Política de Seguridad de la Información y Continuidad de Negocio

2024

VASS

complex made simple

Índice

1. Objeto 3

2. Objetivos de la Política 3

3. SIG 4

4. Obligaciones del Personal 4

Información de Contacto 5

1. Objeto

La Dirección de VASS Consultoría de Sistemas SL (en adelante VASS), dentro de la estrategia definida para el desarrollo del negocio, considera la seguridad de la información y la continuidad de negocio aspectos fundamentales para garantizar la consecución de los objetivos de negocio y la adecuación a la legislación vigente. Por ello, se compromete a mantener un nivel de seguridad adecuado y alineado al negocio, en los procesos asociados a los servicios prestados por la organización, con objeto de ofrecer a sus clientes internos y externos las mayores garantías en cuando a la calidad de dichos servicios.

2. Objetivos de la Política

VASS es una empresa proveedora de soluciones digitales cuya misión es ayudar a los clientes a transformar las oportunidades en negocio.

Para el cumplimiento de su Misión, la prestación de los Servicios y el cumplimiento de sus objetivos, VASS depende de sistemas TIC. Estos sistemas deben ser administrados con diligencia, tomando las medidas adecuadas para protegerlos frente a daños accidentales o deliberados que puedan afectar a la confidencialidad, disponibilidad, integridad, autenticidad y trazabilidad de la información tratada o los servicios prestados.

Con la implantación de un Sistema Integrado de Gestión (en adelante SIG) bajo las Normas UNE ISO/IEC 27001 y UNE-EN-ISO 22301:2020, se fortalece la seguridad y la continuidad de los servicios, así como de la información y datos que incluyen dichos servicios y que son necesarios para su correcta y adecuada prestación, por la estrecha relación entre ambos y los elementos adicionales que mejoran notablemente la gestión de la seguridad que es necesaria para VASS, como parte del cumplimiento satisfactorio de su misión.

El objetivo de la seguridad de la información y de la continuidad de negocio es garantizar la calidad de la información y la prestación continuada de los servicios, actuando preventivamente, supervisando la actividad diaria y reaccionando con presteza a los incidentes.

Dentro de este contexto, los objetivos de la presente Política del Sistema de Gestión de Seguridad de la Información y la Continuidad de Negocio son:

- Garantizar los aspectos de confidencialidad, disponibilidad, integridad, autenticidad y trazabilidad de la información.
- Gestionar el riesgo de seguridad existente hasta los umbrales establecidos por la dirección, en base a la prestación del servicio a clientes.
- Implantar un SIG para gestionar y proteger la información y servicios que presta la compañía.
- Implantar un conjunto de medidas o controles de seguridad adecuados, determinadas por la Norma UNE ISO/IEC 27001, así como cualquier control adicional identificado, como parte del SIG para asegurar la protección ante amenazas que puedan incidir en la autenticidad, trazabilidad, confidencialidad, integridad, disponibilidad, uso previsto y valor de la información y los servicios. a través de la evaluación de amenazas y riesgos.
- Nombrar un responsable del SIG, encargado de gestionar el sistema y velar por el desarrollo, mantenimiento y mejora del mismo.
- Nombrar un Responsable de Seguridad y asegurar que dispone de los recursos necesarios para llevar a cabo los controles de seguridad de la información necesarios.
- Establecer una metodología de revisión, auditoría y mejora continua del SIG, siguiendo un ciclo PDCA que garantice el mantenimiento continuo de los niveles de seguridad deseados.

- Establecer periódicamente un conjunto de objetivos e indicadores en materia de gestión de seguridad de la información y de continuidad de negocio, que permitan a la dirección llevar a cabo un adecuado seguimiento del nivel de seguridad y cumplimiento de los objetivos.
- Garantizar que el personal de la organización dentro del alcance dispone del suficiente conocimiento sobre las políticas y los controles de seguridad de la información y de continuidad de negocio.
- Asegurar que los incidentes de seguridad de la información son correctamente identificados, gestionados y resueltos.
- Cumplir con todos los requisitos legales, normativos, reglamentarios aplicables y obligaciones contractuales.
- Asegurar la continuidad de los procesos de negocio incluidos dentro del alcance.

3. SIG

La Dirección de VASS se compromete a destinar los recursos y medios necesarios para establecer, implantar, mantener y mejorar el SIG y los controles de seguridad necesarios, manteniendo un adecuado balance entre coste y beneficio, así como a demostrar liderazgo y compromiso respecto a este.

3.1. Establecimiento, despliegue y mejora del SIG

El establecimiento y despliegue del SIG de VASS se iniciará a partir del Análisis de Riesgos, que permitirá determinar el nivel de riesgo de seguridad de la información y de continuidad de negocio en que se encuentra VASS e identificar los controles de seguridad necesarios para el tratamiento del riesgo y llevarlo a un nivel aceptable, así como las oportunidades de mejora, considerando las cuestiones internas y externas y los requisitos de las partes interesadas.

Los controles de seguridad deberán implantarse, mantenerse y mejorarse continuamente, y estar disponibles como información documentada, mediante procedimientos, normativas, instrucciones técnicas, y cualquier otra documentación que así se considere, revisados y aprobados por el Comité de Seguridad de la Información y Continuidad de Negocio.

Se deberá comunicar la información documentada de los controles de seguridad al personal que trabaja en VASS (empleados y proveedores), que tendrá la obligación de aplicarla en la realización de sus actividades laborales, comprometiéndose de ese modo, al cumplimiento de los requisitos del SIG.

3.2. Evaluación

Se realizarán auditorías periódicamente que revisen y verifiquen el cumplimiento del SIG con los requisitos de la Norma ISO/IEC 27001, por lo que, en caso necesario, el personal afectado por el alcance deberá colaborar en estas, así como en la aplicación de las acciones correctivas que se deriven para el mejoramiento continuo. Se definirán criterios de cualificación para las personas que realicen dichas auditorías.

4. Obligaciones del Personal

Los gerentes de los departamentos de VASS incluidos dentro del alcance de esta política serán los responsables de asegurar su cumplimiento de dichas políticas dentro de sus departamentos.

Todos los trabajadores de VASS tienen la obligación de conocer esta Política de Seguridad de la Información y la Continuidad de Negocio y la Normativa de Seguridad que la desarrolla, que son de obligado cumplimiento dentro del alcance identificado, siendo responsabilidad del Comité de Seguridad disponer los medios necesarios para que la información llegue a los afectados.

Todo personal contratado deberá recibir y firmar un compromiso de cumplimiento de la política de seguridad de la información y de continuidad de negocio y de la normativa de seguridad, y deberá recibir formación o concienciación relativa a la seguridad de la información y la continuidad de negocio, en función de cuál sea su puesto de trabajo

Información de Contacto

Av de Europa, 1, edificio B. 28108 Alcobendas, Madrid, Spain

info@vasscompany.com

+34 91 662 3404