Política Sistema del SGSI

Table of Contents

Page

1 OBJETIVO

El objetivo global de Seguridad de la Información de ELECTRONIC IDENTIFICATION es garantizar los criterios de Confidencialidad, Integridad y Disponibilidad de la información, así como la continuidad de los servicios ofrecidos a nuestros clientes en caso de ocurrencia de eventos disruptivos en los mismos, articulando para ello un conjunto de procesos internos para responder de forma ordenada ante un suceso, reduciendo al mínimo el impacto sobre el negocio, la información y los clientes.

La Política de del Sistema de Gestión de la Seguridad de la Información (SGSI) establece un marco de actuación común que impacta en la cultura de la empresa y en el cumplimiento de objetivos comunes, por el cual todos los recursos deben estar implicados en el correcto funcionamiento de controles de seguridad y planes de continuidad establecidos en ELECTRONIC IDENTIFICATION.

2 ALCANCE

La Política del Sistema de Gestión de Seguridad de la Información define un conjunto de principios aplicables a todos componentes y sistemas de la API de servicios de confianza electrónica en el entorno de producción y en especial a aquellos que tengan especial implicación en la actuación ante la ocurrencia de eventos disruptivos en materia de seguridad de la información o continuidad de servicios.

3 RESPONSABILIDADES

La principal figura responsable de la Política es el Comité del Sistema de Gestión de Seguridad de la Información y el Responsable del Sistema, pues son los encargados de revisar y aprobar las diferentes estrategias y procesos de seguridad de la información, velando por su calidad y efectividad.

Las funciones y obligaciones para coordinar y ejecutar los principios de Seguridad de la Información están desarrollados en los documentos del SGSI.

4 POLÍTICA DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

- Garantizar que los servicios acordados con los diferentes clientes se prestan ante la ocurrencia de un desastre en ELECTRONIC IDENTIFICATION y los procesos de negocio que lo sustentan.

- Proteger la seguridad de los recursos de ELECTRONIC IDENTIFICATION, ya sea en la gestión diaria como en caso de emergencia de la compañía.

- Establecer periódicamente objetivos de mejora alineados con la presente política.

- La Dirección de ELECTRONIC IDENTIFICATION se responsabilizará de la gestión de los riesgos clave para la seguridad de la información y la continuidad operativa de los procesos considerados críticos para la organización.

- Elaborar un Plan de Continuidad que permita recuperarse ante un desastre, en el menor tiempo posible.

- Formar y concienciar a todos los empleados en materia de seguridad de la información.

- ELECTRONIC IDENTIFICATION velará para que todos los recursos internos estén plenamente informados de las responsabilidades que le competen en el marco de la Seguridad de la Información.

- ELECTRONIC IDENTIFICATION debe minimizar los riesgos de seguridad de la información, asegurando planes de respuesta eficaces ante incidentes.

- ELECTRONIC IDENTIFICATION garantizará la elaboración de planes de comunicación apropiados, tanto internos como externos, que serán revisados y actualizados de forma periódica.

- Hacer patente el compromiso de la Dirección en relación a la Seguridad de la Información en consonancia con la estrategia de negocio, mediante su apoyo al Comité del SGSI dotándole de los medios y facultades necesarias para la realización de sus funciones.

- Definir, desarrollar e implantar los controles técnicos y organizativos que resulten necesarios para garantizar la Confidencialidad, Integridad y Disponibilidad de la información gestionada en la organización.

- Garantizar el cumplimiento de la legislación vigente en materia de protección de datos de carácter personal, propiedad intelectual y sociedad de la información, así como de todos aquellos requerimientos legales, reglamentarios y contractuales que resulten aplicables.

- Crear una “cultura de seguridad” tanto internamente, en relación con todo el personal, como externamente, en relación con los clientes y proveedores.

- Considerar el Sistema de Gestión de Seguridad de la Información como un proceso de mejora continua, realizando revisiones periódicas con el objetivo de alcanzar niveles de seguridad de la información cada vez más avanzados.

Keyword Index

Keyword	Explanation

Document History

Version	Date	Changes made to previous version/ remarks
1.0	22/01/16	Versión Inicial
2.0	14/01/19	Referencias ISO 27001 y cambio de formato