# POLÍTICA DE ACCESO A LA INFORMACIÓN

**Resumen de la política**:
La información debe ser siempre protegida, cualquiera que sea su forma de ser compartida, comunicada o almacenada.

**Introducción**:

a. La información puede existir en diversas formas: impresa o escrita en papel, almacenada electrónicamente, transmitida por correo o por medios electrónicos, mostrada en proyecciones o en forma oral en las conversaciones.
b. La seguridad de la información es la protección de la información contra una amplia gama de amenazas con el fin de garantizar la continuidad del negocio, minimizar los riesgos empresariales y maximizar el retorno de las inversiones y oportunidades de negocio.

**Alcance**:

a. Esta política es de consideración por parte de todos los miembros de la organización.

# POLÍTICA DE ACCESO A LA INFORMACIÓN

**Objetivos de seguridad de la información**:

- Comprender y tratar los riesgos operacionales y estratégicos en seguridad de la información para que permanezcan en niveles aceptables para la organización.
- La protección de la confidencialidad de la información relacionada con los clientes y con los planes de desarrollo.
- La conservación de la integridad de los registros contables.
- Los servicios Web de acceso público y las redes internas cumplen con las especificaciones de disponibilidad requeridas.
- Entender y dar cobertura a las necesidades de todas las partes interesadas.

# POLÍTICA DE ACCESO A LA INFORMACIÓN

**Principios de seguridad de la información**:

1. Esta organización afronta la toma de riesgos y tolera aquellos que, en base a la información disponible, son comprensibles, controlados y tratados cuando es necesario.
2. Todo el personal será informado y responsable de la seguridad de la información, según sea relevante para el desempeño de su trabajo.
3. Se dispondrá de financiación para la gestión operativa de los controles relacionados con la seguridad de la información y en los procesos de gestión para su implantación y mantenimiento.
4. Se tendrán en cuenta aquellas posibilidades de fraude relacionadas con el uso abusivo de los sistemas de información dentro de la gestión global de los sistemas de información.
5. Se harán disponibles informes regulares con información de la situación de la seguridad.
6. Los riesgos en seguridad de la información serán objeto de seguimiento y se adoptarán medidas relevantes cuando existan cambios que impliquen un nivel de riesgo no aceptable.
7. Las situaciones que puedan exponer a la organización a la violación de las leyes y normas legales no serán toleradas.

# POLÍTICA DE ACCESO A LA INFORMACIÓN

## Responsabilidades:

1. El equipo directivo es el responsable de asegurar que la seguridad de la información se gestiona adecuadamente en toda la organización.
2. Cada gerente es responsable de garantizar que las personas que trabajan bajo su control protegen la información de acuerdo con las normas establecidas por la organización.
3. El responsable de seguridad asesora al equipo directivo, proporciona apoyo especializado al personal de la organización y garantiza que los informes sobre la situación de la seguridad de la información están disponibles.
4. Cada miembro del personal tiene la responsabilidad de mantener la seguridad de información dentro de las actividades relacionadas con su trabajo.

## Indicadores clave:

1. Los incidentes en seguridad de la información no se traducirán en costes graves e inesperados, o en una grave perturbación de los servicios y actividades comerciales.
2. Las pérdidas por fraude serán detectadas y permanecerán dentro de unos niveles aceptables.
3. La aceptación del cliente de los productos o servicios no se verá afectada negativamente por aspectos relacionados con la seguridad de la información.