Política de seguridad de la información

ALBI, tiene como misión prestar servicios de alimentación para las personas que nos necesiten, dando un servicio de calidad, arropado por valores universales: el respeto a las personas, el respeto al medioambiente y la integridad profesional. Por todo lo anteriormente expuesto, la Dirección establece los siguientes objetivos de seguridad de la información:

- Proporcionar un marco para aumentar la capacidad de resistencia o resiliencia para dar una respuesta eficaz.
- Asegurar la recuperación rápida y eficiente de los servicios, frente a cualquier desastre físico o contingencia que pudiera ocurrir y que pusiera en riesgo la continuidad de las operaciones
- Prevenir incidentes de seguridad de la información en la medida que sea técnica y económicamente viable, así como mitigar los riesgos de seguridad de la información generados por nuestras actividades.
- Garantizar la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de la información.

Para poder lograr estos objetivos es necesario:

- Mejorar continuamente nuestro sistema de seguridad de la información,
- Cumplir con requisitos legales aplicables y con cualesquiera otros requisitos que suscribamos además de los compromisos adquiridos con los clientes, así como la actualización continúa de los mismos.

El marco legal y regulatorio en el que desarrollamos nuestras actividades es:

- 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
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
- Real Decreto Legislativo 1/1996, de 12 de abril, Ley de Propiedad Intelectual
- Real Decreto-ley 2/2018, de 13 de abril, por el que se modifica el texto refundido de la Ley de Propiedad Intelectual
- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.

Debemos identificar las amenazas potenciales, así como el impacto en las operaciones de negocio que dichas amenazas, caso de materializarse, puedan causar.

Tenemos la obligación de:

➢ Salvaguardar los intereses de nuestras principales partes interesadas (clientes, accionistas, empleados y proveedores), la reputación, la marca y las actividades de creación de valor.

➢ Trabajar de forma conjunta con nuestros suministradores y subcontratistas con el fin de mejorar la prestación de servicios de TI, la continuidad de los servicios y la seguridad de la información, y que repercutan en una mayor eficiencia de nuestra actividad.

➢ Evaluar y garantizar la competencia técnica del personal, así como asegurar la motivación adecuada de éste para su participación en la mejora continua de nuestros

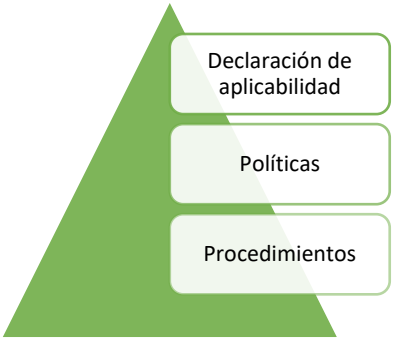
procesos, proporcionando la formación y la comunicación interna adecuada para que desarrollen las buenas prácticas exigidas a los sistemas.

➢ Garantizar el correcto estado de las instalaciones y el equipamiento adecuado, de forma tal que estén en correspondencia con la actividad, objetivos y metas de la empresa.

➢ Garantizar un análisis de manera continua de todos los procesos relevantes, estableciéndose las mejoras pertinentes en cada caso, en función de los resultados obtenidos y de los objetivos establecidos.

➢ Estructurar nuestro sistema de gestión de forma que sea fácil de comprender.

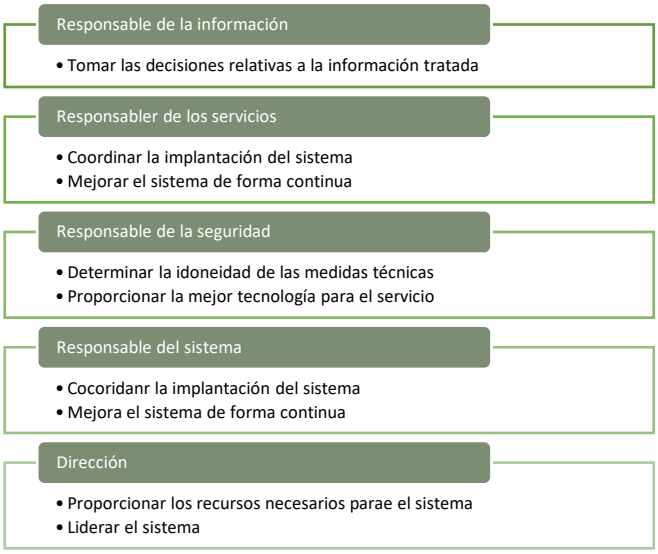
Nuestro sistema de gestión tiene la siguiente estructura:



La gestión de nuestro sistema se encomienda al Responsable de Seguridad y el sistema estará disponible en nuestro sistema de información, en un repositorio, al cual se puede acceder según los perfiles de acceso concedidos conforme nuestro procedimiento en vigor de gestión de los accesos.

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

Los roles o funciones de seguridad definidos en ALBI son:



La descripción se completa en los perfiles de puesto y en los documentos del sistema.

El procedimiento para su designación y renovación será ratificado en el comité de seguridad.
El comité para la gestión y coordinación de la seguridad es el órgano con mayor responsabilidad dentro del sistema de gestión de seguridad de la información, de forma que todas las decisiones más importantes relacionadas con la seguridad se acuerdan por este comité. Los miembros del comité de seguridad de la información son:

- Responsable de la información.
- Responsable de los servicios.
- Responsable de la seguridad.
- Responsable del sistema.
- Dirección Empresa (socios-administradores)

Estos miembros son designados por el citado comité, único órgano que puede nombrarlos, renovarlos y cesarlos.
El comité de seguridad es un órgano ejecutivo y con autonomía para la toma de decisiones y que no tiene que subordinar su actividad a ningún otro elemento de nuestra empresa. Las decisiones en el comité se toman por unanimidad y en el caso de empate el responsable de seguridad tiene voto de calidad.

Nuestra política se desarrolla aplicando los siguientes requisitos mínimos:

a) Organización e implantación del proceso de seguridad: a través del procedimiento PE SGSI A05 Políticas de Seguridad de la Información.
b) Análisis y gestión de los riesgos: a través del procedimiento PE SGSI A08.2 Análisis de Riesgos.
c) Gestión de personal: a través del procedimiento PE SGSI A07 Seguridad relativa a los Recursos Humanos.
d) Profesionalidad: a través del procedimiento PE SGSI A07 Seguridad relativa a los Recursos Humanos.
e) Autorización y control de los accesos: a través nuestro procedimiento PE SGSI A09 Control de accesos.
f) Protección de las instalaciones: a través del procedimiento PE SGSI A11 Seguridad Física y del entorno.
g) Adquisición de productos: a través del procedimiento PE SGSI-A14_Adquisición desarrollo y mantenimiento de sistemas de información.
h) Mínimo privilegio: a través del procedimiento PE SGSI A12 Seguridad de las Operaciones.
i) Integridad y actualización del sistema: PE SGSI A12 Seguridad de las Operaciones.
j) Protección de la información almacenada y en tránsito: a través de nuestro procedimiento PE SGSI A13 Seguridad en las Comunicaciones.
k) Prevención ante otros sistemas de información interconectados mediante el procedimiento PE SGSI A13 Seguridad en las Comunicaciones.
l) Registro de actividad: a través del procedimiento PE SGSI A12 Seguridad de las Operaciones.
m) Incidentes de seguridad: a través del procedimiento PE SGSI A16 Gestión de incidentes de seguridad de la Información
n) Continuidad de la actividad: a través del procedimiento PE SGSI A17- Continuidad del negocio.

o) Mejora continua del proceso de seguridad: a través del Manual Integrado de Sistemas de Gestión.

Está política se complementa con el resto de las políticas, procedimientos y documentos en vigor para desarrollar nuestro sistema de gestión.

En Boadilla del Monte a 30 de noviembre de 2023