accion.point

Política de seguridad de la información

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

INTRODUCCIÓN

Este documento establece la política de ACCION POINT basada en la norma ISO 27001. ACCION POINT es una empresa de tecnología dedicada a la Comercialización, y prestación de servicios de soluciones tecnológicas.

ACCION POINT se compromete a garantizar la confidencialidad, integridad y disponibilidad de la información en todas las áreas de la organización. Para ello establece un Sistema de gestión de seguridad de la información a través de un conjunto de medidas integrales y controles de seguridad para la protección de los activos y datos sensibles de la empresa y sus clientes, asegurando la continuidad del negocio y la preservación de la información.

ACCION POINT se compromete a la mejora continua del SGSI, así como a cumplir con los requisitos legales y regulatorios pertinentes y de sus partes interesadas en materia de seguridad de la información.

OBJETIVO GENERAL

Entre sus objetivos se encuentran:

- Garantizar la asignación de recursos esenciales para alcanzar y mantener los objetivos del SGSI, conservando un adecuado balance entre costo y beneficio.

- Definir y establecer los roles y responsabilidades para con el SGSI de todos los integrantes de ACCION POINT y partes interesadas relevantes, para de esta forma contar con personal competente y debidamente capacitado a los fines de llevar a cabo las tareas relacionadas.

- Constituir un marco general para gestionar adecuadamente la Seguridad de la Información, utilizando información documentada (por ejemplo: las políticas, normas, procedimientos, procesos y estándares, entre otros) y otros criterios necesarios para el SGSI.

ALCANCE DEL SGSI

La presente Política aplica a toda la organización, clientes, proveedores y/o cualquier persona física o jurídica que acceda o interactúe con la información de ACCION POINT para los

procesos de la unidad estratégica de negocios de Servicios Financieros. Dentro de los procesos de Comercialización, análisis, diseño, desarrollo, "testing", implementación y mantenimiento de software.

DISTRIBUCIÓN

Publicado en el repositorio documental de la organización, con acceso a todos los integrantes alcanzados en el Sistema de Gestión y en el sitio web de la organización.

RESPONSABILIDAD

La información relacionada con autoridad y responsabilidades de cada posición de la compañía frente al Sistema de Gestión de la Seguridad de la Información, se encuentra almacenado en el repositorio de descriptivos de puesto en la red interna.

CONTENIDO

Seguridad de la Información

Principios

La PSGSI vela por la seguridad de todos sus procesos, siendo ésta de aplicación en todas las fases del ciclo de vida de los activos intervinientes: generación, distribución, almacenamiento, procesamiento, transporte, consulta y destrucción;

ACCION POINT adoptará acciones tendientes a preservar en cada momento los tres componentes básicos de Seguridad de la Información:

- **Confidencialidad:** Garantizar que a los activos de información solo accedan las personas debidamente autorizadas.
- **Integridad:** Garantizar la exactitud de los activos de información durante todo su ciclo de vida contra cualquier alteración, pérdida y/o destrucción, ya sea de forma accidental o fraudulenta.
- **Disponibilidad:** Garantizar que los activos de información puedan ser utilizados en la forma y tiempo requeridos.

Esto se fundamenta en el hecho de que la Seguridad de la Información es vital para la gestión operativa, la imagen institucional y la calidad administrativa.

Adicionalmente, se adoptarán conductas destinadas a garantizar el cumplimiento de los principios que se detallan a continuación:

- **Autenticidad:** Establecer las identidades de los individuos para asegurar que cada uno sea quién dice ser.
- **Trazabilidad:** Asegurar que cualquier acción o transacción pueda ser relacionada unívocamente, almacenando un histórico de las mismas.
- **Legalidad:** Garantizar que la información de ACCION POINT cumple con las leyes, reglamentaciones y disposiciones vigentes.
- **No repudio:** Gracias a esta característica el emisor no puede negar el envío de un mensaje porque el destinatario tiene pruebas de éste.
- **Privacidad de la Información:** Es el aspecto que se ocupa de la capacidad que una organización o individuo tiene para determinar qué datos en un sistema informático pueden ser compartidos con terceros.

Privacidad de la Información

Gestión de Privacidad de la Información: Establecer, implementar, mantener y mejorar continuamente la gestión de Privacidad de la Información, que permita reducir los riesgos en los tratamientos de datos personales o información de identificación personal (PII), es decir, de aquella información o datos que identifican o podrían servir para identificar a una persona.

Control de la Información y Control de accesos

Se establecen niveles de clasificación de la información para determinar los niveles de acceso y protección requeridos con el fin de prevenir la divulgación, modificación, eliminación o destrucción no autorizadas de información almacenada en medios.
Se asignan permisos de acceso basados en el principio de "menos privilegios". Se implementa un sistema de gestión de identidad y acceso para administrar la autorización de usuarios.
Se establecen controles para garantizar la seguridad en el teletrabajo.

Protección física y del entorno

ACCION POINT impide accesos físicos no autorizados, daños e interferencia a la información y a las instalaciones de procesamiento de información de la organización.

Seguridad de las operaciones

- Garantizamos la operación correcta y segura de las instalaciones de procesamiento de la información.
- Garantizamos que la información y las instalaciones de procesamiento de información estén protegidas contra código malicioso y otras vulnerabilidades técnicas.
- Nos protegemos contra la pérdida de datos y hackeos.
- Registramos eventos y generamos evidencia en nuestro sistema.

- Garantizamos la integridad de los sistemas en nuestros ambientes para la posterior puesta en producción.

Desarrollo de software seguro

Se siguen prácticas de desarrollo seguro, como revisión de código, pruebas de seguridad y evaluaciones de vulnerabilidades.
Se mantienen actualizados los componentes y bibliotecas de software utilizados.

Seguridad de las comunicaciones

Garantizamos la protección de la información en las redes y sus instalaciones de procesamiento de la información que la soportan.

Relación con los proveedores

Garantizamos la protección de los activos de la organización a los cuales tienen acceso los proveedores, manteniendo un nivel acordado de seguridad de la información y de prestación de servicio alineados con los acuerdos con los proveedores.

Seguridad en la Infraestructura

Los sistemas críticos se alojan en entornos seguros y se aplican actualizaciones regularmente.

Respuesta a Incidentes

Se mantiene un plan de respuesta a incidentes que incluya procedimientos para detectar, informar y mitigar incidentes de seguridad.
Los incidentes se documentan y se realizan análisis post-incidentes para mejorar la seguridad.

Continuidad del Negocio

Consideramos la continuidad en los sistemas de gestión del negocio, garantizando la disponibilidad de las instalaciones de procesamiento de la información de los clientes y los sistemas internos para poder atender las demandas de los mismos.

Formación y Concienciación

Se llevan a cabo programas regulares de formación en seguridad para empleados y contratistas para garantizar que todos comprendan sus responsabilidades y estén al tanto de las amenazas y mejores prácticas. De esa forma garantizar que las personas que realizan el trabajo bajo el control de la organización entiendan sus responsabilidades y sean idóneos para los roles para los cuales se los considera.

Se provee la concienciación sobre seguridad de la información a través de campañas de sensibilización y capacitación.

Revisión de la política:
Esta política se revisará, al menos, anualmente para garantizar su relevancia y eficacia en un entorno en constante evolución.
La mejora continua es un pilar fundamental para mantener y actualizar el SGSI de acuerdo con las cambiantes amenazas y requisitos de seguridad.

Documentos relacionados:
El documento de aplicabilidad explica la aplicación de cada control al SGSI.

Aprobación y divulgación
Todos los empleados, contratistas y terceros deben leer, comprender y aceptar esta política antes de interactuar con los sistemas y la información.

GENERALIDADES

El incumplimiento manifiesto de la presente política será sancionado mediante la aplicación de las normas vigentes.

Suscribe y aprueba,