

Política de ciberseguridad 2025



www.adisli.org

Elaborado por: Dirección y responsable informático Fecha: 01.10.2025	Revisado por: Grupo Motor	Aprobado última actualización: Junta Directiva 23/10/2025	Edición 1
---	--	--	--------------------------------

Cuando se modifique el procedimiento, avanzará secuencialmente el estado de edición del documento, actualizándose también la fecha del mismo.

Dichos cambios se detallarán en la siguiente tabla:

FECHA	MOTIVO DE MODIFICACIÓN	APARTADO MODIFICADO	EDICIÓN
01/10/2025	Creación del documento		1

Política de Ciberseguridad de Adisli

La presente Política de Ciberseguridad tiene como objetivo establecer un marco de actuación que proteja la información de Adisli, de las personas usuarias, sus familias, el personal y los proveedores. En un entorno en el que toda la entidad trabaja con herramientas digitales de Google (Gmail, Drive, Docs, Calendar), y cada profesional dispone de un portátil de uso personal y de un móvil profesional, resulta fundamental contar con medidas claras que garanticen la seguridad y la continuidad de las actividades.

1. Objetivo

El objetivo de esta política es proteger la información y los sistemas de Adisli, garantizar la confianza de las familias y cumplir con las normativas vigentes en materia de seguridad de la información y protección de datos (RGPD y LOPDGDD).

- Asegurar la confidencialidad, integridad y disponibilidad de la información.
- Reducir la probabilidad de incidentes de ciberseguridad.
- Cumplir con los requisitos legales y éticos en el tratamiento de datos sensibles.

2. Alcance

Esta política aplica a todo el personal de Adisli, voluntariado, colaboradores y proveedores que tengan acceso a los sistemas y datos de la organización. Incluye el uso de portátiles de uso personal, móviles profesionales, acceso a la nube corporativa de Google y a las redes internas.

- Aplicación al conjunto de la plantilla y voluntariado.
- Aplicación a todos los dispositivos utilizados en el desempeño profesional.
- Aplicación a proveedores que gestionen datos o sistemas de Adisli.

3. Principios Generales

La ciberseguridad de Adisli se fundamenta en tres principios esenciales, reconocidos a nivel internacional:

- Confidencialidad: solo las personas autorizadas pueden acceder a los datos.
- Integridad: la información debe mantenerse completa, exacta y no ser alterada sin autorización.
- Disponibilidad: los sistemas y la información deben estar accesibles siempre que se necesiten.

4. Normas de Seguridad

Las normas de seguridad recogen las prácticas que cada persona de la organización debe cumplir en el uso de equipos, dispositivos móviles y servicios digitales.

- Uso de contraseñas seguras y cambio periódico. Recomendación de autenticación multifactor en el acceso a cuentas de Google.
- Bloqueo de pantalla en dispositivos y uso de antivirus actualizado en portátiles.
- Uso responsable del correo electrónico: comprobar remitentes, no abrir adjuntos sospechosos y denunciar intentos de phishing.
- Almacenamiento seguro: todos los datos sensibles se guardan en Google Drive corporativo, evitando guardar información en ordenadores locales o dispositivos externos.
- Prohibición de memorias USB no verificadas.
- Uso de redes Wi-Fi seguras, evitando redes públicas o no protegidas.

5. Gestión de Información de Familias y Usuarios

Las familias y personas usuarias comparten información confidencial a través del correo electrónico. Para proteger estos datos, Adisli establece reglas específicas de custodia:

- Toda la información recibida se almacena exclusivamente en Google Drive corporativo bajo cuentas profesionales.
- Está prohibido guardar datos de familias en dispositivos personales.
- Se garantiza que el acceso a esta información queda restringido únicamente a las personas autorizadas.
- El servicio de mantenimiento informático supervisa las copias de seguridad en la nube.

6. Roles y Responsabilidades

La protección de la información es responsabilidad de toda la organización, aunque existen funciones específicas:

- La Dirección aprueba y revisa esta política y asegura los recursos necesarios.
- Se designa a un Responsable de Ciberseguridad que coordina la implementación y seguimiento: Israel Carbonero Martínez.
- El proveedor externo de mantenimiento informático supervisa las copias de seguridad y el soporte técnico.
- Cada miembro de la plantilla es responsable de cumplir las normas y de informar de posibles incidentes.

7. Formación y Concienciación

La formación es clave para que la plantilla entienda los riesgos y adopte buenas prácticas.

- Adisli organiza sesiones periódicas de formación en ciberseguridad (uso seguro de correo, gestión de contraseñas, prevención de phishing).
- Se refuerza la concienciación mediante comunicaciones internas y recordatorios periódicos.
- Se promueve la cultura de la seguridad como parte integral de la actividad de Adisli.

8. Cumplimiento Normativo

El cumplimiento normativo garantiza que Adisli protege adecuadamente la información y responde a exigencias legales.

- Cumplimiento con el RGPD y la LOPDGDD.
- Inclusión de cláusulas contractuales de seguridad en los acuerdos con proveedores.
- Alineación con buenas prácticas internacionales de seguridad.

9. Revisión y Mejora Continua

La ciberseguridad es un ámbito en constante evolución. Esta política debe revisarse con regularidad.

- Revisión anual de la política y actualización en caso de cambios normativos.
- Incorporación de lecciones aprendidas tras incidentes o simulacros.
- Evaluación de nuevas amenazas y adaptación de medidas.