



# POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

## 1. INTRODUCCIÓN

---

La presente política define los criterios y lineamientos esenciales para la administración, uso y protección de la información, al igual que de los recursos informáticos asociados a su tratamiento, almacenamiento y transmisión.

La misma se basa en estándares, normas y regulaciones nacionales e internacionales de Seguridad de Información y Ciberseguridad como el estándar del organismo International Organization for Standardization (ISO) / International Electrotechnical Commission (IEC) con sus estándares para directrices de un Sistema de Gestión de Seguridad de Información y su estándar directrices Ciberseguridad, serie de publicaciones especiales 800 del National Institute of Standard and Technology (NIST), recomendaciones del organismo Center for Internet Security (CIS) y en los lineamientos estratégicos de Jiménez & Espinoza Asociados. La Dirección de Jiménez & Espinoza Asociados, su cuerpo ejecutivo y todo el personal entienden que la Información propia y de clientes es un recurso fundamental para la organización y por consiguiente asumen la responsabilidad que les corresponde por la adecuada protección de ésta.

## 2. DEFINICIÓN

---

Se define como Seguridad de la Información a la protección de la misma de un amplio espectro de amenazas. Su propósito es minimizar los riesgos del negocio, garantizar la continuidad operacional y maximizar el retorno sobre las inversiones y oportunidades de negocio de Jiménez & Espinoza Asociados.

## 3. ALCANCE

---

La presente política es aplicable a la empresa Jiménez & Espinoza Asociados e incluye:

- Los activos de información físicos o digitales, ya sea propiedad de Jiménez & Espinoza Asociados o de sus clientes que se encuentren bajo la custodia o administración de Jiménez & Espinoza Asociados.
- La infraestructura tecnológica que permite generación, procesamiento, transmisión y almacenamiento de información.
- La infraestructura tecnológica que brinda el soporte para los productos y/o servicios que la compañía ofrece en sus distintos mercados, la cual constituye el ciberespacio de la compañía.



## POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

- Las instalaciones físicas donde residen los activos físicos y digitales o la infraestructura tecnológica de la compañía.
- Las personas que hacen uso de los activos de información y ciberespacio sean estas personal de Jiménez & Espinoza Asociados, de los clientes o pertenecientes a empresas prestadoras de servicios.

### 4. REVISIÓN, VALIDACIÓN Y DIFUSIÓN

---

La presente política debe ser revisada en forma anual y actualizada cuando sea necesario. La Dirección de Jiménez & Espinoza Asociados es la encargada de aprobar la política corporativa de Seguridad de la Información y sus actualizaciones.

En caso de no existir modificaciones, ya sea a esta u otras políticas corporativas, deberá indicarse la justificación correspondiente en el registro de cambios del documento respectivo.

Una copia de esta política general debe ser distribuida a todo el personal de Jiménez & Espinoza Asociados actualmente contratado, a aquellos empleados que estén siendo incorporados a la organización y a terceros que presten servicios.

### 5. OBJETIVOS DE LA POLÍTICA

---

- Establecer requerimientos que permitan la incorporación de prácticas para la protección adecuada, razonable y efectiva de los activos físicos o digitales de la organización y su ciberespacio durante el uso cotidiano de los mismos.
- Mantener la confidencialidad, integridad y disponibilidad de los activos físicos o digitales y ciberespacio de la compañía.
- Identificar los riesgos que pudieran materializarse sobre los activos físicos o digitales y ciberespacio de la compañía, a través de una adecuada evaluación de riesgo, de forma de entender las vulnerabilidades y las amenazas a las cuales están expuestos.
- Gestionar los riesgos en un nivel aceptable a través del diseño, implementación y mantenimiento de un Sistema de Gestión de la Seguridad de la Información (SGSI).



## POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

- Favorecer la comunicación, sensibilización e información de los lineamientos de seguridad a todos los Integrantes de la empresa.

### 6. DOCUMENTOS DE LA POLÍTICA

---

Todos los documentos componentes de la presente política se encuentran disponibles en la Intranet.

Los mismos están organizados según el siguiente criterio:

**Nivel 1:** Política de Seguridad de la Información.

**Nivel 2:** Normativas de Seguridad.

**Nivel 3:** Estándares de seguridad de información y otros lineamientos de nivel operativo, procedimientos y guías.

### 7. REGLAS DE LA POLÍTICA

---

- a) Todo el personal de Jiménez & Espinoza Asociados sea este permanente o temporal, tiene la obligación de proteger los activos de información físicos o digitales, los sistemas y la infraestructura tecnológica de la organización, actuando siempre de forma responsable y profesional, manteniendo pleno conocimiento de los establecido por la presente política.
- b) Todos los activos de información físicos o digitales, como la infraestructura tecnológica, al igual que los riesgos a los que están expuestos deben poseer un dueño designado, quien será responsable de asegurar que los mismos se encuentren debidamente inventariados y clasificados según su sensibilidad y criticidad. Es también su responsabilidad el realizar una revisión periódica de dicha clasificación y de las autorizaciones de acceso a los mismos.
- c) Todos los activos de información físicos o digitales y la infraestructura física y tecnológica deben ser protegidos en función de su clasificación y según lo definido por la evaluación de riesgos correspondiente.
- d) Todo proyecto que involucre activos de información ya sea física y digital, o infraestructura tecnológica, debe desde su concepción, incorporar los requerimientos de seguridad definidos por los dueños de los activos afectados. El proceso de incorporación y validación de la seguridad de los activos debe estar integrado a la administración de proyectos desde la etapa de diseño.
- e) Todo el personal Jiménez & Espinoza Asociados tiene la responsabilidad de notificar incidentes de seguridad y potenciales debilidades que pudieran detectarse.
- f) Será responsabilidad del Oficial de Seguridad de la Información, la implementación de un programa adecuado de sensibilización y capacitación. Este programa deberá estar disponible para todo el personal de Jiménez & Espinoza Asociados incluyendo empleados permanentes, temporales y externos.



## POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

- g) La organización declara su decisión de mejorar continuamente los procesos y niveles de seguridad a través de un seguimiento permanente de los controles y procedimientos implantados. Del mismo modo, declara su intención de asegurar la existencia de planes de contingencia que permitan garantizar la continuidad de la operación de la compañía y de sus clientes.
- h) La organización declara su decisión de cumplir con la normativa y legislación vigente en temas de Seguridad de la Información, junto a los requerimientos contractuales establecidos por los clientes con relación a la misma.
- i) Cada Gerencia dueña de activos será responsable de eliminar, mitigar, transferir o aceptar los riesgos asociados a estos durante todo el ciclo de vida del activo.
- j) Cada gerencia responsable de activos debe identificar las amenazas a las que están expuestos, para posteriormente seleccionar e implementar los controles que apoyen la mitigación de los riesgos que implican las amenazas., considerando una estrategia de defensa en profundidad.
- k) La Gerencia de Ciberseguridad de Jiménez & Espinoza Asociados será responsable de la gestión de los temas de la Seguridad de la Información, teniendo la autoridad para su implantación, control y autorización de desviaciones o excepciones que, por naturaleza del alcance, no apliquen.

### 8. SANCIONES

---

- a) El incumplimiento de las normas de Seguridad de la Información se sujetará a las medidas y procedimientos previstos en el Reglamento Interno de Orden, Higiene y Seguridad.

### 9. Instrucciones de Trabajo Asociadas

---

✓ No aplica.

### 10. Registros

---

NOMBRE	RESPONSABLE	LUGAR DE ALMACENAMIENTO	TIPO DE PROTECCIÓN	RECUPERACION	TIEMPO ALMACENAMIENTO	DISPOSICIÓN

### Anexos

---

✓ No Aplica