CiberConscientes
Creando nidos seguros en redes inseguras

POLÍTICAS

Política de Uso Aceptable

Modelo genérico y editable de Política de Uso Aceptable: las reglas de qué se puede y qué no se puede hacer con los equipos, las cuentas y la conexión de la organización. Es el complemento operativo de la Política de Seguridad de la Información, escrito en lenguaje que cualquier persona del equipo puede entender y firmar.

Versión 1.1 · Agosto 2026

> Antes de usarla
>
> Este es un modelo de base. Reemplazá los campos entre corchetes —[ORGANIZACIÓN], [RESPONSABLE], [CANAL DE REPORTE]— y ajustá los controles al tamaño y al rubro de tu empresa. Una política que copiás sin adaptar no sirve para exigir su cumplimiento.

1. Objetivo y alcance

Esta Política de Uso Aceptable (PUA) establece qué usos de los recursos tecnológicos de [ORGANIZACIÓN] están permitidos y cuáles no. Su objetivo es proteger la información, los sistemas y la reputación de la organización, y también dar claridad a las personas sobre qué se espera de ellas.

Alcance. Esta política aplica a:

- Todo el personal: empleados, socios, pasantes, personal temporal y colaboradores externos.
- Proveedores y terceros que accedan a sistemas, cuentas o información de la organización.
- Todos los recursos tecnológicos: computadoras, celulares, cuentas de correo, sistemas de gestión, servicios en la nube, conexión a internet y redes de la organización.
- Los dispositivos personales que se usen para trabajar, en la medida en que accedan a información de la organización.

2. Principio general

Los recursos tecnológicos son herramientas de trabajo provistas por la organización para cumplir funciones laborales. Se admite un uso personal ocasional y razonable, siempre que no afecte la productividad, no consuma recursos de forma desmedida, no comprometa la seguridad y no exponga a la organización a riesgos legales o de imagen.

Ante la duda sobre si un uso es aceptable, la persona debe consultar a [RESPONSABLE] antes de actuar.

3. Usos permitidos

- Utilizar los equipos, sistemas y conexiones para las tareas propias del puesto.
- Acceder a recursos de internet relacionados con el trabajo, la capacitación y la investigación profesional.
- Instalar o solicitar la instalación de software necesario para el trabajo, a través del circuito de autorización definido.

- Uso personal ocasional y moderado fuera de las tareas críticas, dentro de los límites de esta política.
- Guardar información laboral únicamente en los repositorios aprobados por la organización.

4. Usos prohibidos

Las siguientes conductas están expresamente prohibidas y pueden dar lugar a las medidas previstas en la sección 11.

Seguridad de la información

- Compartir usuarios, contraseñas, tokens o códigos de verificación con otras personas, incluidos compañeros de trabajo y personal de soporte técnico.
- Desactivar o eludir controles de seguridad: antivirus, firewall, cifrado, bloqueo de pantalla, filtros de correo o registro de actividad.
- Instalar software no autorizado, especialmente el descargado de sitios no oficiales o versiones pirateadas.
- Conectar dispositivos USB o medios extraíbles de procedencia desconocida a equipos de la organización.
- Acceder, copiar, modificar o eliminar información de otras personas o áreas sin autorización expresa.
- Intentar acceder a sistemas, cuentas o datos para los que no se tiene permiso, aun por curiosidad y aun sin causar daño.

Manejo de la información

- Enviar información confidencial de la organización, de clientes o de terceros a cuentas personales o a servicios no aprobados.
- Publicar información interna, datos de clientes, capturas de sistemas o documentación en redes sociales, foros, grupos de mensajería o herramientas de inteligencia artificial públicas.
- Almacenar información laboral en dispositivos o servicios personales sin autorización.
- Extraer bases de datos, listados de clientes o documentación al desvincularse de la organización.

Conducta y contenidos

- Utilizar los recursos para acosar, discriminar, amenazar o dañar a otras personas.
- Acceder, almacenar o distribuir contenido ilegal, violento, discriminatorio o sexual explícito.
- Usar los recursos para actividades comerciales personales ajenas a la organización.
- Suplantar la identidad de otra persona o de la organización en cualquier comunicación.
- Consumir recursos de forma desmedida: minería de criptomonedas, descargas masivas o servicios de streaming ajenos al trabajo.

> Esta lista no es exhaustiva. Que una conducta no esté enumerada no significa que esté permitida: rige el principio general de la sección 2.

5. Correo electrónico y mensajería

- La cuenta de correo provista por la organización es de uso laboral y su contenido es información de la organización.

- Verificá la identidad del remitente antes de abrir adjuntos o hacer clic en enlaces, especialmente si el mensaje transmite urgencia.
- Ninguna solicitud de transferencia, cambio de datos bancarios o envío de información sensible debe ejecutarse solo por correo o mensajería: debe verificarse por un canal distinto, previamente conocido.
- Los correos sospechosos se reportan a [CANAL DE REPORTE] sin reenviarlos a otros compañeros.
- No se deben usar cuentas personales de correo o mensajería para gestionar asuntos laborales sensibles.

6. Dispositivos y puestos de trabajo

- Los equipos deben mantener el sistema operativo y las aplicaciones actualizados. No se deben posponer las actualizaciones de seguridad indefinidamente.
- Todo equipo debe tener bloqueo de pantalla automático tras un período de inactividad (se recomienda un máximo de [5] minutos) y bloqueo manual al alejarse del puesto.
- Los equipos móviles no deben dejarse desatendidos en lugares públicos ni a la vista dentro de un vehículo.
- La pérdida o el robo de un equipo debe reportarse de inmediato, sin esperar al día siguiente.
- No se deben modificar las configuraciones de seguridad ni utilizar cuentas con privilegios de administrador para tareas cotidianas.

7. Trabajo remoto y dispositivos personales

- El acceso a sistemas internos desde fuera de la organización debe realizarse por los medios aprobados ([VPN / plataforma autorizada]).
- Evitá operar con información de la organización desde redes Wi-Fi públicas sin protección.
- Los dispositivos personales usados para trabajar deben cumplir los mismos requisitos mínimos: bloqueo de pantalla, actualizaciones al día y antivirus donde corresponda.
- La organización podrá requerir el borrado de la información corporativa de un dispositivo personal en caso de pérdida, robo o desvinculación.
- No compartas el equipo de trabajo con familiares o terceros.

8. Inteligencia artificial y servicios en la nube

El uso de herramientas de inteligencia artificial y de servicios en la nube externos puede aportar valor, pero implica que la información sale del control de la organización. Por eso:

- No se debe ingresar información confidencial, datos personales de clientes o empleados, credenciales ni código propietario en herramientas de inteligencia artificial públicas o servicios no aprobados.
- El listado de herramientas aprobadas lo mantiene [RESPONSABLE]. Para incorporar una nueva, hay que solicitarlo antes de usarla.
- Los resultados generados por estas herramientas deben revisarse antes de usarse en decisiones, comunicaciones a clientes o documentos formales.
- La responsabilidad por el contenido publicado o enviado es siempre de la persona que lo utiliza, no de la herramienta.

9. Privacidad y monitoreo

La organización puede supervisar el uso de sus recursos tecnológicos con fines de seguridad, continuidad operativa y cumplimiento normativo. Este monitoreo se realiza sobre los recursos provistos por la organización, de manera proporcional y no discriminatoria.

- Las personas alcanzadas por esta política son informadas de esta facultad y prestan conformidad al firmar el acuse de recibo.
- La información obtenida se usa exclusivamente para los fines indicados y se conserva por el plazo definido en [POLÍTICA DE RETENCIÓN].
- El tratamiento de datos personales se rige por la normativa aplicable, incluida la Ley N.° 25.326 de Protección de Datos Personales en Argentina.

> Punto sensible
>
> El monitoreo del personal tiene límites legales que varían según la jurisdicción y que se cruzan con el derecho laboral y el derecho a la intimidad. Antes de implementar cualquier control sobre la actividad de las personas, hacé revisar esta sección con asesoramiento legal.

10. Reporte de incidentes

Reportar rápido reduce el daño. No se aplicarán sanciones a quien reporte de buena fe un error propio: se busca que los problemas salgan a la luz, no que se escondan.

Qué reportar	Ejemplos
Pérdida o robo de equipos	Notebook, celular, pendrive, credencial de acceso.
Correos y mensajes sospechosos	Phishing, pedidos de transferencia, adjuntos inesperados.
Accesos indebidos	Ver información que no corresponde al rol, sesiones abiertas ajenas.
Comportamiento anómalo del equipo	Lentitud extrema, archivos cifrados, programas desconocidos.
Errores propios	Haber hecho clic en un enlace, haber enviado información al destinatario equivocado.

Canal de reporte: [CANAL DE REPORTE] · Responsable: [RESPONSABLE] · Contacto de emergencia: [TELÉFONO]

11. Cumplimiento y consecuencias

- El cumplimiento de esta política es obligatorio y forma parte de las responsabilidades de cada puesto.
- El incumplimiento puede dar lugar a medidas disciplinarias, proporcionales a la gravedad y al impacto, conforme a la normativa laboral aplicable y al reglamento interno de la organización.
- Los incumplimientos que constituyan delito podrán ser denunciados ante las autoridades competentes.
- Para proveedores y terceros, el incumplimiento puede implicar la revocación inmediata de los accesos y la revisión de la relación contractual.

12. Vigencia y revisión

- Esta política entra en vigencia el [FECHA] y debe revisarse al menos una vez al año, o ante cambios relevantes en la organización, los sistemas o el contexto de amenazas.
- La revisión la coordina [RESPONSABLE] y la aprueba [DIRECCIÓN].
- Cada persona debe firmar un acuse de recibo al incorporarse y cada vez que la política se actualice.

Versión	Fecha	Cambio	Aprobado por
1.0	[FECHA]	Versión inicial adaptada del modelo de CiberConscientes.	[NOMBRE / CARGO]

13. Acuse de recibo

Declaro haber recibido, leído y comprendido la Política de Uso Aceptable de [ORGANIZACIÓN], y me comprometo a cumplirla en el desempeño de mis funciones. Entiendo que los recursos tecnológicos que utilizo son propiedad de la organización y que su uso puede ser supervisado en los términos de la sección 9.

Nombre y apellido	DNI	Área / Puesto	Fecha	Firma

14. Reglas claras, nido ordenado

Una política que nadie leyó no protege a nadie. Cuando la adaptes, dedicale quince minutos a explicarla en una reunión de equipo: se cumple mucho más lo que se entiende que lo que solo se firma.

Esto no termina acá

Si querés enterarte de las estafas que están circulando de verdad, qué revisar y los documentos nuevos, sumate al correo de CiberConscientes. Sin vueltas y con baja en un clic. www.ciberconscientes.io

Versión 1.1 · Agosto 2026 · Próxima revisión: Agosto 2027 · www.ciberconscientes.io