PLAN DE TRATAMIENTO DE RIESGO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.

TABLA DE CONTENIDO.

INTRODUCCIÓN

El plan de tratamiento de riesgo de seguridad y privacidad de la información es fundamental en cualquier organización debido a su papel en proteger la privacidad y la integridad de los datos. Este plan implica identificar controles específicos para mitigar los riesgos asociados con el acceso no autorizado a los datos, lo que contribuye a garantizar la confidencialidad y la protección de la información sensible.

La implementación del plan de tratamiento de riesgo de seguridad y privacidad de la información es justificada por su papel crucial en proteger los datos sensibles de una organización. Este plan define acciones específicas para gestionar los riesgos de seguridad de la información inaceptables, lo que contribuye a garantizar la confidencialidad y la integridad de los datos

Al llevar a cabo este plan, se pueden identificar y aplicar controles que ayudan a mitigar los riesgos asociados con el acceso no autorizado a la información, fortaleciendo así la seguridad de la organización en su conjunto

La implementación de este plan no solo protege la información crítica de la organización, sino que también cumple con los estándares y regulaciones de seguridad de la información, lo que es fundamental en un entorno donde la protección de datos es cada vez más relevante y necesaria para evitar posibles brechas de seguridad y proteger la reputación de la organización.

OBJETIVO.

Establecer la gestión necesaria para mitigar los riesgos relacionados con la seguridad y privacidad de los datos en una organización. Este plan define las acciones específicas que se deben llevar a cabo para gestionar los riesgos de seguridad de la información inaceptables e implementar los controles necesarios para protegerla

Al tener este plan en marcha, se busca identificar y abordar los riesgos potenciales que podrían afectar la confidencialidad, integridad y disponibilidad de la información sensible, garantizando así la protección adecuada de los activos de información de la organización.

ALCANCE

Abarca la gestión integral de los riesgos asociados con la seguridad y privacidad de los datos en una organización. Este alcance implica determinar las acciones necesarias para identificar, evaluar y mitigar los riesgos de seguridad digital sobre los activos de información.

Además, el plan define las medidas específicas que se deben implementar para proteger la confidencialidad, integridad y disponibilidad de la información sensible, abarcando a todos los funcionarios y activos de la organización.

DEFINICIONES

Activos de información: en el contexto de la seguridad digital son elementos tales como aplicaciones de la organización, servicios web, redes, Hardware,

información física o digital, recurso humano, entre otros, que utiliza la organización para funcionar en el entorno digital.

Amenaza: causa potencial de un incidente no deseado, el cual puede ocasionar daño a un sistema o a una organización.

Ataque cibernético: Acción organizada y premeditada de una o más personas para causar daño o problemas a un sistema informático a través del ciberespacio. (Ministerio de Defensa de Colombia)

Consecuencia: Efectos o situaciones resultantes de la materialización del riesgo que impactan en el proceso, la entidad, sus grupos de valor y demás partes interesadas.

Confidencialidad: propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados.

Control: Medida que modifica al riesgo (procesos, políticas, dispositivos, prácticas u otras acciones).

Integridad: propiedad de salvaguardar la exactitud y estado completo de los activos.

Disponibilidad: propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada.

Riesgo cibernético: posibilidad de que se materialice una falla en la seguridad de los componentes tecnológicos o servicios de información, sistemas de control, sistemas electrónicos y las telecomunicaciones que por ataques o intrusiones

podrían impactar la movilidad de personas, alimentos, mercancías peligrosas y elementos esenciales y de carácter vital.

Enlace: son las personas designadas por los directivos de área para realizar la identificación de activos de información y la identificación y tratamiento de riesgos de seguridad digital.

Evento de seguridad de la información: presencia identificada de una condición de un sistema, servicio o red, que indica una posible violación de la política de seguridad de la información o la falla de las salvaguardas, o una situación desconocida previamente que puede ser pertinente a la seguridad.

Gestión de activos: consiste en obtener el máximo rendimiento de los bienes o recursos, es decir de todo aquello que tenga valor para una organización.

Infraestructuras criticas cibernéticas- ICC-: instalaciones, redes, servicios y equipos físicos y de tecnología de la información cuya interrupción o destrucción tendría un impacto mayor en la salud, la seguridad o el bienestar de los ciudadanos.

Mapa de riesgos: Documento con la información resultante de la gestión del riesgo.

Probabilidad: Posibilidad de ocurrencia del riesgo, ésta puede ser medida con criterios de frecuencia o factibilidad.

Tratamiento al riesgo: Respuesta establecida por la primera línea de defensa para la mitigación de los diferentes riesgos, incluyendo los riesgos de corrupción.

Vulnerabilidad: Debilidad, atributo, causa o falta de control que permitiría a explotación por parte de una o más amenazas contra los activos.

Riesgo de seguridad digital: combinación de amenazas y vulnerabilidades en el entorno digital. Puede debilitar el logro de objetivos económicos y sociales, así como afectar la soberanía nacional, la integridad territorial el orden institucional y los intereses nacionales, incluye aspectos relacionados con el aspecto físico, digital y las personas.

Seguridad digital: preservación de la confidencialidad, integridad y disponibilidad de la información; además, puede involucrar otras propiedades tales como: autenticidad, trazabilidad (Accountability), no repudio y fiabilidad.

Clasificación de Activos de información: orden y agrupación de los activos de información en función de los requisitos legales, valor, criticidad y susceptibilidad a la divulgación o a la modificación no autorizada de los recursos tecnológicos con los que cuenta una organización para agilizar su gestión.

IMPLEMENTACIÓN

Para realizar la implementación del Modelo de Seguridad y Privacidad de la Información en la empresa de servicios públicos de Pamplona Empopamplona S.A E.S.P., se toma como base la metodología PHVA (Planear, Hacer, Verificar y Actuar) y los lineamientos emitidos por el Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC, a través de los decretos emitidos.

De acuerdo con esto, se definen las siguientes fases de implementación:

- ✓ Diagnosticar
- ✓ Planear

- ✓ Hacer
- ✓ Verificar
- ✓ Actuar

Actividades de Implementación.

- ✓ Realización del Diagnóstico.
- ✓ Elaborar el Alcance del Plan del Tratamiento de Riesgo de Seguridad y Privacidad de la Información.
- ✓ Realizar la Identificación de los Riesgos con los líderes del Proceso.
- ✓ Entrevistar con los líderes del Proceso.
- ✓ Valorar del riesgo inherente y del riesgo residual.
- ✓ Realizar Mapas de calor donde se ubican los riesgos.
- ✓ Plantear al plan de tratamiento de riego aprobado por los lideres.

Cumplimiento en la Implementación

De acuerdo a las fases mencionadas anteriormente, se describe a continuación los dominios que se deben desarrollar y los plazos de implementación de acuerdo a lo establecido por la organización:

- ✓ Revisión y/o Modificación de la actual Política de Seguridad.
- ✓ Aspectos organizativos de la seguridad de la información.
- ✓ Seguridad Ligada a los recursos humanos.
- ✓ Revisión del Control de acceso.
- ✓ Seguridad en la operativa.
- ✓ Seguridad en las telecomunicaciones.
- ✓ Gestión de Incidentes de Seguridad de la Información.

- ✓ Aspectos de seguridad de la información en la gestión de continuidad del negocio.

CRONOGRAMA.

ítem	Actividad	Producto	Fecha Inicio	Fecha Final	Responsable
1	Revisión del Contexto del Sistema de Gestión de Seguridad y Privacidad de la Información. (SGSI)	Documento con Misión, Visión, Objetivos del Negocio y Procesos seleccionados.	1/04/2024	1/06/2024	Líder Infraestructura Tecnológica
2	Identificación y Valoración de Activos de Información.	Matriz con la identificación y clasificación de activos de información.	1/06/2024	1/07/2024	Líder Infraestructura Tecnológica
3	Identificación de amenazas y vulnerabilidades en la Infraestructura tecnológica y los sistemas de Información	Documento diagnostico	1/07/2024	1/08/2024	Líder Infraestructura Tecnológica
4	Establecimiento de los escenarios de riesgos	Documento con escenarios de riesgos y las diferentes probabilidades de ocurrencia e impactos en la entidad.	1/08/2024	1/09/2024	Líder Infraestructura Tecnológica
5	Valoración de los Riesgos	Matriz con valor de activo, probabilidad e impacto.	1/09/2024	1/10/2024	Líder Infraestructura Tecnológica
6	Identificación, Valoración y tratamiento de riesgo	Estrategias de tratamiento y Mapa de Calor.	1/09/2024	1/10/2024	Líder Infraestructura Tecnológica
7	Identificación de los controles existentes	Documento con la identificación de riesgos inherentes y	1/09/2024	1/10/2024	Líder Infraestructura Tecnológica

		residuales.			
8	Selección de las opciones para el tratamiento de riesgos	Plan de Tratamiento de riesgos	1/10/2024	1/11/2024	Líder Infraestructura Tecnológica
9	Elaboración la declaración de aplicabilidad (SOA)	Matriz de Riesgos	1/11/2024	31/12/2024	Líder Infraestructura Tecnológica
10	Implementación del plan de control operacional	Cumplimiento de los requisitos establecidos para el cumplimiento del Plan	1/11/2024	31/12/2024	Líder Infraestructura Tecnológica
11	Elaboración de los Indicadores De GestiónIndicadores de Gestión	Documento con los	1/11/2024	31/12/2024	Líder Infraestructura Tecnológica

SEGUIMIENTO Y EVALUACIÓN

El proceso de seguimiento y evaluación del Plan de Riesgos de Seguridad y Privacidad de la Información se realizará con los resultados que arrojen los indicadores de Gestión propuestos para verificación de la efectividad, la eficiencia y la eficacia de las acciones implementadas, lo cual contempla las siguientes actividades:

- ✓ Revisión de la evaluación de los niveles de riesgo y riesgo residual después de la aplicación de controles y medidas administrativas.
- ✓ Seguimiento al alcance y a la implementación de los planes de manejo de riesgos.
- ✓ Seguimiento a los registros de acciones y eventos / incidentes que podrían tener impacto en la eficacia o desempeño de la seguridad de la información al interior de la