SAAAB

SOCIEDAD DE ACUEDUCTO, ALCANTARILLADO Y ASEO DE BUENAVENTURA S.A. E.S.P.

PLAN OPERACIONAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN (POSPI) PARA SAAAB. SA.ESP.

	NOMBRE	CARGO	FIRMA
Elabora:	Alexander Gamboa Patiño	Analista de Sistemas	
Revisó:	Verónica Vallecilla Vargas	Apoyo Profesional a la Coordinación Administrativa	
Revisó:	Martha Lucia torres Cruz	Analista de Sistema de Gestión Institucional	
Revisó:	Edgar Banguera Celorio	Sub gerente	
Aprobó:	Enna Rut Cruz Montaño	Gerente	

SAAAB
SOCIEDAD DE ACUEDUCTO, ALCANTARILLADO Y ASEO DE BUENAVENTURA S.A. E.S.P.

TABLA DE CONTENIDO

1. RESUMEN EJECUTIVO

El POSPI de SAAAB SA. ESP., se establece con el propósito de garantizar la seguridad y privacidad de la información en toda la organización. Reconociendo la importancia crítica de la información en nuestras operaciones y en la satisfacción del cliente, hemos desarrollado un plan exhaustivo para proteger y gestionar adecuadamente todos los activos de información.

2. ALCANCE DEL POSPI

Este plan se aplica a todos los activos de información de SAAAB SA. ESP, incluidos datos de clientes, datos financieros, datos de empleados y cualquier otra información confidencial o sensible. Se extiende a todos los empleados, contratistas y terceros que interactúan con los activos de información de la empresa.

3. OBJETIVOS DEL POSPI

El POSPI de SAAAB S.A. ESP., tiene como objetivo principal proteger la confidencialidad, integridad y disponibilidad de la información de la organización. Esto se logrará mediante la implementación de políticas, procesos y medidas técnicas que minimicen los riesgos de seguridad y garanticen el cumplimiento de las regulaciones de privacidad de datos.

4. DEFINICIONES CLAVE

a) **Activos de Información**: Todos los elementos de datos y recursos relacionados con la información que son valiosos para una organización, incluyendo datos, sistemas, documentos, hardware y software.

b) **Confidencialidad**: El principio de seguridad de la información que asegura que solo las personas autorizadas tengan acceso a la información y que la información sensible o confidencial no se divulgue a personas no autorizadas.

c) **Integridad de Datos**: Garantizar que la información y los datos se mantengan precisos, completos y no sean alterados de manera no autorizada durante su procesamiento, almacenamiento o transmisión.

d) **Disponibilidad**: El principio de seguridad de la información que se refiere a la garantía de que la información y los recursos estén disponibles y accesibles cuando se necesiten y que los servicios no sufran interrupciones no planificadas.

e) **Riesgo de Seguridad**: La probabilidad de que una amenaza o evento no deseado tenga un impacto negativo en la seguridad de la información de la organización.

f) **Regulaciones de Privacidad de Datos**: Conjunto de leyes, normativas y regulaciones que rigen la recopilación, procesamiento, almacenamiento y divulgación de datos personales de individuos, con el propósito de proteger la privacidad y los derechos de las personas.

g) **Política de Seguridad de la Información**: Un documento formal que establece las directrices, objetivos y responsabilidades para proteger la información y los activos de la organización. Define cómo se deben abordar los riesgos de seguridad.

h) **Política de Privacidad de Datos**: Un documento que establece las prácticas y procedimientos que una organización seguirá para garantizar la privacidad y

protección de los datos personales de sus clientes, empleados y otras partes interesadas.

i) **Propietarios de Datos**: Individuos o departamentos designados que son responsables de supervisar y gestionar la información y los activos de información en una organización. Los propietarios de datos garantizan la integridad y confidencialidad de los datos bajo su control.

j) **Evaluación de Riesgos**: Un proceso sistemático para identificar, analizar y evaluar los riesgos de seguridad de la información que enfrenta una organización, con el objetivo de tomar medidas adecuadas para mitigarlos.

k) **Control de Acceso**: Medidas y políticas implementadas para garantizar que solo las personas autorizadas tengan acceso a sistemas, datos y recursos de información.

l) **Gestión de Identidad**: Un conjunto de políticas, procesos y tecnologías utilizadas para administrar y autenticar la identidad de usuarios y garantizar que solo tengan acceso a los recursos apropiados.

m) **OPSI**: Oficial de Seguridad de la Información.

n) **ERI:** Equipo de respuesta a Incidentes

5. POLÍTICAS DE SEGURIDAD Y PRIVACIDAD

5.1. Política de Seguridad de la Información

SAAAB establece una política de seguridad de la información que proporciona una guía clara sobre cómo proteger y manejar los activos de información. Esta política establece las responsabilidades y roles de todos los empleados y define las medidas de seguridad que deben implementarse.

5.2. Objetivo

La Política de Seguridad de la Información de SAAAB. SA. ESP., tiene como objetivo principal establecer los principios y directrices que garantizarán la protección, confidencialidad, integridad y disponibilidad de la información y los activos de información de la organización.

5.3. Alcance

Esta política es aplicable a todos los empleados, contratistas, proveedores y terceros que interactúen con los activos de información de SAAAB. SA. ESP.

5.4. Responsabilidades y Roles

5.5. Alta Dirección

La alta dirección de SAAAB. SA. ESP., tiene la responsabilidad de liderar y respaldar las iniciativas de seguridad de la información y garantizar la asignación adecuada de recursos para su implementación.

a. Funciones de Oficial de Seguridad de la Información (OSI)

El OSI es responsable de supervisar y coordinar todas las actividades relacionadas con la seguridad de la información. (Que para el caso de la entidad es el Analista de Informática) Esto incluye la evaluación de riesgos, la implementación de controles de seguridad y la gestión de incidentes.

b. Propietarios de Datos

Se designarán propietarios de datos para cada categoría de información. Los propietarios de datos garantizarán la confidencialidad e integridad de los datos bajo su control.

c. Clasificación de Datos

1. Categorización de Datos

Los datos de la SAAAB. SA. ESP., se clasificarán en tres categorías principales: Alta Confidencialidad, Confidencialidad Media y No Confidencial, según su importancia y nivel de sensibilidad.

2. Manejo de Datos Confidenciales

Los datos clasificados como "Alta Confidencialidad" estarán sujetos a medidas de seguridad adicionales, incluida la encriptación y el acceso restringido.

d. Control de Acceso

1. Política de Acceso

El acceso a los activos de información de SAAAB, SA. ESP., se basará en el principio de necesidad. Los empleados solo tendrán acceso a la información necesaria para cumplir con sus responsabilidades laborales.

2. Autenticación de Usuarios

Se implementarán medidas de autenticación sólidas, como contraseñas seguras y autenticación de dos factores, para garantizar que solo los usuarios autorizados puedan acceder a sistemas y datos.

3. Gestión de Derechos de Acceso

Los derechos de acceso se gestionarán de manera eficiente, y se revocarán o modificarán cuando sea necesario debido a cambios en las funciones laborales.

4. Auditoría de Acceso

Se llevará un registro de auditoría de todos los accesos a los sistemas y datos sensibles para fines de revisión y seguimiento.

e. Protección de Redes y Sistemas

1. Firewalls y Seguridad de Red

Se implementarán firewalls y medidas de seguridad de red para proteger los sistemas contra intrusiones no autorizadas.

2. Actualizaciones de Software y Parches

   Se aplicarán regularmente actualizaciones de software y parches de seguridad para proteger los sistemas contra vulnerabilidades conocidas.

3. Antivirus y Antimalware

   Se instalará software antivirus y antimalware en todos los sistemas para detectar y prevenir amenazas de software malicioso.

f. Seguridad Física

1. Control de Acceso Físico

Se implementarán medidas de control de acceso físico, como acceso biométrico y cámaras de seguridad, para proteger las instalaciones que albergan activos de información.

2. Respaldo y Almacenamiento Seguro

Se realizarán copias de seguridad regulares de datos críticos y se almacenarán de forma segura fuera del sitio para garantizar la recuperación ante desastres.

g. Gestión de Incidentes de Seguridad

1. Notificación de Incidentes

Se establecerá un proceso de notificación de incidentes para que los empleados informen rápidamente sobre cualquier evento de seguridad sospechoso o confirmado.

2. Investigación y Respuesta

Se llevará a cabo una investigación completa de los incidentes de seguridad y se tomarán medidas correctivas adecuadas.

h. Auditoría y Monitoreo

1. Auditoría de Seguridad

Se realizarán auditorías de seguridad regulares para evaluar la eficacia de las medidas de seguridad y garantizar el cumplimiento de esta política.

2. Monitoreo Continuo

Se establecerá un sistema de monitoreo continuo para detectar y responder rápidamente a cualquier actividad sospechosa en la red y los sistemas.

i. Cumplimiento Legal y Regulatorio

3. Cumplimiento Legal

SAAAB. SA. ESP., se compromete a cumplir todas las leyes y regulaciones aplicables relacionadas con la seguridad de la información y la privacidad de los datos.

j. Marco Legal Colombiano

SAAAB. SA. ESP., reconoce que el cumplimiento de las leyes y regulaciones relacionadas con la seguridad de la información y la privacidad de los datos es fundamental para operar de manera ética y legal en Colombia. La organización está comprometida a respetar y cumplir todas las normativas colombianas pertinentes en materia de seguridad de la información, incluyendo, pero no limitado a:

- Ley 1581 de 2012 (Ley de Protección de Datos Personales)

Esta ley regula la protección de datos personales en Colombia. SAAAB. SA. ESP., se compromete a cumplir con los requisitos de esta ley en lo que respecta a la recopilación, procesamiento y protección de datos personales de sus empleados, clientes y terceros.

- Resolución 1790 de 2017

Esta resolución establece los requisitos de seguridad de la información para las entidades públicas y privadas en Colombia. SAAAB. SA. ESP., adoptará las medidas y controles de seguridad recomendados en esta resolución para proteger sus activos de información.

- Protección de la Privacidad de Datos
- Consentimiento Informado

SAAAB. SA. ESP., se compromete a obtener el consentimiento informado de los individuos antes de recopilar y procesar sus datos personales. Esto se aplica a empleados, clientes y cualquier otra parte interesada.

- Derechos de los Titulares

La organización respetará los derechos de los titulares de datos personales, incluyendo el acceso, rectificación, cancelación y oposición (derechos ARCO). Se proporcionará un mecanismo para que los titulares ejerzan estos derechos.

- Reporte de Incidentes y Brechas

Ley 1273 de 2009 (Ley de Delitos Informáticos)

Esta ley establece disposiciones relacionadas con delitos informáticos, incluyendo el acceso no autorizado a sistemas y la divulgación no autorizada de información.

SAAAB SA. ESP., se compromete a cumplir con esta ley y a informar cualquier incidente de seguridad de acuerdo con sus disposiciones.

Auditorías y Supervisión

- Superintendencia de Industria y Comercio (SIC)

La SIC es la autoridad de supervisión en Colombia para la protección de datos personales. SAAAB. SA. ESP., de la Ley 1581 de 2012 y otras regulaciones relevantes.

Capacitación y Concientización

SAAAB. SA. ESP., proporcionará capacitación regular a sus empleados sobre las leyes y regulaciones colombianas pertinentes en materia de seguridad de la información y privacidad de datos. Esto incluirá la formación sobre la Ley 1581 de 2012 y la importancia del cumplimiento legal y ético.

Actualización y Seguimiento

La alta dirección de SAAAB. SA. ESP., se compromete a mantenerse al tanto de cualquier cambio en las leyes y regulaciones colombianas relacionadas con la seguridad de la información y la privacidad de datos, y a actualizar esta política y los controles de seguridad en consecuencia.

Revisión y Actualización

Esta política se revisará y actualizará periódicamente para asegurarse de que refleje las mejores prácticas de seguridad de la información y los cambios en el entorno de amenazas.

6. EVALUACIÓN DE RIESGOS Y AMENAZAS

a. Evaluación de Riesgos

SAAAB. SA. ESP., reconoce la importancia crítica de evaluar y gestionar los riesgos de seguridad de la información de manera sistemática y continua. La evaluación de riesgos es un proceso fundamental para identificar y abordar las amenazas que podrían afectar a nuestros activos de información. Para llevar a cabo una evaluación de riesgos efectiva, se seguirán los siguientes pasos:

- Identificación de Activos de Información

Se identificarán y catalogarán todos los activos de información de SAAAB, SA. ESP., incluyendo datos, sistemas, documentos y recursos relacionados con la información.

- Identificación de Amenazas

Se llevará a cabo una revisión exhaustiva para identificar todas las amenazas potenciales que podrían afectar a nuestros activos de información. Esto incluirá amenazas físicas, tecnológicas, humanas y ambientales.

- Evaluación de Vulnerabilidades

Se evaluarán las vulnerabilidades actuales en nuestros sistemas, procesos y controles de seguridad. Esto incluirá la identificación de posibles brechas de seguridad y puntos débiles.

- Análisis de Impacto

Se determinará el impacto potencial que cada amenaza podría tener en nuestros activos de información. Esto incluirá la evaluación de las consecuencias financieras, operativas y de reputación.

Evaluación de Impacto

Para cada activo crítico, se llevará a cabo una evaluación de impacto que incluirá una revisión exhaustiva de las posibles consecuencias de su pérdida o compromiso. Las áreas clave de impacto incluirán:

- **Impacto financiero**: Evaluar cómo la pérdida de un activo podría afectar a los resultados financieros de la organización.
- **Impacto operativo**: Evaluar cómo la pérdida de un activo podría afectar la capacidad de SAAAB para operar eficazmente.
- **Impacto de reputación**: Evaluar cómo la pérdida de un activo podría afectar la reputación y la confianza de los clientes y socios comerciales.

Se asignarán prioridades a los activos críticos en función de su impacto potencial. Esto permitirá una focalización efectiva de los recursos de seguridad.

- Evaluación de Riesgos

Se calculará el nivel de riesgo para cada amenaza identificada, teniendo en cuenta la probabilidad de ocurrencia y el impacto potencial. Los riesgos se categorizarán en función de su gravedad.

- Priorización de Riesgos

Se asignarán prioridades a los riesgos identificados para que se puedan abordar de manera efectiva. Se prestará especial atención a los riesgos de alta gravedad.

b. Gestión de Riesgos

1. Mitigación de Riesgos

   Se desarrollarán planes de mitigación para abordar los riesgos identificados. Estos planes incluirán la implementación de controles de seguridad adicionales, revisiones de procesos y procedimientos, y la asignación de responsabilidades claras.

2. Monitoreo Continuo

   Se establecerá un sistema de monitoreo continuo para evaluar la efectividad de las medidas de mitigación y para detectar cualquier cambio en el entorno de amenazas.

3. Actualización Periódica

   La evaluación de riesgos se revisará y actualizará periódicamente para garantizar que refleje los cambios en el entorno operativo y las amenazas emergentes.

a. Documentación de Riesgos

Todos los resultados de la evaluación de riesgos, las medidas de mitigación y las actualizaciones se documentarán en un registro de riesgos que estará a disposición de la alta dirección y el funcionario del área de informática encargado de "Seguridad de la Información (OSI)".

SAAAB. SA. ESP., se compromete a mantener una cultura de seguridad de la información sólida y proactiva, y la evaluación de riesgos y amenazas es un componente esencial para lograr este objetivo. El proceso de evaluación de riesgos se llevará a cabo con regularidad y se utilizará para guiar nuestras decisiones en materia de seguridad.

Riesgo	**Probabilidad (P)**	**Impacto (I)**	**Nivel de Riesgo (P x I)**	**Prioridad**
Acceso no autorizado a datos	Moderada	Alto	Moderado	Alta
Pérdida de datos	Baja	Muy Alto	Moderado	Alta
Ataque de malware	Alta	Moderado	Alto	Alta
Fallo en la seguridad física	Baja	Alto	Moderado	Media
Robo de dispositivos	Moderada	Alto	Moderado	Media
Interrupción del servicio	Baja	Muy Alto	Alto	Alta

Notas:

- Probabilidad: Evalúa cuán probable es que ocurra el riesgo (Baja, Moderada, Alta).
- Impacto: Evalúa el impacto potencial si el riesgo se materializa (Bajo, Moderado, Alto, Muy Alto).
- Nivel de Riesgo: Es el producto de la probabilidad y el impacto (P x I). Este número ayuda a priorizar los riesgos.
- Prioridad: Esta columna podría utilizarse para establecer la prioridad de mitigación, donde "Alta" significa que el riesgo debe abordarse de inmediato.

7. GESTIÓN DE INCIDENTES DE SEGURIDAD

Definición de Incidentes

- Incidentes de Seguridad de la Información

Se consideran incidentes de seguridad de la información cualquier evento o situación que comprometa la confidencialidad, integridad o disponibilidad de los activos de información de SAAAB. SA. ESP., Estos incidentes pueden ser intencionales o accidentales y pueden involucrar a personas, procesos o tecnología. Algunos ejemplos de incidentes de seguridad de la información incluyen:

- Acceso no autorizado a sistemas o datos.
- Pérdida o robo de dispositivos o documentos que contienen información confidencial.
- Ataques cibernéticos, como malware o phishing.
- Divulgación no autorizada de información confidencial.
- Interrupciones en los servicios críticos.
- Proceso de Notificación de Incidentes
- Responsabilidad de Notificación

Todos los empleados de SAAAB. SA. ESP., tienen la responsabilidad de notificar de inmediato cualquier incidente de seguridad de la información que identifiquen o sospechen. Esto incluye a empleados de todos los niveles jerárquicos, contratistas, proveedores y terceros que trabajen con la organización.

- Canales de Notificación

Se establecerán canales de notificación de incidentes, que incluirán un punto de contacto designado para recibir informes de incidentes. Los canales pueden incluir una línea directa de seguridad, una dirección de correo electrónico designada o un formulario en línea.

- Contenido de la Notificación

Los informes de incidentes deberán contener información detallada sobre la naturaleza del incidente, su ubicación, las personas involucradas (si se conocen), el impacto potencial y cualquier acción inmediata que se haya tomado.

- Confidencialidad de la Notificación

SAAAB. SA. ESP., garantizará que los informes de incidentes se manejen de manera confidencial y se proteja la identidad del informante, si así lo solicita.

Investigación y Respuesta

- **Equipo de Respuesta a Incidentes**

Se designará un Equipo de Respuesta a Incidentes (ERI) que estará compuesto por profesionales de seguridad de la información y representantes de otras áreas relevantes de la organización. El ERI será responsable de la gestión de incidentes y de llevar a cabo investigaciones y respuestas adecuadas.

Evaluación y Clasificación de Incidentes

El ERI evaluará cada incidente reportado y lo clasificará según su gravedad. Se establecerán criterios de clasificación claros para determinar la respuesta apropiada.

Respuesta Inmediata

Para incidentes graves que requieran una respuesta inmediata, el ERI tomará medidas para contener la situación y minimizar el impacto. Esto puede incluir la desconexión de sistemas comprometidos, la notificación a las autoridades apropiadas y la mitigación de amenazas.

Investigación Detallada

Para incidentes que requieran una investigación más detallada, el ERI llevará a cabo una investigación exhaustiva para determinar la causa raíz, el alcance del incidente y las lecciones aprendidas.

Notificación a Afectados

SAAAB. SA. ESP., notificará a todas las partes afectadas por un incidente de seguridad de la información de manera oportuna y de acuerdo con las leyes y regulaciones aplicables. Esto incluirá a los empleados, clientes, socios comerciales y otras partes interesadas.

7. AUDITORÍA Y MONITOREO

7.1 Auditoría de Seguridad

7.1.1 Propósito de las Auditorías

Las auditorías de seguridad se llevarán a cabo con el propósito de evaluar y garantizar la eficacia de las medidas de seguridad de la información de SAAAB. SA. ESP., Estas auditorías ayudarán a identificar posibles debilidades, brechas de seguridad y áreas de mejora.

7.1.2 Programa de Auditoría

SAAAB. SA. ESP., establecerá un programa de auditoría de seguridad que especificará la periodicidad de las auditorías y los activos de información que serán objeto de auditoría. Las auditorías se llevarán a cabo al menos anualmente.

7.1.3 Auditoría Interna y Externa

Se llevarán a cabo auditorías internas por parte del equipo de auditoría interna designado, así como auditorías externas por terceros expertos en seguridad de la información, de manera periódica. Las auditorías externas pueden incluir pruebas de penetración y evaluación de vulnerabilidades.

7.2 Monitoreo Continuo

7.2.1 Sistema de Monitoreo

SAAAB. SA. ESP., establecerá un sistema de monitoreo continuo que supervisará los eventos y actividades relacionados con la seguridad de la información. Este sistema utilizará herramientas de seguridad de la información para detectar y alertar sobre posibles incidentes de seguridad en tiempo real.

7.2.2 Registros de Auditoría

Se mantendrán registros de auditoría que registrarán eventos relevantes de seguridad, incluyendo accesos, cambios en configuraciones y actividades de administración de sistemas. Estos registros serán revisados regularmente como parte del proceso de monitoreo.

7.2.3 Respuesta a Incidentes

El sistema de monitoreo continuo permitirá una respuesta más rápida a incidentes de seguridad. Se establecerán procedimientos claros para responder a las alertas de seguridad, investigar las posibles amenazas y tomar medidas correctivas.

7.2.4 Informes de Monitoreo

Se generarán informes periódicos de monitoreo que resumirán las actividades de seguridad y los incidentes detectados. Estos informes serán revisados por la alta dirección y el Equipo de Respuesta a Incidentes (ERI).

7.3 Cumplimiento y Mejora

7.3.1 Acciones Correctivas

Cualquier hallazgo o debilidad identificada durante las auditorías o el monitoreo continuo será abordado con acciones correctivas apropiadas. Estas acciones se documentarán y se realizará un seguimiento para garantizar su resolución.

7.3.2 Mejora Continua

La información recopilada a través de auditorías y monitoreo se utilizará para mejorar continuamente las medidas de seguridad de la información de SAAAB. SA. ESP., Se buscarán oportunidades para fortalecer los controles de seguridad y la preparación para incidentes.

8. CONTROL DE CAMBIOS

Versión	Fecha	Identificación de los Cambios	Observaciones
01	28-09-2023	Versión Inicial	