POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

CEITA, es una empresa tecnológica que ofrece servicios y productos a medida de consultoría e implementación de digitalización de BPM, y solución entre industrias.

Por este motivo ha implantado un **Sistema de Gestión de Seguridad de la Información**, cuyo objetivo es alcanzar la satisfacción esperada por los clientes a través de unos procesos establecidos y fundamentados en la mejora continua, garantizando la continuidad de los sistemas de información, minimizando riesgos y asegurando el cumplimiento de los objetivos fijados, para asegurar en todo momento la **confidencialidad, integridad** y **disponibilidad** de la información.

Para ello asumimos nuestro compromiso con la seguridad de la información, según las normas de referencia **ISO /IEC 27001:2013**, para lo que la Dirección establece los siguientes principios:

- **Competencia y liderazgo** por parte de la Dirección como compromiso para desarrollar el sistema de Seguridad de la Información.
- Determinar las **partes interesadas** internas y externas involucradas en el sistema de gestión de seguridad de la información y cumplir con sus requisitos.
- Entender el **contexto de la Organización** y determinar las oportunidades y los **riesgos** de la misma, como base para la planificación de acciones, asumirlos o tratarlos.
- Garantizar la **satisfacción de nuestros clientes**, incluyendo las partes interesadas en los resultados de la empresa, en todo lo referente al desarrollo de nuestras actividades y su posible repercusión en la sociedad.
- Establecer **objetivos y metas** enfocados hacia la evaluación del desempeño en materia de seguridad, así como a la **mejora continua** en las actividades reguladas en el Sistema de Gestión de seguridad de la información.
- Cumplir los requisitos de la **legislación aplicable** a nuestra actividad, los compromisos adquiridos con los clientes y las partes interesadas, y todas aquellas normas internas o pautas de actuación a los que se someta la empresa.
- Asegurar la **confidencialidad** de los datos gestionados, la **integridad** y la **disponibilidad** de los sistemas de información, tanto en los servicios ofrecidos a los clientes, como en la gestión interna, evitando alteraciones indebidas en la información.

- Asegurar la **capacidad de respuesta ante situaciones de emergencia**, restableciendo el funcionamiento de los servicios críticos en el menor tiempo posible.
- Establecer las medidas oportunas para **el tratamiento de los riesgos** derivados de la identificación y evaluación de activos.
- **Motivar y formar a todo el personal** que trabaja en la Organización, tanto para el correcto desempeño de su puesto de trabajo y para actuar según los requisitos de las normas de referencia; proporcionando un **ambiente adecuado** para desarrollar los procesos.
- Mantener una **comunicación** fluida tanto interna, como con clientes.
- Evaluar y garantizar la **competencia técnica del personal** para el desempeño de sus funciones, así como asegurar la adecuada motivación de éste para su participación en la mejora continua de nuestros procesos.
- Controlar y mantener un sistema de **evaluación continua de proveedores y subcontratistas** en el desempeño de su actividad y en especial en aquellos relacionados con el SGSI.
- Garantizar el **correcto estado de las instalaciones y equipamiento**, de forma tal que estén en correspondencia con la actividad, objetivos y metas de la empresa
- Garantizar un **análisis** continuo de todos los **procesos relevantes**, estableciendo las mejoras pertinentes en cada caso, en función de los resultados obtenidos y de los objetivos establecidos.

Estos principios son asumidos por la Dirección, que dispone los medios necesarios y dota a sus empleados de los recursos suficientes para su cumplimiento, plasmándose y poniéndolos en público conocimiento a través de la presente Política de Calidad y Seguridad de la Información.

ROLES Y RESPONSABILIDADES EN SEGURIDAD DE LA INFORMACIÓN

Todas las responsabilidades en seguridad de la información deben ser definidas y asignadas.

La Dirección General designa un Comité de Seguridad de la Información con los siguientes objetivos:

1. Elaborar, revisar y aprobar la política de seguridad de la información y las funciones generales en materia de seguridad de la información que fueran convenientes y apropiadas para la Empresa.

2. Monitorear cambios significativos en los riesgos que afectan a los recursos de la información de la Empresa frente a posibles amenazas, sean internas o externas.

3. Tomar conocimiento y supervisar la investigación y monitoreo de los incidentes, relativos a la seguridad de la información, que se produzcan en el ámbito de la Empresa.

4. Aprobar las principales iniciativas para incrementar la seguridad de la información, de acuerdo a las competencias y responsabilidades asignadas a cada departamento, así como acordar y aprobar procedimientos y procesos específicos relativos a la seguridad de la información.

5. Evaluar y coordinar la implementación de controles específicos de seguridad de la información para los sistemas o servicios de esta Empresa, sean preexistentes o nuevos.

6. Promover la difusión y apoyo a la seguridad de la información dentro de la Empresa, así como, coordinar el proceso de administración de la continuidad de las actividades.

El Comité de Seguridad de la Información estará integrado por representantes de la dirección y de las seguridad física y lógica.

La Dirección General asigna las funciones relativas a la Seguridad de la Información de la Empresa al "Responsable de Seguridad de la Información", quien tiene a cargo las funciones relativas a la seguridad de los sistemas de información de la Empresa, lo cual incluye la supervisión de todos los aspectos inherentes a seguridad de la información tratados en la presente Política.

En Rubí, a 06 de Marzo de 2023

Nombre del responsable: Jordi Bellver
Dirección General