POLÍTICA DE USO ACEPTABLE

PUA — Uso de Sistemas, Correo e Internet

Razón Social	**[Nombre del estudio o empresa]**
CUIT	**[CUIT del estudio]**
Versión	1.0 — Primera emisión
Fecha de emisión	**[DD/MM/AAAA]**
Próxima revisión	**[DD/MM/AAAA — recomendado: 12 meses]**
Responsable	**[Nombre y cargo del responsable de seguridad]**
Aprobado por	**[Nombre y cargo del socio/director que aprueba]**

1. Propósito

Esta política define el uso aceptable de los recursos tecnológicos de **[Nombre del estudio]**: computadoras, laptops, teléfonos, correo electrónico, internet, sistemas de software contable y cualquier otro recurso digital propiedad del estudio o administrado por este.

Su objetivo es proteger la información de los clientes, la reputación del estudio y la continuidad operativa, estableciendo reglas claras sobre qué está permitido y qué está prohibido en el uso de la tecnología en el entorno laboral.

Esta política aplica durante el horario laboral, fuera del horario cuando se utilizan recursos del estudio, y en todo momento cuando se trata de información de clientes.

2. Alcance

Esta política aplica a todas las personas que utilizan recursos tecnológicos del estudio:

- Socios, empleados en relación de dependencia y pasantes.
- Colaboradores externos y proveedores con acceso a sistemas del estudio.
- Cualquier persona que utilice dispositivos, redes o sistemas propiedad del estudio, independientemente de su ubicación física.

Los recursos tecnológicos cubiertos por esta política incluyen:

- Computadoras de escritorio, laptops y tablets propiedad del estudio.
- Teléfonos móviles provistos por el estudio.
- Cuentas de correo electrónico corporativo.
- Conexión a internet provista por el estudio, tanto en la oficina como via VPN remota.
- Software contable, fiscal y de gestión documental (sistemas de liquidación de sueldos, facturación, AFIP, etc.).
- Sistemas de almacenamiento compartido (servidores locales, nube corporativa).
- Impresoras, escáneres y dispositivos de almacenamiento externo (pendrives, discos externos).

3. Uso Aceptable — Lo que Está Permitido

Los siguientes usos son aceptables dentro del estudio:

✔	COMPUTADORAS Y SISTEMAS
✔	Utilizar los sistemas del estudio para realizar las tareas asignadas por la dirección.
✔	Acceder a los sistemas contables y fiscales (AFIP, software de liquidación, ERP) para las tareas profesionales autorizadas.
✔	Instalar software aprobado por el Responsable de Seguridad mediante solicitud formal.
✔	Guardar archivos de trabajo en las carpetas designadas de la red o nube corporativa.
✔	Uso personal ocasional y de baja intensidad del equipo (por ejemplo, revisar correo personal brevemente durante un descanso), siempre que no interfiera con el trabajo ni exponga al estudio a riesgos.

✔	CORREO ELECTRÓNICO CORPORATIVO
✔	Enviar y recibir comunicaciones profesionales con clientes, organismos (AFIP, ANSES, COMARB) y colegas.
✔	Adjuntar documentación de clientes mediante canales seguros y cifrados cuando sea necesario.
✔	Utilizar la firma corporativa aprobada por el estudio en todos los correos salientes.
✔	Comunicaciones internas entre miembros del equipo relacionadas con tareas del estudio.

✔	INTERNET
✔	Acceder a sitios web relacionados con la actividad profesional: organismos fiscales, boletín oficial, publicaciones técnicas, capacitaciones.
✔	Utilizar plataformas de videoconferencia aprobadas para reuniones con clientes (Zoom, Meet, Teams).
✔	Consultar bases de datos jurídicas y contables de referencia.
✔	Acceso a redes sociales profesionales (LinkedIn) para comunicaciones del estudio, si está autorizado.

4. Uso Inaceptable — Lo que Está Prohibido

Los siguientes usos están estrictamente prohibidos y pueden dar lugar a medidas disciplinarias:

✖	COMPUTADORAS Y SISTEMAS

✖	Instalar software no autorizado: juegos, aplicaciones de descarga de contenido, herramientas de acceso remoto no aprobadas.
✖	Desactivar o modificar el antivirus, firewall u otros controles de seguridad instalados.
✖	Acceder a sistemas o carpetas para los que no se tiene autorización expresa.
✖	Utilizar los equipos del estudio para actividades comerciales personales ajenas al estudio.
✖	Conectar dispositivos de almacenamiento externos (pendrives, discos) no autorizados por el Responsable de Seguridad.
✖	Almacenar información de clientes en dispositivos personales no gestionados por el estudio.

✖ CORREO ELECTRÓNICO

✖	Enviar información confidencial de clientes (CUITs, claves fiscales, datos patrimoniales) por correo sin cifrado ni autorización.
✖	Abrir archivos adjuntos de remitentes desconocidos sin verificación previa.
✖	Responder a solicitudes de credenciales o datos sensibles recibidas por correo (phishing).
✖	Utilizar el correo corporativo para suscripciones a sitios no relacionados con la actividad profesional.
✖	Reenviar correos con información de clientes a cuentas personales.
✖	Enviar comunicaciones que puedan ser consideradas acoso, discriminación o contenido inapropiado.

✖ INTERNET

✖	Acceder a sitios de descarga ilegal de software, música, películas o cualquier contenido protegido por derechos de autor.
✖	Visitar sitios de juegos de azar, apuestas o contenido para adultos desde los equipos del estudio.
✖	Descargar software, extensiones de navegador o archivos de fuentes no verificadas.
✖	Utilizar redes Wi-Fi públicas sin VPN para acceder a sistemas del estudio.
✖	Publicar información del estudio o de sus clientes en redes sociales sin autorización expresa de la dirección.
✖	Usar herramientas de inteligencia artificial online (ChatGPT, Gemini, etc.) para procesar datos reales de clientes.

✖	CREDENCIALES Y ACCESOS
✖	Compartir usuario y contraseña con cualquier persona, incluyendo compañeros de trabajo.
✖	Utilizar las credenciales de AFIP de un cliente para fines distintos a las tareas asignadas.
✖	Dejar sesiones abiertas en sistemas del estudio al alejarse del equipo.
✖	Utilizar la misma contraseña para sistemas del estudio que para cuentas personales.
✖	Anotar contraseñas en papeles visibles o en archivos no cifrados.

5. Uso del Correo Electrónico Corporativo

El correo electrónico corporativo es una herramienta profesional y su uso implica representar al estudio. Se establecen las siguientes reglas específicas:

5.1 Identidad y firma

- Todos los correos salientes deben incluir la firma corporativa aprobada.
- No se puede modificar el nombre del remitente de forma que induzca a confusión sobre la identidad.

Formato de firma obligatorio: [Definir el formato estándar: nombre, cargo, teléfono, dirección, logo]

5.2 Información confidencial por correo

- Nunca enviar claves fiscales de AFIP, contraseñas ni datos de acceso por correo electrónico, ni siquiera a los propios clientes.
- Para enviar documentación con datos sensibles (balances, declaraciones juradas, legajos), utilizar el canal seguro designado por el estudio.

Canal seguro aprobado para envío de documentación sensible: [Indicar: plataforma de intercambio seguro, carpeta compartida cifrada, etc.]

- Al recibir un correo sospechoso que solicita credenciales o datos urgentes, reportarlo inmediatamente al Responsable de Seguridad antes de responder.

5.3 Retención y archivo

- Los correos relacionados con clientes deben archivarse según los criterios del estudio para auditoría y trazabilidad.

Período de retención de correos: [Indicar período mínimo: recomendado 5 años para estudios contables/jurídicos]

- No eliminar correos que puedan ser relevantes en caso de disputa con un cliente o revisión fiscal.

6. Uso de Internet

El acceso a internet provisto por el estudio es una herramienta de trabajo. Su uso excesivo para fines personales reduce la productividad y puede exponer al estudio a amenazas de seguridad.

6.1 Navegación en horario laboral

- El uso de internet para fines personales debe limitarse a momentos de descanso y no puede interferir con las tareas asignadas.
- El estudio puede implementar filtros de navegación que bloqueen categorías de sitios no relacionados con la actividad profesional.

Herramienta de filtrado de navegación utilizada: [Indicar si usan filtro DNS, proxy, o si no aplica actualmente]

6.2 Inteligencia Artificial y herramientas online

- Está prohibido ingresar datos reales de clientes (nombre, CUIT, información patrimonial, declaraciones juradas) en herramientas de inteligencia artificial públicas como ChatGPT, Gemini, Copilot u otras similares.
- El uso de IA para tareas genéricas (redacción, búsqueda de normativa, ejemplos teóricos) sin datos reales de clientes puede ser aceptable con autorización del Responsable de Seguridad.

Herramientas de IA aprobadas para uso profesional: [Indicar si hay herramientas específicas aprobadas o si está todo restringido]

6.3 Redes sociales

- El acceso a redes sociales personales (Instagram, TikTok, Twitter/X) desde equipos del estudio está permitido únicamente durante momentos de descanso.
- Ningún empleado puede publicar información del estudio, de sus clientes o de sus procesos internos en redes sociales personales.
- Las comunicaciones oficiales del estudio en redes sociales son gestionadas exclusivamente por la persona designada por la dirección.

Responsable de redes sociales del estudio: [Nombre y cargo]

7. Dispositivos Móviles Corporativos

Los teléfonos y tablets provistos por el estudio están sujetos a las siguientes reglas:

- Deben estar protegidos con PIN, huella digital o contraseña en todo momento.

- No se puede instalar aplicaciones de fuentes desconocidas (solo App Store / Google Play oficial).
- La información de clientes accedida desde el dispositivo no puede ser guardada en la galería de fotos ni compartida por WhatsApp personal.
- En caso de pérdida o robo, reportarlo al Responsable de Seguridad dentro de la hora de detectado el incidente para proceder al borrado remoto.

Procedimiento de reporte de pérdida: [Teléfono/email del Responsable de Seguridad para emergencias]

- Los dispositivos corporativos no deben ser usados por familiares ni personas ajenas al estudio.

8. Monitoreo y Privacidad

⚠ **AVISO IMPORTANTE: El estudio se reserva el derecho de monitorear el uso de sus recursos tecnológicos para garantizar el cumplimiento de esta política y la protección de la información. Los empleados no tienen expectativa de privacidad en el uso de los dispositivos y sistemas del estudio.**

El monitoreo puede incluir:

- Revisión de registros de navegación web en la red del estudio.
- Auditoría de accesos a los sistemas contables y carpetas compartidas.
- Revisión de correos corporativos ante investigación de incidentes de seguridad.
- Registro de dispositivos conectados a la red del estudio.

El monitoreo se realiza con el único fin de garantizar la seguridad de la información y el cumplimiento de esta política. Los resultados son confidenciales y sólo son accesibles por el Responsable de Seguridad y la dirección del estudio.

9. Consecuencias del Incumplimiento

El incumplimiento de esta política se trata conforme al régimen disciplinario del estudio y puede derivar en las siguientes consecuencias:

Gravedad	Ejemplo	Consecuencia posible
⚠ **Leve**	Uso excesivo de redes sociales en horario laboral	Advertencia verbal y recordatorio de política

⛔ **Grave**	Instalar software no autorizado que exponga el sistema	Apercibimiento formal + restricción de privilegios de instalación
🚨 **Crítico**	Enviar datos de clientes a terceros no autorizados	Desvinculación + posible denuncia ante AAIP y acción legal

10. Revisión de la Política

Esta política se revisará anualmente o ante cambios significativos en la tecnología utilizada por el estudio, incorporación de nuevas plataformas, o incidentes que evidencien la necesidad de actualización.

Próxima revisión programada: [DD/MM/AAAA] | Responsable de la revisión: [Nombre y cargo]

Anexo A — Acuse de Recibo y Compromiso de Cumplimiento

El presente acuse de recibo debe ser completado y firmado por cada empleado al incorporarse al estudio y cada vez que la política sea actualizada. Una copia firmada debe ser conservada en el legajo del empleado.

DECLARACIÓN DE RECEPCIÓN Y COMPROMISO

Yo, **[Nombre y apellido completo]**, con DNI **[Número de DNI]**, en mi carácter de **[Cargo / Función]**, declaro que:

- He recibido, leído y comprendido la Política de Uso Aceptable de los recursos tecnológicos del estudio.
- Me comprometo a cumplir todas las disposiciones de esta política en el ejercicio de mis funciones.
- Entiendo que el incumplimiento puede dar lugar a medidas disciplinarias conforme a la gravedad de la infracción.
- Entiendo que el estudio se reserva el derecho de monitorear el uso de sus recursos tecnológicos.

Fecha: [DD/MM/AAAA]

Nombre completo del empleado	Firma y fecha
[Nombre y apellido]	**[Firma / Fecha]**

Anexo B — Listado de Tecnologías y Software Aprobados

El siguiente listado contiene el software y las plataformas autorizadas para uso en el estudio. Cualquier herramienta no incluida requiere aprobación previa del Responsable de Seguridad.

Categoría	Software / Plataforma aprobada	Observaciones
Software contable	**[Ej: Tango Gestión, Bejerman, SW Estudio]**	*Licencia vigente obligatoria*
Sistema AFIP	AFIP — Servicios web oficiales (afip.gob.ar)	*Solo acceso desde red del estudio o VPN*
Correo electrónico	**[Ej: Google Workspace, Microsoft 365, otro]**	*Solo cuentas corporativas del dominio del estudio*
Almacenamiento en nube	**[Ej: Google Drive corporativo, OneDrive, otro]**	*Exclusivamente cuentas corporativas*
Videoconferencia	**[Ej: Zoom, Google Meet, Microsoft Teams]**	*No grabar reuniones con info de clientes sin consentimiento*
Antivirus	**[Ej: Kaspersky, ESET, Windows Defender]**	*Actualización automática habilitada*
Gestor de contraseñas	**[Ej: Bitwarden Business, 1Password Teams]**	*Obligatorio para todos los empleados*
VPN	**[Indicar solución de VPN utilizada]**	*Obligatoria para trabajo remoto*
Firma digital	**[Indicar si usan token AFIP, firma digital otro organismo]**	*Custodiar dispositivo de firma*

Para solicitar la aprobación de una nueva herramienta, completar el formulario de solicitud disponible en: **[Indicar dónde está disponible el formulario: carpeta compartida, email al Responsable, etc.]**

— Fin del Documento —