					Introduzca aquí la denominación de la entidad jurídica registrada							
Número de documento: P09S					Título del documento: **Política de Trabajo Remoto**							
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**

Alineada con normas y reglamentos

Norma/Reglamento	Cláusula/Artículo	Comentario
ISO/IEC 27001:2022	Cláusulas 6.1, 6.2, 8	
ISO/IEC 27002:2022	Control 6	
NIST SP 800-53 Rev.5	AC-17, AC-2	
Directiva NIS2 de la UE	Artículos 21(2)(b), 21(2)(h)	Directiva NIS2 de la UE
DORA de la UE	Artículo 9	DORA de la UE
COBIT 2019	DSS05, APO13	COBIT 2019
RGPD de la UE	Artículo 32	RGPD de la UE

1. Propósito

1.1 Esta política establece los requisitos de seguridad aplicables a empleados y contratistas que trabajen en modalidad remota, incluido el trabajo desde el domicilio, espacios de trabajo compartidos o durante desplazamientos.

1.2 Su objetivo es proteger la confidencialidad, integridad y disponibilidad de la información de la organización a la que se acceda fuera de entornos controlados por la empresa.

1.3 Esta política asegura el cumplimiento de normas internacionales y reduce riesgos como el acceso no autorizado, la pérdida de datos y la interrupción del servicio.

2. Alcance

2.1 Esta política se aplica a todos los miembros del personal (empleados, contratistas, consultores y trabajadores temporales) que accedan a sistemas, redes o datos de la empresa mientras trabajen fuera de las instalaciones.

2.2 Abarca:

2.2.1 El uso de dispositivos proporcionados por la empresa y de dispositivos personales

2.2.2 El acceso mediante VPN, escritorio remoto o servicios en la nube

2.2.3 La gestión segura de la información fuera de las instalaciones de la empresa

2.2.4 La supervisión, la gestión de excepciones y las medidas de cumplimiento

2.3 Se aplica tanto a modalidades de trabajo remoto a tiempo completo como parcial, incluido el acceso remoto ad hoc.

3. Objetivos

3.1 Prevenir el acceso no autorizado a los sistemas de la empresa o a datos sensibles durante el trabajo remoto.

3.2 Garantizar que los dispositivos y enlaces de comunicación utilizados fuera de la oficina cumplan los requisitos mínimos de seguridad.

3.3 Mantener el control sobre los privilegios de acceso remoto y su supervisión.

3.4 Proporcionar directrices claras a empleados y responsables para unas prácticas seguras de trabajo remoto.

3.5 Cumplir las expectativas de ISO, NIS2, RGPD, DORA y COBIT en materia de trabajo remoto y movilidad.

4. Funciones y responsabilidades

4.1 Director General

4.1.1 Aprueba las modalidades de trabajo remoto y supervisa el cumplimiento.

4.1.2 Escala los incidentes de seguridad o los incumplimientos reiterados.

4.1.3 Revisa las excepciones y garantiza el seguimiento de los incidentes.

4.2 Soporte de TI o proveedor externo de TI

4.2.1 Configura el acceso remoto seguro (p. ej., VPN, MFA, gestión de dispositivos móviles).

4.2.2 Aplica controles de seguridad de endpoints, cifrado y configuraciones seguras en los dispositivos.

4.2.3 Presta soporte a los usuarios e investiga cualquier incidencia técnica de seguridad.

[... 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 Revisión anual de la política

9.1.1 El Director General y Soporte de TI deben revisar esta política al menos una vez al año para alinearla con los cambios tecnológicos, laborales y regulatorios.

9.2 Desencadenantes de actualización anticipada

9.2.1 Se requiere una revisión inmediata tras:

9.2.1.1 Un incidente grave de seguridad relacionado con el trabajo remoto

9.2.1.2 Cambios en los requisitos de NIS2, RGPD o DORA

9.2.1.3 La transición a una nueva tecnología de acceso remoto (p. ej., una plataforma VPN diferente)

9.3 Control de versiones y archivo

9.3.1 Todas las versiones de esta política deben:

9.3.1.1 Estar fechadas y aprobadas por el Director General

9.3.1.2 Tener un número de versión

9.3.1.3 Archivarse durante al menos tres años

9.4 Comunicación al personal

9.4.1 Las actualizaciones de la política deben comunicarse a todos los usuarios remotos. Se requiere acuse de recibo de la política para cualquier cambio significativo.

10. Políticas relacionadas y vinculaciones

10.1 Esta política se vincula con las siguientes y les da soporte:

10.1.1 P2S – Política de funciones y responsabilidades de gobernanza: define quién autoriza y supervisa el acceso remoto

10.1.2 P4S – Política de control de acceso: establece la configuración segura del acceso remoto y los procedimientos de revocación

10.1.3 P6S – Política de gestión de riesgos: realiza el seguimiento y la evaluación de los riesgos relacionados con el acceso fuera de las instalaciones

10.1.4 P8S – Política de concienciación y formación en seguridad de la información: forma a los usuarios sobre los riesgos del trabajo remoto y las buenas prácticas

10.1.5 P30S – Política de respuesta a incidentes: gestiona la respuesta a incidentes de acceso remoto, como filtraciones de credenciales o pérdida de dispositivos

11. Normas y marcos de referencia

11.1 ISO/IEC 27001

11.1.1 Cláusula 6.1 – Planificación basada en riesgos para escenarios de acceso remoto

11.1.2 Cláusula 6.2 – Aborda las responsabilidades de recursos humanos en contextos móviles o remotos

11.1.3 Cláusula 8.1 – Planificación y control operacional de procesos remotos

11.2 ISO/IEC 27002

11.2.1 Control 6.7 – Proporciona orientación práctica sobre seguridad para el trabajo remoto y móvil

11.3 NIST SP 800-53 Rev.5

11.3.1 AC-17 – Control de acceso remoto, protecciones de sesión y monitorización de seguridad

11.3.2 AC-2 – Control de cuentas para usuarios fuera de las instalaciones

11.4 RGPD de la UE

11.4.1 Artículo 32 – Exige protección de datos «desde el diseño y por defecto», también en entornos remotos

11.5 Directiva NIS2 de la UE

11.5.1 Artículo 21(2)(b) – Exige un uso seguro de los sistemas de redes y de información

11.5.2 Artículo 21(2)(h) – Exige medidas de seguridad relacionadas con recursos humanos, incluidos controles fuera de las instalaciones

11.6 DORA de la UE

11.6.1 Artículo 9 – Exige que las entidades financieras mantengan la resiliencia de las TIC en todos los modos operativos, incluido el acceso remoto

11.7 COBIT 2019

11.7.1 DSS05 – Gestionar los servicios de seguridad: incluye protección de endpoints y prácticas seguras de trabajo remoto

11.7.2 APO13 – Seguridad gestionada: garantiza el aprovisionamiento seguro y la supervisión de riesgos del acceso móvil y remoto