					Introduzca aquí la denominación de la entidad jurídica registrada							
Número de documento: P03					Título del documento: **Política de Uso Aceptable**							
Versión: 1.0		Fecha de entrada en vigor: 01.01.2025			Propietario del documento:							
X	Política		Norma		Procedimiento		Formulario		Registro		Otro	

Historial de revisiones				
Número de revisión	**Fecha de revisión**	**Cambios**	**Revisado por**	**Propietario del proceso**

Aprobaciones			
Nombre	**Cargo**	**Fecha**	**Firma**

Alineación con normas y regulaciones

Norma/Regulación	Cláusula/Artículo	Comentario
ISO/IEC 27001:2022	Cláusula 5	Establece normas de comportamiento y requisitos aplicables a la Política de Uso Aceptable
ISO/IEC 27002:2022	Controles 6.1, 6.2, 8.1, 8.12	Orienta las responsabilidades en seguridad de la información, la concienciación y la gobernanza de dispositivos y datos
NIST SP 800-53 Rev. 5	AC-19, AC-20, AT-2	Controles de acceso y de concienciación/normas de comportamiento relevantes para el uso de activos de TI
RGPD de la UE	Artículos 5.1.f), 32; considerando 39	Exige confidencialidad e integridad, impone controles técnicos y organizativos, y bases jurídicas para el uso adecuado
Directiva NIS2 de la UE	Artículo 21.2.a)-d)	Exige políticas operativas y formación sobre uso seguro
DORA de la UE	Artículo 5	Refuerza la gestión del riesgo de las TIC mediante la regulación del comportamiento de los usuarios
COBIT 2019	APO07, BAI05, DSS05, MEA01	Recursos humanos, gestión del cambio, gestión de la seguridad y supervisión del cumplimiento y del rendimiento

1. Propósito

1.1 Esta política define el uso aceptable y no aceptable de los sistemas de información, los recursos informáticos, las herramientas de comunicación y las prácticas de tratamiento de datos de la organización.

1.2 Garantiza que todos los usuarios comprendan sus responsabilidades al utilizar los activos de TI corporativos y que sus acciones respalden la confidencialidad, integridad, disponibilidad y el tratamiento lícito de la información.

1.3 La política da cumplimiento a la cláusula 5.10 de ISO/IEC 27001:2022 al establecer normas de comportamiento para el uso de los sistemas e implantar salvaguardas técnicas y procedimentales para minimizar el riesgo de uso indebido, negligencia o abuso.

1.4 Asimismo, respalda las actividades de investigación y ejecución de medidas, incluida la respuesta a incidentes y la adopción de medidas disciplinarias por incumplimiento.

2. Alcance

2.1 Esta política aplica a todas las personas y entidades a las que se les conceda acceso a los sistemas de información y activos de la organización, incluidas, entre otras:

2.1.1 Empleados, contratistas, consultores, becarios y personal de empresas de trabajo temporal

2.1.2 Proveedores externos con acceso a sistemas o funciones administrativas delegadas

2.1.3 Invitados o socios que utilicen infraestructura de TI propiedad de la organización o autorizada por esta

2.2 El alcance incluye todos los activos tecnológicos y de datos de la organización, incluidos:

2.2.1 Estaciones de trabajo, equipos portátiles, dispositivos móviles y servidores

2.2.2 Infraestructura de red y servicios alojados en la nube

2.2.3 Correo electrónico, mensajería, almacenamiento de archivos, plataformas de colaboración y VPN

2.2.4 Datos en reposo, en tránsito o en tratamiento, con independencia de su formato o ubicación

2.2.5 Cualquier dispositivo personal utilizado en el marco de un esquema BYOD que se conecte a los sistemas de la organización

2.3 Esta política es de obligado cumplimiento en todos los entornos de trabajo, incluidos:

2.3.1 Oficinas corporativas y centros de producción

2.3.2 Ubicaciones de trabajo en remoto o esquemas híbridos

2.3.3 Operaciones sobre el terreno o instalaciones gestionadas por terceros

2.4 Todos los usuarios deben reconocer y cumplir esta política como condición para acceder a los sistemas de la organización o tratar datos corporativos.

3. Objetivos

3.1 Definir y hacer cumplir las reglas para el uso aceptable de los recursos de TI de la organización.

3.2 Prevenir accesos no autorizados, fugas de datos o daños derivados de un uso negligente o malicioso.

3.3 Proteger las redes, los activos y los datos de la organización frente a amenazas introducidas a través del comportamiento de los usuarios.

3.4 Respaldar las obligaciones legales y contractuales demostrando diligencia debida en la gobernanza de los recursos de TI.

3.5 Garantizar coherencia y claridad en la aplicación de medidas disciplinarias y en los procesos de gestión de excepciones.

3.6 Promover una cultura de uso ético, seguro y responsable de los recursos informáticos, tanto digitales como físicos.

4. Funciones y responsabilidades

4.1 Dirección

4.1.1 Aprueba la Política de Uso Aceptable (AUP) y garantiza su alineación con los objetivos del negocio, los requisitos regulatorios y los valores de la organización.

4.1.2 Asigna recursos para la aplicación, la formación, la supervisión y la revisión de la política.

4.1.3 Revisa el estado de cumplimiento y las medidas disciplinarias asociadas a incumplimientos de la política como parte de la gobernanza del SGSI.

4.2 Equipos de TI y de Seguridad de la Información

4.2.1 Implantan salvaguardas técnicas para hacer cumplir esta política, incluidas:

4.2.2 Herramientas de filtrado de contenidos, protección contra malware, seguridad de endpoints y monitorización de red

4.2.3 Configuraciones de seguridad del correo electrónico y soluciones de prevención de pérdida de datos (DLP)

4.2.4 Listas de bloqueo y listas de permitidos para software, hardware y sitios web

4.2.5 Mantienen un inventario de software, dispositivos y servicios aprobados y prohibidos.

4.2.6 Investigan presuntos incumplimientos de la AUP, recopilan evidencias forenses y respaldan medidas disciplinarias o acciones legales cuando corresponda.

4.2.7 Colaboran con Recursos Humanos y Asesoría Jurídica en la gestión de incidentes, la escalada y las obligaciones de notificación.

[... Las secciones 4.3–8 no están incluidas en esta vista previa. Adquiera el documento completo para acceder al contenido íntegro. ...]

9. Requisitos de revisión y actualización

9.1 Desencadenantes y frecuencia de revisión

9.1.1 Esta política debe revisarse:

9.1.1.1 Al menos una vez al año

9.1.1.2 Tras cualquier cambio significativo en la tecnología o la infraestructura

9.1.1.3 Después de incidentes o hallazgos de auditoría que pongan de manifiesto deficiencias en la aplicación

9.1.1.4 En respuesta a cambios en la legislación o en los contratos aplicables

9.2 Titularidad y aprobación

9.2.1 El CISO o el Responsable del SGSI designado es responsable del proceso de revisión.

9.2.2 Las actualizaciones deben ser aprobadas por la Dirección y comunicadas a toda la organización.

9.2.3 El reconocimiento de los términos actualizados debe recabarse nuevamente cuando se vuelva a emitir la política.

9.3 Gestión documental

9.3.1 La política debe incluir los siguientes metadatos y datos de versionado:

9.3.1.1 Título, identificador y nivel de clasificación

9.3.1.2 Propietario de la política y responsable de custodia del documento

9.3.1.3 Historial de cambios y justificación de las actualizaciones

9.3.1.4 Fechas de revisión y de la próxima actualización programada

9.3.1.5 Referencias al registro de distribución y de reconocimientos

9.3.2 La copia maestra se conservará en el Repositorio Documental del SGSI bajo control de versiones.

10. Políticas relacionadas y vinculaciones

10.1 Esta política debe interpretarse conjuntamente con las siguientes:

10.1.1 P1 – Política de Seguridad de la Información: Establece las expectativas básicas de comportamiento y el compromiso de la alta dirección con el uso aceptable.

10.1.2 P4 – Política de Control de Acceso: Define los permisos y derechos asociados a usuarios, sistemas y acceso a datos, aplicando directamente los límites del uso aceptable.

10.1.3 P6 – Política de Gestión de Riesgos: Aborda los riesgos relacionados con el comportamiento y respalda las actividades de supervisión y tratamiento asociadas a amenazas originadas por los usuarios.

10.1.4 P7 – Política de Incorporación y Baja: Garantiza que los términos de uso aceptable se reconozcan al incorporarse y se revoquen al finalizar la relación.

10.1.5 P9 – Política de Trabajo en Remoto: Amplía las disposiciones de uso aceptable a los entornos de trabajo en remoto e híbrido.

10.2 Estas políticas relacionadas conforman un modelo de defensa en profundidad para la gobernanza del comportamiento, la tecnología y los aspectos contractuales.

11. Normas y marcos de referencia

11.1 Esta Política de Uso Aceptable (AUP) está alineada con normas reconocidas internacionalmente y marcos jurídicos para garantizar controles de comportamiento exigibles, auditables y basados en el riesgo en todo uso digital y físico de los sistemas de información.

11.2 ISO/IEC 27001:2022

11.2.1 Cláusula 5.10 – Uso aceptable de la información y otros activos asociados: Esta política cumple directamente el requisito de definir, comunicar y hacer cumplir reglas que regulen el uso adecuado de los recursos de TI.

11.2.2 Anexo A, control 6.1 – Responsabilidades en seguridad de la información: Asigna responsabilidades claras respecto del comportamiento de los usuarios y la supervisión del cumplimiento.

11.2.3 Anexo A, control 6.2 – Concienciación, educación y formación en seguridad de la información: Los procesos de formación integrada y reconocimiento de la política forman parte de la aplicación de la AUP.

11.2.4 Anexo A, control 8.1 – Dispositivos endpoint del usuario, y control 8.12 – Prevención de pérdida de datos: Aborda el comportamiento aceptable en dispositivos de usuario y regula actividades que podrían dar lugar a exposición o fuga de datos.

11.3 NIST SP 800-53 Rev. 5:

11.3.1 AC-19 (Control de acceso para dispositivos móviles) y AC-20 (Uso de sistemas de información externos): Esta política define obligaciones y restricciones de los usuarios para BYOD y acceso a sistemas de terceros.

11.3.2 PL-4 (Normas de comportamiento): Establece requisitos detallados de uso aceptable coherentes con esta política.

11.3.3 AT-2 (Formación de concienciación en seguridad): Se respalda mediante formación a usuarios y reconocimiento documentado de la política.

11.3.4 AU-2 (Eventos de auditoría) y AU-12 (Generación de registros de auditoría): La aplicación se basa en la supervisión de las acciones de los usuarios y en la generación de alertas sobre incumplimientos.

11.4 RGPD de la UE (2016/679):

11.4.1 Artículo 5.1.f): Exige la seguridad e integridad de los datos personales; esta política mitiga riesgos introducidos por el comportamiento humano y el uso no autorizado.

11.4.2 Artículo 32: Exige medidas técnicas y organizativas, como controles de comportamiento y restricciones de uso, para proteger los datos personales.

11.4.3 Considerando 39: Destaca la necesidad de garantizar que solo las personas autorizadas tengan el acceso necesario y hagan un uso lícito de los datos.

11.5 Directiva NIS2 de la UE (2022/2555):

11.5.1 Artículo 21.2.a)-d): Exige políticas operativas y formación para el uso seguro de los sistemas, lo que esta AUP proporciona al definir comportamiento, supervisión y procesos de aplicación.

11.6 DORA de la UE (2022/2554):

11.6.1 Artículo 5: Esta política respalda el marco de gestión del riesgo de las TIC al definir reglas para la interacción entre personas y sistemas y minimizar la exposición al ciberriesgo basado en el comportamiento.

11.7 COBIT 2019:

11.7.1 APO07 – Gestión de recursos humanos: Refuerza las responsabilidades de los usuarios y la concienciación a lo largo del ciclo de vida del empleado.

11.7.2 BAI05 – Gestión del cambio organizativo: Integra la gobernanza del uso aceptable en los procesos de cambio que afectan al comportamiento de los usuarios.

11.7.3 DSS05 – Gestión de servicios de seguridad: Respalda la supervisión de actividades de usuarios, las alertas de comportamiento y los mecanismos de respuesta automatizada.

11.7.4 MEA01 – Supervisar, evaluar y valorar el rendimiento y la conformidad: La política define métricas y mecanismos para validar el cumplimiento por parte de los usuarios de las expectativas de comportamiento.