

 Azahara de Comunicaciones	POLÍTICA DE USO ACEPTABLE DE ACTIVOS DE LA INFORMACIÓN	ANEXO XIII. REVISIÓN 00 08/04/2025
--	---	--

OBJETIVO

Establecer las normas para el uso seguro de los activos de información (equipos, redes, software y soportes) con el fin de proteger la confidencialidad, integridad y disponibilidad de los datos de la empresa y sus clientes.

NORMAS GENERALES

Uso de Equipos Corporativos

- Los dispositivos proporcionados por la empresa (ordenadores, móviles, tablets) deben utilizarse exclusivamente para fines profesionales.
- Prohibido instalar software no autorizado por el departamento de TI.
- Obligatorio utilizar antivirus corporativo y mantener los sistemas actualizados.

Redes y Conectividad

- La red Wi-Fi corporativa es de uso interno. Los invitados deben acceder a la red de visitantes con credenciales temporales.
- Prohibido el uso de VPN personales o herramientas de acceso remoto no autorizadas.

Soportes Extraíbles y Almacenamiento

- Solo se permiten dispositivos USB/disco duro autorizados.
- Prohibido conectar soportes de origen desconocido sin escaneo previo de malware.

Correo Electrónico y Comunicaciones

- Reportar inmediatamente correos sospechosos (phishing) al responsable de TI.

Teletrabajo

- Herramientas de acceso remoto autorizadas.
- Los equipos personales deben cumplir la Política BYOD (antivirus, cortafuegos activo).

CLASIFICACIÓN DE LA INFORMACIÓN

- Público: Puede compartirse sin restricciones (ej.: folletos comerciales).
- Interno: Solo para empleados (ej.: manuales de procesos).
- Confidencial: Requiere autorización explícita (ej.: contratos de clientes, proyectos no publicados).

PROHIBICIONES EXPLÍCITAS

- Compartir credenciales de acceso.
- Almacenar información confidencial en servicios cloud no autorizados (Dropbox, WeTransfer).
- Acceder a sitios web de alto riesgo (apuestas, pornografía, descargas P2P).



Azahara de
Comunicaciones

POLÍTICA DE USO ACEPTABLE DE ACTIVOS DE LA INFORMACIÓN

ANEXO XIII.
REVISIÓN 00
08/04/2025

RESPONSABILIDADES

- Empleados: Cumplir las normas y reportar incidencias.
- Departamento de TI: Supervisar el cumplimiento y bloquear accesos no autorizados.
- Dirección: Aprobar excepciones justificadas.

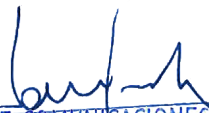
SANCIONES

El incumplimiento puede derivar en:

- Amonestación escrita.
- Retirada de privilegios de acceso.
- Acciones legales en casos graves (pérdida de datos o fraude).

En Huelva, a 8 de Abril de 2025

José Suárez Mora- Presidente



AZAHARA DE COMUNICACIONES, S.A.
P.P.