# Política de Uso Aceptable de Bienes

[Soggetto]

# 1 Control de versiones de documentos

| | **última edición** | **Última edición por** | **Cambios en documentos** |
|---|---|---|---|
| 0.1 | [FECHA] | | Documento creado por primera vez |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

# 2 Índice

# 3 Política de Uso Aceptable de Bienes

## 3.1 Alcance

El propósito de esta política es dar a conocer a los empleados y usuarios de terceros las reglas para el uso aceptable de los recursos asociados con la información y el procesamiento de la información.

## 3.2 Destinatarios

Todos los empleados y terceros usuarios.

## 3.3 Principio

El uso de los recursos está en línea con la legislación aplicable, las políticas de la empresa y se implementa para salvaguardar los datos de la empresa, los empleados y los clientes. Cada usuario debe ser responsable de sus actos y actuar con responsabilidad y profesionalidad.

## 3.4 Responsabilidad individual

El acceso a los sistemas informáticos se controla mediante ID de usuario, contraseña y/o token. Todos los ID de usuario y contraseñas deben asignarse de manera exclusiva a personas designadas y, como resultado, las personas son responsables de todas las acciones en los sistemas de TI corporativos.

Los individuos no deben:

- Permita que cualquier otra persona use su ID de usuario/token y contraseña en cualquier sistema de TI corporativo.
- Deje sus cuentas de usuario iniciadas en una computadora desatendida y desbloqueada.
- Use el ID de usuario y la contraseña de otra persona para acceder a los sistemas de TI corporativos.
- Deje la contraseña sin protección (por ejemplo, escríbala).
- Realizar cambios no autorizados en los sistemas o la información de la empresa.
- Intentar acceder a datos que no están autorizados a usar o acceder.
- Exceda los límites de su autorización o necesidad comercial específica para consultar el sistema o los datos.
- Conectar cualquier dispositivo no autorizado por la empresa a la red corporativa o sistemas informáticos.
- Almacene datos corporativos en cualquier equipo corporativo no autorizado.

- Proporcionar o transferir datos o software de la Compañía a cualquier persona u organización fuera de la Compañía sin la autorización de la Compañía,

Los gerentes de línea deben asegurarse de que las personas reciban una guía clara sobre el alcance y los límites de su autoridad sobre los sistemas y datos de TI.

## 3.5 Uso de Internet y correo electrónico

El uso de Internet y el correo electrónico de la empresa está destinado a uso comercial. El uso personal está permitido cuando dicho uso no afecta negativamente el desempeño comercial del individuo, no es perjudicial para el negocio de ninguna manera, no viola los términos y condiciones de empleo, y no coloca al individuo o al negocio en incumplimiento de la ley. u otras obligaciones legales.

Todos los individuos son responsables de sus propias acciones en Internet y en los sistemas de correo electrónico.

**no deben** :

- Enviar o almacenar información de tarjetas de pago como:

  Número de tarjeta de pago (número de cuenta principal o PAN)

  Código de seguridad (CVV2, etc.)

  Fechas de inicio y vencimiento

- Utilizar Internet o el correo electrónico con fines de acoso o abuso.
- Usar blasfemias, obscenidades o comentarios despectivos en las comunicaciones.
- Acceda, descargue, envíe o reciba datos (incluidas imágenes) que la empresa considere ofensivos de cualquier forma, incluido material sexualmente explícito, discriminatorio, difamatorio o calumnioso.
- Usar Internet o el correo electrónico para obtener ingresos personales o para realizar un negocio personal.
- Utilice Internet o el correo electrónico para apostar.
- Usar los sistemas de correo electrónico de una manera que pueda comprometer su confiabilidad o efectividad, como distribuir cartas en cadena o spam.
- Publicar cualquier información en Internet relacionada con la Compañía, alterar cualquier información al respecto o expresar opiniones sobre la Compañía a menos que sean

  específicamente autorizado para ello.
- Enviar información sensible, interna o confidencial que no esté protegida.
- Reenviar correo corporativo a cuentas de correo electrónico personales (no corporativas) (como una nube personal o una cuenta de dominio propio).
- Hacer compromisos oficiales a través de Internet o correo electrónico en nombre de la empresa, a menos que esté autorizado para hacerlo.

- Descargue cualquier material protegido por derechos de autor, como archivos multimedia de música (MP3), películas y archivos de video (lista no exhaustiva) sin la debida aprobación.
- Infringir cualquier derecho de autor, derecho de base de datos, marca registrada u otra propiedad intelectual de cualquier manera.
- Descargue, instale o distribuya cualquier software de Internet sin la aprobación previa del departamento de TI.
- Conecte dispositivos corporativos a Internet mediante conexiones no estándar.

## 3.6 Trabajando fuera del sitio

Es aceptable que las computadoras portátiles y los dispositivos móviles se retiren del sitio. Se deben aplicar los siguientes controles:

- El trabajo fuera del sitio debe estar en línea con la política de trabajo remoto de la empresa.
- Debe usar encriptación en su computadora portátil y dispositivo móvil.
- Las computadoras portátiles y los dispositivos móviles también deben estar protegidos al menos con una contraseña o PIN.
- El equipo y los medios que se lleven fuera del sitio no deben dejarse desatendidos en lugares públicos, incluido el transporte público, y no deben dejarse a la vista en un automóvil.

- Las computadoras portátiles y los dispositivos móviles deben llevarse como equipaje de mano durante el viaje.
- La información debe protegerse contra pérdida o compromiso cuando se trabaja de forma remota (por ejemplo, en casa o en lugares públicos).

## 3.7 Dispositivos de almacenamiento móvil

Los dispositivos móviles como tarjetas de memoria, CD, DVD y discos duros extraíbles no deben usarse a menos que estén autorizados. Cuando transfiera datos internos o confidenciales, debe usar solo dispositivos de almacenamiento móviles con licencia, administrados y propiedad de la empresa con cifrado habilitado.

## 3.8 Monitoreo y filtrado

Todos los datos creados y almacenados en las computadoras de la Compañía son propiedad de la Compañía y no existe una disposición oficial para la privacidad de los datos individuales; sin embargo, siempre que sea posible, la Compañía se abstendrá de abrir correos electrónicos personales.

El registro del sistema informático se llevará a cabo cuando corresponda y se llevarán a cabo investigaciones cuando exista una sospecha razonable de incumplimiento de esta o cualquier otra política. La Compañía tiene el derecho (sujeto a ciertas condiciones) de monitorear la actividad en sus sistemas, incluido el uso de Internet y

el correo electrónico, para garantizar la seguridad de los sistemas y el funcionamiento efectivo y para proteger contra el uso indebido.

## 3.9 Informe

Es su responsabilidad informar de inmediato las sospechas de violaciones de la política de seguridad a su línea de gestión, al departamento de TI, al departamento de seguridad de la información o al servicio de asistencia de TI.

Todas las violaciones de las políticas de seguridad de la información serán investigadas. Cuando las investigaciones revelen una conducta indebida, se pueden tomar medidas disciplinarias de acuerdo con los procedimientos disciplinarios de la Compañía.

# 4 Cumplimiento normativo

## 4.1 Medición de cumplimiento

El equipo de administración de seguridad de la información verificará el cumplimiento de esta política a través de varios métodos, incluidos, entre otros, informes de herramientas de la empresa, auditorías internas y externas y comentarios al propietario de la política.

## 4.2 Excepciones

Cualquier excepción a la política debe ser aprobada y registrada por el oficial de seguridad de la información con anticipación e informada al equipo de revisión de la gerencia.

## 4.3 Por defecto

Un empleado que haya violado esta política puede estar sujeto a medidas disciplinarias, que pueden incluir el despido.

## 4.4 Mejora continua

La política se actualiza y revisa como parte del proceso de mejora continua.

# 5 Referencia de control Anexo A

| ISO27001:2022 | ISO27002:2022 | ISO27001:2013/2017 | ISO27002:2013/2017 |
|---|---|---|---|
| ISO27001:2022 Cláusula 5 Liderazgo<br><br>ISO27001:2022 Cláusula 5.1 Liderazgo y compromiso<br><br>ISO27001:2022 Cláusula 5.2 Política<br><br>ISO27001:2022 Cláusula 6.2 Objetivos de seguridad de la información y planificación para alcanzarlos<br><br>ISO27001:2022 Cláusula 7.3 Conocimiento | ISO27002:2022 Cláusula 5 Controles organizacionales<br><br>ISO27002:2022 Cláusula 5.1 Políticas de seguridad de la información<br><br>ISO27002:2022 Cláusula 5.36 Cumplimiento de las políticas, normas y estándares de seguridad de la información<br><br>ISO27002:2022 Cláusula 5.4 Responsabilidad de la dirección<br><br>ISO27002:2022 Cláusula 6 Comprobaciones de personas | ISO27001:2013/2017 Cláusula 5 Liderazgo<br><br>ISO27001:2013/2017 Cláusula 5.1 Liderazgo y compromiso<br><br>ISO27001:2013/2017 Cláusula 5.2 Política<br><br>ISO27001:2013/2017 Cláusula 6.2 Objetivos de seguridad de la información y planificación para alcanzarlos<br><br>ISO27001:2013/2017 Cláusula 7.3 Conocimiento | ISO27002:2013/2017 Cláusula 5 Políticas de seguridad de la información<br><br>ISO27002:2013/2017 Cláusula 5.1 Dirección de la Dirección de Seguridad de la Información<br><br>ISO27002:2013/2017 Cláusula 5.1.1 Políticas de seguridad de la información<br><br>ISO27002:2013/2017 Cláusula 5.1.2 Revisión de las políticas de seguridad de la información<br><br>ISO27002:2013/2017 Cláusula 7 Seguridad de los recursos humanos |

| | | | |
|---|---|---|---|
| | ISO27002:2022 Cláusula 6.3 Concientización, educación y capacitación en seguridad de la información<br><br>ISO27002:2022 Cláusula 6.4 Proceso disciplinario<br><br>ISO27002:2022 Cláusula 5.10 Uso aceptable de la información y otros activos asociados<br><br>ISO27002:2022 Cláusula 5.14 Transferencia de información<br><br>ISO27002:2022 Cláusula 8 Controles tecnológicos<br><br>ISO27002:2022 Cláusula 8.1 Dispositivos de punto final de usuario | | ISO27002:2013/2017 Cláusula 7.2.1 Responsabilidad de la dirección<br><br>ISO27002:2013/2017 Cláusula 7.2.2 Concientización, educación y capacitación en seguridad de la información<br><br>ISO27002:2013/2017 Cláusula 7.2.3 Proceso disciplinario<br><br>ISO27002:2013/2017 Cláusula 8 Gestión de recursos<br><br>ISO27002:2013/2017 Cláusula 8.1 Responsabilidad por bienes<br><br>ISO27002:2013/2017 Cláusula 8.1.3 Uso aceptable de los bienes<br><br>ISO27002:2013/2017 Cláusula 8.2.3 Gestión de activos<br><br>ISO27002:2013/2017 Cláusula 13 Seguridad de las comunicaciones<br><br>ISO27002:2013/2017 Cláusula 13.1 Gestión de la seguridad de la red<br><br>ISO27002:2013/2017 Cláusula 13.2.1 Políticas y procedimientos de transferencia de información<br><br>ISO27002:2013/2017 Cláusula 13.2.2 Acuerdos de transferencia de información |