales para proteger la información. Esto incluye la definición del alcance, identificación de procesos y servicios, valoración y clasificación de activos de información, determinación de dependencias, identificación de amenazas y vulnerabilidades, evaluación de impactos y probabilidades de amenazas, y establecimiento de controles para el tratamiento de riesgos.

Además, este alcance se extiende a garantizar la confidencialidad, integridad, disponibilidad, control y autenticidad de la información manejada, así como a proteger los datos confidenciales contra accesos no autorizados.

DEFINICIONES.

Las definiciones asociadas al plan de seguridad y privacidad de la información incluyen términos clave relacionados con la protección de datos y la seguridad informática. Algunos de estos términos son:

Ciberseguridad: Conjunto de tecnologías, procesos y prácticas diseñados para proteger redes, computadoras, programas y datos de ataques y daños.

Metadatos: Información que enriquece un documento al que está asociado.
Parche de seguridad: Conjunto de cambios aplicados a un software para corregir errores de seguridad.

Prueba de penetración (Pentest): Ataque a un sistema software o hardware con el objetivo de encontrar vulnerabilidades.

PCI DSS (Payment Card Industry Data Security Standard): Estándar de Seguridad de Datos para la Industria de Tarjetas de Pago.

Pharming: Ataque informático que aprovecha una vulnerabilidad del software de los servidores DNS.

Phishing: Estafa cometida a través de medios telemáticos para obtener información confidencial de forma fraudulenta.

Política de seguridad: Decisiones o medidas de seguridad que una empresa ha decidido tomar respecto a la seguridad de sus sistemas.

Puerta trasera (Backdoor): Punto débil de un programa o sistema que puede ser utilizado con fines ilícitos.

Gusano (Worm): Programa malicioso que se propaga rápidamente.

IDS (Intrusion Detection System): Sistema de detección de intrusos.

Estos términos son fundamentales para comprender y gestionar eficazmente la seguridad y privacidad de la información en entorno de nuestra organización.

PARTES INTERESADAS.

Grupos de interés de la empresa de servicios públicos de Pamplona Empopamplona S.A E.S.P. que accedan a los sistemas de información e instalaciones físicas de la entidad.

ESQUEMA DEL PLAN.

El Plan de Seguridad y Privacidad de la Información es la declaración general que representa la posición la empresa de servicios públicos de Pamplona Empopamplona S.A E.S.P .con respecto a la protección de los activos de información que soportan los procesos de la Entidad y apoyan la implementación del Sistema de Gestión de Seguridad de la Información.

DESARROLLO DEL PLAN.

de la empresa de servicios públicos de Pamplona Empopamplona S.A E.S.P., para asegurar la dirección estratégica de la Entidad, establece la compatibilidad de la política de seguridad de la información y las acciones a implementar son:

- ✓ Minimizar el riesgo de los procesos misionales de la entidad.
- ✓ Cumplir con los principios de seguridad de la información.
- ✓ Cumplir con los principios de la función administrativa.
- ✓ Mantener la confianza de los grupos de interés de la entidad.
- ✓ Apoyar la innovación tecnológica.
- ✓ Implementar el sistema de gestión de seguridad de la información.
- ✓ Proteger los activos de información.
- ✓ Establecer las políticas, en materia de seguridad de la información.
- ✓ Fortalecer la cultura de seguridad de la información en los grupos de interés de la entidad.
- ✓ Garantizar la continuidad del negocio frente a incidentes.

ELABORACIÓN DE POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Para crear una política de seguridad y privacidad de la información efectiva, es fundamental seguir un proceso estructurado que abarque los siguientes pasos:

Definir el Alcance y Objetivos:

Establecer el propósito y alcance de la política.

Definir los objetivos específicos de seguridad y privacidad de la información que se desean lograr.

Identificar los Activos de Información:

Identificar y clasificar los activos de información críticos para la organización.

Evaluar Riesgos:

Realizar una evaluación de riesgos para identificar amenazas, vulnerabilidades y posibles impactos en la seguridad de la información.

Establecer Controles:

Definir controles de seguridad apropiados para mitigar los riesgos identificados.

Incluir medidas técnicas, organizativas y procedimentales para proteger la información.

Implementar Procedimientos:

Desarrollar procedimientos claros para la gestión de incidentes, acceso a la información, protección de datos personales, entre otros.

Capacitación y Concientización:

Brindar capacitación regular a empleados sobre las políticas y procedimientos de seguridad.

Fomentar una cultura de conciencia sobre la importancia de la seguridad y privacidad de la información.

Revisión y Mejora Continua:

Realizar revisiones periódicas de la política para asegurar su eficacia.

Actualizar la política en función de cambios en el entorno tecnológico o normativo.

Al seguir estos pasos y adaptarlos a las necesidades específicas de nuestra organización, se puede crear una política sólida que garantice la protección adecuada de la información sensible y promueva una cultura de seguridad en toda la entidad.