Tipo de Documento: POLÍTICA

Política de Seguridad de la Información

ÍNDICE

1.- OBJETO, ALCANCE Y NORMA

Objeto:

Esta Política tiene por objeto facilitar las directivas o directrices que deben seguirse para proteger la información de la Organización de una amplia gama de amenazas, a fin de:

- Garantizar la seguridad de las operaciones realizadas mediante los Sistemas de Información.
- Minimizar los riesgos de daño.
- Asegurar el cumplimiento de los objetivos de la Organización.

Tecnología y Sistemas de Información tiene la voluntad de conseguir que los principios de la Política de Seguridad de la Información formen parte de la cultura de PortAventura, para lo cual ha implementado un Sistema de Gestión de la Seguridad de la Información con base a un estándar reconocido internacionalmente.

Todo el personal de Tecnología y Sistemas de Información, incluidos colaboradores, proveedores y la dirección, debe conocer y cumplir esta Política.

Esta Política se desarrollará mediante una normativa, procedimientos, instrucciones operativas, guías, manuales y todos aquellos instrumentos organizativos considerados útiles para alcanzar sus objetivos.

Alcance:

Esta normativa se aplica a todo el ámbito de actuación de Tecnología y Sistemas de Información (en adelante, TSI), y sus contenidos traen causa de las directrices de carácter más general definidas en el ordenamiento jurídico vigente, en la Política de Seguridad de la Información y en las Normas de Seguridad de TSI.

El alcance de la Política de Seguridad de la Información coincide con el alcance del Sistema de Gestión de la Seguridad de Información (SGSI).

Norma:

Las referencias tenidas en cuenta para la redacción de esta normativa han sido:

- ISO/IEC 27001:2013 en su dominio N.5.2 «Política»
- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (RGPD).
- Ley 3/2018 de Protección de Datos y Garantía de los Derechos Digitales (LOPD-GDD).

Este procedimiento se aplica a todos los documentos y registros relacionados con el SGSI, creados por PortAventura.

2.– DEFINICIONES

A los efectos de una correcta interpretación de la presente Política, se incluyen las siguientes definiciones:

- **Información**: datos que poseen significado, en cualquier formato o soporte. Se refiere a toda comunicación o representación de conocimiento.
- **Sistema de Información**: un conjunto de recursos relacionados y organizados para el tratamiento de información, según determinados procedimientos, tanto informáticos como manuales.

3.– ESPECIFICACIONES

3.1 Objetivos de la Política de Seguridad de la Información

El objetivo principal de la creación de esta Política de Seguridad de la Información, por parte del Responsable de Seguridad del Sistema de Gestión de la Seguridad de la Información (SGSI) y de la Dirección de Tecnología y Sistemas de Información, es garantizar a los clientes y usuarios de los servicios el acceso a la información con la calidad y el nivel de servicio que se requieren para el desempeño acordado, así como evitar serias pérdidas o alteración de la información, y accesos no autorizados.

Se establece un marco para la consecución de los objetivos de Seguridad de la Información para la Organización. Dichos objetivos se alcanzarán mediante una serie de medidas organizativas y de normas concretas y claramente definidas.

Esta Política de Seguridad será mantenida, actualizada y adecuada a los fines de la Organización.

Los principios que deben respetarse, con base a las dimensiones básicas de la seguridad, son los siguientes:

- **Confidencialidad**: propiedad por la cual únicamente puede acceder a la información gestionada por Tecnología y Sistemas de Información quien esté autorizado para ello, previa identificación, en el momento y por los medios habilitados.
- **Integridad**: propiedad que garantiza la validez, exactitud y completitud de la información gestionada por Tecnología y Sistemas de Información, siendo su contenido el facilitado por los

afectados sin ningún tipo de manipulación y permitiendo que sea modificada únicamente por quien esté autorizado para ello.

- **Disponibilidad**: propiedad que puede ser accesible y utilizada en los intervalos acordados. La información gestionada por Tecnología y Sistemas de Información es accesible y utilizable por los clientes y usuarios autorizados e identificados en todo momento, quedando garantizada su propia persistencia ante cualquier eventualidad prevista.

Adicionalmente, dado que cualquier Sistema de Gestión de la Seguridad de la Información debe cumplir con la legislación vigente, se atenderá al siguiente principio:

- **Legalidad**: en referencia al cumplimiento de las leyes, normas, reglamentaciones o disposiciones a las que está sujeta Tecnología y Sistemas de Información, especialmente en materia de protección de datos personales.

3.2 Política de Control de Gestión del Riesgo

La Gestión de la Seguridad de la Información en Tecnología y Sistemas de Información está basada en el riesgo, de conformidad con la Norma internacional ISO/IEC 27001:2013.

Se articula mediante un proceso general de apreciación y tratamiento del riesgo, que potencialmente puede afectar a la seguridad de la información de los servicios prestados, consistente en:

- **Identificar las amenazas**, que aprovecharán vulnerabilidades de los Sistemas de Información que soportan, o de los que depende, la seguridad de la información.
- **Analizar el riesgo** con base a la consecuencia de materializarse la amenaza y de la probabilidad de ocurrencia.
- **Evaluar el riesgo** según un nivel previamente establecido y aprobado de riesgo (ampliamente aceptable, tolerable e inaceptable).
- **Tratar el riesgo inaceptable** mediante los controles o salvaguardas adecuados.

Dicho proceso es cíclico y debe llevarse a cabo de forma periódica, como mínimo una vez al año. Para cada riesgo identificado se asignará un propietario, pudiendo recaer múltiples responsabilidades en una misma persona o comité.

3.3 Roles, responsabilidad y autoridad

La organización de la Seguridad de la Información gira en torno a un Sistema de Gestión de Seguridad de la Información (SGSI) y a una serie de comités y roles involucrados en su ámbito.

3.4 Marco para la fijación de objetivos de Seguridad de la Información

La fijación de objetivos de Seguridad de la Información se realiza teniendo en cuenta las siguientes entradas:

- Informes del Responsable de Seguridad del Sistema de Gestión de la Seguridad de la Información, aprobados por la Dirección de Tecnología y Sistemas de Información.
- Oportunidades de mejora encontradas durante la operación del SGSI.

En la fijación de objetivos, se debe tener en cuenta que los mismos deben ser medibles y alcanzables, de ahí que la planificación para su consecución deba incluir:

- Lo que se va a hacer
- Los recursos necesarios
- Quién será el responsable
- El plazo para su consecución
- Cómo se evaluarán los resultados
- Si procede, el indicador asociado a dicho objetivo

La Dirección, junto con el Responsable de Seguridad del Sistema de Gestión de la Seguridad de la Información, se responsabilizará de definir los objetivos de seguridad de la información para Tecnología y Sistemas de Información, que deberán ser específicos y consecuentes con su Política de Seguridad de la Información, misión, visión y valores.

3.5 Objetivo del SGSI

El SGSI de Tecnología y Sistemas de Información debe garantizar:

- Que se desarrollen políticas, normativas, procedimientos y guías operativas para apoyar la Política de Seguridad de la Información.
- Que se identifique la información que deba ser protegida.
- Que se establezca y mantenga la gestión del riesgo alineada con los requerimientos de la Política del SGSI y la estrategia de Tecnología de Sistemas de Información.
- Que se establezca una metodología para la apreciación y el tratamiento del riesgo.
- Que se establezcan criterios con los que medir el nivel de cumplimiento del SGSI.
- Que se revise el nivel de cumplimiento del SGSI.
- Que se corrijan las no conformidades mediante la implementación de acciones correctivas.
- Que el personal reciba formación y concienciación sobre la seguridad de la información.
- Que todo el personal sea informado sobre la obligación de cumplimiento de la Política de Seguridad de la Información.
- Que se asignen los recursos necesarios para gestionar el SGSI.
- Que se identifiquen y se cumplan todos los requisitos legales, regulatorios y contractuales.
- Que se identifiquen y analicen las implicaciones de seguridad de la información respecto a los requerimientos de negocio.

- Que se mida el grado de madurez del propio Sistema de Gestión de la Seguridad de la Información.

3.6 Organización y responsabilidad

- La Dirección de Tecnología y Sistemas de Información es la responsable de aprobar la presente política.
- El Comité de Gestión de la Seguridad de la Información es el responsable de revisar la presente Política.
- El Responsable de Seguridad del SGSI es el responsable de mantener la presente política.

Esta política debe ser revisada regularmente junto al resto de las Políticas Corporativas sobre la base del esquema de revisión acordado, y siempre que se realicen cambios relevantes, con el fin de asegurar que esté alineada con la estrategia de TSI.

3.7 Aplicación de la Política

La Dirección de Tecnología y Sistemas ha desarrollado el presente documento, que contiene la Política General para la Seguridad de la Información y que ha sido aprobada por la Dirección General y dada a conocer a todo el personal.

3.8 Formación y concienciación

El Responsable de Seguridad del Sistema de Gestión de la Seguridad de la Información debe garantizar que todo el personal involucrado en el SGSI conoce esta Política, sus objetivos y procesos, mediante su divulgación, acciones formativas y acciones de concienciación.

También debe garantizar la distribución de los documentos que aplican a cada nivel, de acuerdo con los diferentes roles definidos en TSI.

3.9 Auditoría

La Dirección General de Tecnología y Sistemas de Información debe garantizar y verificar, mediante auditorías internas y externas, el grado de cumplimiento y el correcto cumplimiento y operatividad de las directrices de esta Política, responsabilizándose del cumplimiento de las medidas correctivas que hayan podido determinarse con el fin de mantener la mejora continua.

3.10 Validez y actualización

Esta Política es efectiva desde el momento de su publicación y se revisa como mínimo una vez al año.

El objetivo de las revisiones periódicas es adecuarla a los cambios en el contexto de la Organización, con atención a las cuestiones externas e internas, y analizando las incidencias acaecidas de Seguridad de la Información y las no conformidades encontradas en el SGSI. Todo ello, armonizado con los resultados de los diferentes procesos de apreciación del riesgo.

Al revisar la Política también se revisarán todas las normas y demás documentos que la desarrollan, siguiendo un proceso de actualización periódica sujeto a los cambios relevantes que pudieran acontecer: crecimiento del área de TSI y cambios organizacionales, cambios en la infraestructura o desarrollo de nuevos servicios, entre otros.

En consecuencia, se elaborará una lista de objetivos y acciones a emprender y ejecutar durante el año siguiente para garantizar la Seguridad de la Información y el buen uso de los recursos que la soportan y tratan en Tecnología y Sistemas de Información.

4. SANCIONES

El incumplimiento de la Política de Seguridad de la Información y del resto de normativas y procedimientos que la desarrollan, tendrá como consecuencia la aplicación de sanciones, conforme a la magnitud y a las características del aspecto no cumplido, y de acuerdo con la legislación laboral vigente.