					Introduzca aquí la denominación de la entidad jurídica registrada							
Número de documento: P09					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**

1. Propósito

1.1 Esta política establece los requisitos obligatorios para realizar trabajo remoto de forma segura, incluido el uso de los sistemas de la organización, el acceso a los datos y la ejecución de las funciones laborales fuera de las instalaciones corporativas.

1.2 Garantiza la confidencialidad, integridad y disponibilidad de los activos de información a los que se accede de forma remota y establece controles para mitigar los riesgos asociados a entornos de trabajo distribuidos.

1.3 La política da cumplimiento al control 6.7 del anexo A de ISO/IEC 27001:2022 mediante la implantación de salvaguardas técnicas y procedimentales adaptadas a las condiciones del trabajo remoto.

2. Alcance

2.1 Esta política se aplica a todo el personal autorizado para trabajar en remoto, incluido:

2.1.1 Empleados (a tiempo completo, a tiempo parcial y contratados)

2.1.2 Proveedores de servicios externos, consultores y terceros

2.1.3 Personal temporal y asignado a proyectos con acceso remoto aprobado (VPN, gestión de dispositivos móviles)

2.2 Abarca:

2.2.1 El acceso a los sistemas de la organización mediante VPN o herramientas remotas aprobadas

2.2.2 El manejo de datos sensibles y regulados fuera de instalaciones seguras

2.2.3 El uso de equipos propiedad de la organización o de dispositivos personales autorizados (BYOD)

2.2.4 Las protecciones físicas y lógicas en entornos remotos

2.3 La política se aplica en todas las ubicaciones geográficas y zonas horarias en las que la organización permita el trabajo remoto, ya sea de forma habitual, puntual o durante eventos de continuidad del negocio.

3. Objetivos

3.1 Garantizar que solo las personas autorizadas puedan acceder de forma remota a los sistemas internos y a la información.

3.2 Aplicar cifrado, autenticación multifactor y protecciones de endpoint en todas las vías de acceso remoto.

3.3 Mantener una postura de seguridad frente a amenazas como phishing, software malicioso, exfiltración de datos y exposición no autorizada de sistemas.

3.4 Regular cómo se transmiten, almacenan o imprimen los datos sensibles en entornos externos a las instalaciones corporativas.

3.5 Integrar medidas de seguridad física que reduzcan la visibilidad y la observación no autorizada durante las sesiones remotas.

3.6 Cumplir los requisitos reglamentarios internacionales relativos al acceso remoto a datos, incluidos el RGPD de la UE, la Directiva NIS2 de la UE y DORA de la UE.

4. Funciones y responsabilidades

4.1 Alta Dirección

4.1.1 Aprueba esta política y garantiza que disponga de recursos suficientes y que esté integrada en las operaciones de Recursos Humanos, TI y seguridad.

4.1.2 Autoriza los criterios de elegibilidad para el trabajo remoto y su aplicabilidad por unidad de negocio.

4.2 Director de Seguridad de la Información / Responsable del SGSI

4.2.1 Es responsable de la política, la mantiene y garantiza su alineación con la postura de riesgo y los requisitos reglamentarios.

4.2.2 Define los controles de seguridad para el acceso remoto (por ejemplo, cifrado, protección de endpoint y tiempos de espera de sesión).

4.2.3 Aprueba la gestión de excepciones y supervisa la eficacia de los controles.

[... 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 Frecuencia de revisión

9.1.1 Esta política debe revisarse anualmente, o con mayor frecuencia en caso de:

9.1.1.1 Introducción de nuevas tecnologías de acceso remoto

9.1.1.2 Expansión significativa del trabajo remoto (por ejemplo, iniciativas de trabajo híbrido)

9.1.1.3 Aparición de nuevas amenazas, vulnerabilidades o incidentes vinculados a entornos remotos

9.1.1.4 Cambios en los marcos legales o reglamentarios aplicables

9.2 Titularidad y proceso de revisión

9.2.1 El propietario de la política es el Director de Seguridad de la Información. La revisión debe coordinarse con:

9.2.1.1 Operaciones y Arquitectura de TI

9.2.1.2 Recursos Humanos e Instalaciones (por sus implicaciones operativas y sobre los espacios de trabajo)

9.2.1.3 Delegado de Protección de Datos (por la privacidad y los controles sobre datos transfronterizos)

9.2.2 Las actualizaciones de la política deben:

9.2.2.1 Ser aprobadas por el Comité Directivo de Seguridad de la Información

9.2.2.2 Comunicarse a todo el personal y contratistas afectados

9.2.2.3 Integrarse en los materiales de incorporación y formación de reciclaje

9.3 Control documental y distribución

9.3.1 La política debe incluir control de versiones, fecha de entrada en vigor e historial de cambios.

9.3.2 Las versiones sustituidas deben conservarse conforme a la Política de Gestión Documental (P14).

9.3.3 Las versiones revisadas deben activar la obligatoriedad de un nuevo acuse de recibo para los usuarios elegibles para trabajo remoto.

10. Políticas relacionadas y vinculaciones

10.1 Esta política opera conjuntamente con:

10.1.1 P1 – Política de Seguridad de la Información: Establece la base para el manejo seguro de activos, aplicable a todos los entornos de trabajo, incluido el remoto.

10.1.2 P3 – Política de Uso Aceptable: Regula el uso adecuado de los dispositivos y sistemas de la organización durante las sesiones de trabajo remoto.

10.1.3 P4 – Política de Control de Acceso: Garantiza que los privilegios de acceso remoto sigan el principio de mínimo privilegio y mecanismos adecuados de autenticación.

10.1.4 P6 – Política de Gestión de Riesgos: Define cómo se identifican, tratan y supervisan los riesgos del trabajo remoto dentro del SGSI.

10.1.5 P12 – Política de Gestión de Activos: Exige inventario y gestión de configuraciones para todos los dispositivos utilizados en remoto.

10.1.6 P22 – Política de Registro de Eventos y Supervisión: Garantiza que las sesiones remotas se supervisen, auditen y conserven conforme a los requisitos de cumplimiento.

10.1.7 P14 – Política de Conservación y Eliminación de Datos: Define reglas de manejo de datos relevantes para el trabajo remoto, incluidos los medios extraíbles y la retirada de dispositivos.

10.2 Estas políticas garantizan de forma conjunta que el trabajo remoto sea seguro, conforme y aplicable en todas las funciones y ubicaciones geográficas.

11. Normas y marcos de referencia

11.1 Esta política se alinea con marcos reconocidos internacionalmente en materia de seguridad, protección de datos y gestión del riesgo de las TIC para garantizar prácticas de trabajo remoto seguras, trazables y conformes.

11.2 ISO/IEC 27001

11.2.1 Cláusula 6.1.3 – Planificación del tratamiento de riesgos: Esta política contribuye al tratamiento de los riesgos asociados al acceso remoto y a los entornos de trabajo distribuidos.

11.2.2 Cláusula 8.1 – Planificación y control operacional: Exige la implantación de controles para los sistemas a los que se accede fuera de las instalaciones de la organización.

11.2.3 Control 6.7 del anexo A – Trabajo remoto: Esta política aborda plenamente los controles exigidos para la seguridad de la información cuando el personal trabaja fuera de las instalaciones de la organización, incluidas las protecciones físicas y lógicas, la gobernanza del acceso y la supervisión del comportamiento de los usuarios.

11.3 ISO/IEC 27002:2022 – Control 6

11.3.1 Este control exige salvaguardas procedimentales y técnicas para el trabajo remoto. Incluye requisitos de seguridad de los dispositivos, métodos de acceso, manejo de datos, salvaguardas del entorno y gestión de terceros, todos ellos aplicados mediante esta política.

11.4 NIST SP 800-53 Rev.5

11.4.1 AC-17 (Acceso remoto): Respaldado directamente mediante controles de VPN, autenticación multifactor, registro de sesiones y autorización de acceso basada en roles para usuarios remotos.

11.4.2 AC-2 (Gestión de cuentas): Controla la elegibilidad de acceso, la asignación de privilegios remotos y la desactivación de cuentas.

11.4.3 SC-12 a SC-13 (Protección criptográfica, establecimiento de claves criptográficas): Implantados mediante el uso obligatorio de VPN y cifrado completo de disco para endpoints remotos.

11.4.4 MP-5 (Protección del transporte de soportes) y PE-18 (Ubicación de componentes del sistema de información): Las directrices de trabajo remoto exigen protección en el transporte y salvaguardas físicas en entornos fuera de las instalaciones.

11.4.5 AU-2, AU-6: El registro de eventos y la supervisión de sesiones remotas respaldan los requisitos de auditoría y respuesta ante incidentes.

11.5 RGPD de la UE (2016/679)

11.5.1 Artículo 32 – Seguridad del tratamiento: Esta política aplica controles de seguridad de acceso remoto, cifrado y registro de eventos necesarios para proteger los datos personales a los que se accede o que se tratan de forma remota.

11.5.2 Artículo 5(1)(f): Garantiza que los datos personales a los que se accede fuera de las instalaciones estén protegidos frente al tratamiento no autorizado o ilícito y frente a su pérdida accidental.

11.5.3 Considerando 39: Hace hincapié en la limitación del acceso, la integridad y la confidencialidad, especialmente relevante cuando los dispositivos salen de instalaciones seguras.

11.6 Directiva NIS2 de la UE (2022/2555)

11.6.1 Artículo 21(2)(a, b, d): Exige que el acceso remoto esté protegido como parte del marco de gestión del riesgo de las TIC de la organización. Esta política cumple el requisito de medidas de seguridad que cubran el control de acceso, la seguridad de los datos y las políticas organizativas para entornos remotos.

11.6.2 Artículo 21(3): Fomenta la concienciación en seguridad y la aplicación de políticas entre el personal que trabaja fuera de las instalaciones centrales.

11.7 DORA de la UE (2022/2554)

11.7.1 Artículo 5 – Marco de gobernanza y control interno: Esta política respalda las expectativas de control del riesgo de las TIC para todos los escenarios operativos, incluidos los modelos híbridos y remotos.

11.7.2 Artículo 8 – Marco de gestión del riesgo de las TIC: Los riesgos de acceso remoto se identifican, mitigan y gobiernan mediante los controles técnicos y organizativos aplicados en esta política.

11.7.3 Artículo 9 – Acuerdos de intercambio de información: Protege frente a la fuga remota de información compartida dentro de redes de resiliencia operativa digital.

11.8 COBIT 2019

11.8.1 DSS01 – Operaciones gestionadas: Esta política respalda la continuidad segura de las operaciones de la organización con independencia de la ubicación física.

11.8.2 BAI06 – Cambios de TI gestionados y BAI09 – Activos gestionados: Garantizan que los dispositivos de trabajo remoto sean objeto de seguimiento, se configuren de forma segura y se gestionen como activos críticos.

11.8.3 APO13 – Seguridad gestionada: Promueve un marco definido de gobernanza de la seguridad para entornos remotos.

11.8.4 MEA03 – Supervisar, evaluar y valorar el cumplimiento: Establece que la actividad de trabajo remoto debe registrarse, revisarse y auditarse.