

## **POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN**

REV 0  
FECHA 24/01/2022

La dirección de BizAway Srl SB, ha definido esta Política de Protección de Datos y se compromete a:

- Mantenerla activa asegurándose de que se revisa y actualiza periódicamente;
- Garantizar los recursos necesarios para la protección efectiva de la información;
- Definir los objetivos de seguridad de la información;
- Difundirlo a todos los niveles de su organización.

La aplicación del sistema de gestión requiere la plena participación, compromiso e interacción de todos los recursos humanos y tecnológicos.

Todas las personas que trabajan en la empresa para lograr sus objetivos están obligadas, sin excepción, a cumplir esta política en el tratamiento de datos.

El objetivo es:

1. Garantizar la seguridad y la protección de la información frente a todas las amenazas, internas o externas, intencionadas o accidentales vinculadas al ámbito de sus actividades conforme con la normativa ISO/IEC 27001 y las directrices ISO/IEC 27002.
2. Garantizar la seguridad y la protección de los datos de acuerdo con las indicaciones del Reglamento Europeo de Protección de Datos (GDPR 679/16).
3. Garantizar la activación de un proceso continuo que permita el control y la adaptación a los cambios de gestión, medioambientales, empresariales y legales que pueda encontrar la empresa.

Por lo tanto, es necesario garantizar:

1. La confidencialidad de los datos, es decir, que sólo deben ser accesibles a las personas autorizadas para ello.
2. La integridad de los datos, o lo que es lo mismo, garantizar la exactitud y exhaustividad de los mismos así como los métodos para procesarlos.

## **POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN**

REV 0

FECHA 24/01/2022

3. La disponibilidad de los datos, lo que se traduce en que sólo los usuarios autorizados puedan acceder realmente a ellos cuando los necesiten. La comunicación y difusión de datos al exterior únicamente para el correcto desempeño de las actividades de la Empresa en cumplimiento de las normas y reglamentos de obligado cumplimiento.
4. Cumplimiento de los requisitos legales y los principios de seguridad de los datos en los contratos con terceros.
5. Acatar las disposiciones legales, estatutarias, reglamentarias y obligaciones contractuales, así como de cualquier requisito de seguridad de los datos.
6. Los aspectos de seguridad deben incluirse en todas las fases de diseño, desarrollo, funcionamiento, mantenimiento, revisión y desmantelamiento de los sistemas.
7. Todo acceso a los sistemas estará sujeto a un procedimiento de identificación y autenticación, se impedirá el acceso no autorizado a los locales y a los locales individuales de la empresa donde se gestionen los datos y se garantizará la seguridad de los equipos.
8. Las autorizaciones de acceso a los datos se diferenciarán en base de la función y las obligaciones de las personas, de modo que cada usuario sólo pueda acceder a los datos que necesite revisándose periódicamente.
9. Tratarse a tiempo cualquier incidente, es decir, que todo el mundo informe de cualquier problema de seguridad.

La dirección