POLÍTICA DE CIBERSEGURIDAD GRUPO PIKOLINOS

Referencia: DOC_P_01_Política de Ciberseguridad WEB

Versión: v 1.0

Clasificación: Público

Fecha: 26 de junio de 2024

Tabla de contenido

1 Introducción

1.1 Propósito

El objetivo final de la presente política de ciberseguridad es mantener en un nivel aceptable de riesgo los sistemas de información del Grupo Pikolinos (En delante Pikolinos), desde el punto de vista de la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de datos a través de **políticas y procedimientos** específicos que conforman el **cuerpo normativo de ciberseguridad** de Pikolinos.

La importancia creciente de la información, junto con la gran cantidad de canales por la que ésta viaja, obliga a encontrar la manera de poder asegurar dicha información.

La ciberseguridad en Pikolinos es un proceso continuo cuyos principales objetivos son:

- Mitigar el daño sufrido en las áreas funcionales de Pikolinos.
- Reducir las amenazas.
- Asegurar la continuidad de las funciones críticas soportadas por las tecnologías de la información.
- Facilitar la introducción segura de nuevos servicios y tecnologías.

La dirección de Pikolinos, dentro de la estrategia global definida para el desarrollo del negocio, considera la ciberseguridad y la de los datos personales como un aspecto vital para garantizar la consecución de forma efectiva y eficaz de los objetivos de negocio definidos.

La dirección de Pikolinos se compromete a liderar y fomentar a todos los niveles la seguridad de acuerdo con la política de ciberseguridad y los objetivos que en ella se definen.

2 Objetivos de ciberseguridad

La política de ciberseguridad de Pikolinos supone el compromiso expreso del grupo en determinar y establecer las directivas y el soporte adecuado para la administración de la ciberseguridad que maneja, de acuerdo con los requerimientos propios y con las leyes y regulaciones vigentes.

Se asumen de este modo los siguientes objetivos:

- Considerar la información y los sistemas que la soportan como activos estratégicos. Así pues, Pikolinos manifiesta su determinación de alcanzar los niveles de seguridad necesarios que garanticen los requisitos de confidencialidad, integridad, autenticidad, trazabilidad y disponibilidad de la información procesada en la organización y de los recursos de los sistemas de información que la procesan, almacenan o distribuyen.
- Garantizar la difusión de la normativa y procedimientos definidos como soporte de esta política, con el objetivo de conseguir infundir entre el personal que preste sus servicios en Pikoli-

nos un nivel de concienciación y formación en materia de ciberseguridad que garantice la aplicación de prácticas adecuadas en esta materia, como elemento inherente al desarrollo de sus funciones.

- Promover que la consecución de los niveles de ciberseguridad requeridos se desarrolle como un proceso continuo de mejora y progreso constante, sustentado en la definición de los objetivos y requisitos a cumplir, la implantación de los procesos y medidas oportunas, la comprobación constante de su efectividad, eficacia y eficiencia, y la adopción de las correcciones y modificaciones que resulten adecuadas.
- Adoptar la política de ciberseguridad como la principal herramienta para garantizar adecuadamente la ciberseguridad, promoviendo y asegurando su cumplimiento dentro de los diferentes servicios.
- Velar por la existencia de los mecanismos necesarios que aseguren la continuidad de las actividades críticas de la empresa que estén sustentadas en los sistemas de información, permitiendo la recuperación de estos en un periodo de tiempo aceptable.
- Maximizar la calidad de los servicios prestados.
- Reducir o eliminar los peligros y riesgos en los activos, procesos y servicios de Pikolinos.

3 Principios básicos de Ciberseguridad

Los principios básicos de ciberseguridad de Pikolinos deben promoverse a través de los siguientes enfoques y acciones:

Principio 1: impulsar y mejorar continuamente la gestión de la seguridad integrada en el modelo de Gestión, de forma que nos permita cumplir con las obligaciones legales y contractuales, así como satisfacer las necesidades y expectativas de nuestros clientes y demás grupos de interés.

Se entiende por gestión de la ciberseguridad el conjunto de actividades que permiten adoptar las medidas técnicas y organizativas que garanticen la integridad, confidencialidad y disponibilidad de la información manejada en Pikolinos.

Principio 2: Promocionar una cultura de seguridad entre el personal y colaboradores externos, implicándolos en la consecución de los objetivos.

Una cultura de ciberseguridad para las personas implica:

- Establecer, desplegar y mantener políticas, normas y procedimientos de ciberseguridad.
- Definir los planes de formación en ciberseguridad.
- Concienciar sobre la ciberseguridad.
- Supervisar el cumplimiento de las buenas prácticas de ciberseguridad.

El Comité de Ciberseguridad en conjunto con el Departamento de Sistemas define y revisa las directrices generales de ciberseguridad para establecer los principios y directrices de actuación para toda Pikolinos. Los responsables de ciberseguridad de las Filiales son los que garantizan su despliegue y aplicación.

Principio 3: Salvaguardar los datos de toda índole relativos a Pikolinos y a sus grupos de interés, ya sea en términos tanto en materia de propiedad intelectual, industrial, secretos comerciales u otros ámbitos.

La protección de los datos se consigue mediante la definición y el establecimiento de normas, procedimientos y controles que aseguren la disponibilidad, confidencialidad e integridad de la información y los datos de Pikolinos y de las partes externas (proveedores, socios, clientes, etc.).

Deben establecerse los requisitos de clasificación de la información para determinar el nivel de confidencialidad que corresponde a los diferentes datos e informaciones. Son las filiales las que clasifican la información en sus respectivos filiales en base a la documentación corporativa y conceden especial atención a los datos personales y otros datos identificados como sensibles en Pikolinos, incluyendo los acuerdos de confidencialidad con los proveedores y socios, la propiedad intelectual, industrial y los secretos comerciales.

4 Implementación

Para la implementación de esta política, cada filial establece planes de acción que son supervisados por el Comité Corporativo de Ciberseguridad.

5 Actualizaciones de la política de seguridad

Debido a la propia evolución de la tecnología, las amenazas de seguridad y a las nuevas aportaciones legales en la materia, Pikolinos se reserva el derecho a modificar estas políticas cuando sea necesario. Los cambios realizados en estas políticas serán divulgados a toda la plantilla y personas usuarias utilizando los medios que se consideren pertinentes. Es responsabilidad de cada uno de estos la lectura y conocimiento de las políticas de seguridad más recientes de Pikolinos.

Se revisará anualmente la presente política, a efectos de mantenerla actualizada. Estos cambios deberán ser revisados y aprobados por el Comité de Seguridad de Pikolinos.