					Introduzca aquí la denominación de la entidad jurídica registrada							
Número de documento: P10S					Título del documento: **Política de escritorio y pantalla despejados**							
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 reglamentos

Norma/Reglamento	Cláusula/Artículo	Comentario
ISO/IEC 27001:2022	Cláusulas 7.2, 8	
ISO/IEC 27002:2022	Control 7	
NIST SP 800-53 Rev. 5	PE-2, AC-11	
Directiva NIS2 de la UE	Artículo 21(2)(d)	
DORA de la UE	Artículo 9(2)(f)	
COBIT 2019	DSS01.06, DSS05	
RGPD de la UE	Artículo 32	

1. Finalidad

1.1 Esta política establece directrices de cumplimiento obligatorio para mantener un entorno de trabajo seguro, garantizando que los escritorios, los puestos de trabajo y las pantallas permanezcan libres de información confidencial visible cuando queden desatendidos.

1.2 Su finalidad principal es prevenir el acceso no autorizado a información sensible a través de impresiones desatendidas, pantallas desbloqueadas o soportes extraíbles mal custodiados, tanto en entornos físicos de oficina como en ubicaciones de trabajo remoto.

1.3 Las prácticas de escritorio y pantalla despejados definidas en esta política refuerzan la capacidad de la organización para cumplir los requisitos de certificación ISO/IEC 27001 al minimizar riesgos de exposición evitables. Estas prácticas también ofrecen garantías a clientes, socios y auditores de que la organización se toma en serio la seguridad de la información, incluso en entornos con recursos limitados.

1.4 Esta política promueve una cultura de responsabilidad proactiva y concienciación, garantizando que todo el personal, con independencia de su función o nivel de conocimientos técnicos, entienda su responsabilidad de proteger la información de la empresa y de los clientes frente a la exposición visual, el robo o la pérdida.

2. Alcance

2.1 Esta política se aplica a:

2.1.1 Todos los empleados, contratistas, becarios y personal temporal que utilicen puestos de trabajo, escritorios o dispositivos móviles propiedad de la empresa o asignados individualmente

2.1.2 Todas las ubicaciones físicas utilizadas para la actividad de la organización, incluidas oficinas dedicadas, entornos de coworking y espacios de trabajo remotos o domiciliarios

2.1.3 Todos los dispositivos digitales con capacidad de visualización, incluidos equipos de sobremesa, portátiles, tabletas y monitores externos utilizados con fines profesionales

2.2 La política se extiende a cualquier activo físico o digital que pueda mostrar, contener o transmitir información sensible, incluidos:

2.2.1 Registros impresos o notas manuscritas

2.2.2 Unidades USB, CD y discos duros externos

2.2.3 Teléfonos móviles utilizados para mensajería profesional o correo electrónico

2.2.4 Monitores de ordenador y proyectores conectados a sistemas de trabajo

2.3 Esta política sigue siendo aplicable fuera del horario laboral habitual y durante operaciones no habituales (p. ej., mantenimiento fuera de horario o trabajos de respuesta ante emergencias).

3. Objetivos

3.1 Aplicar controles prácticos y coherentes que garanticen que no se deje información sensible expuesta en escritorios, pantallas o espacios comunes.

3.2 Minimizar el riesgo de acceso no autorizado, tanto de fuentes internas (p. ej., acceso no intencionado por parte de otros empleados) como de amenazas externas (p. ej., visitantes, personal de limpieza o contratistas).

3.3 Reforzar las restricciones de acceso físico y lógico exigiendo al personal que proteja activamente los materiales de trabajo y bloquee los equipos cuando queden desatendidos.

3.4 Reforzar la concienciación del personal sobre prácticas de trabajo seguras y proporcionar reglas sencillas y exigibles aplicables a las operaciones diarias, con independencia del lugar de trabajo.

3.5 Garantizar la alineación con el control 7.7 del Anexo A de ISO/IEC 27001 y con su guía de implantación conforme a ISO/IEC 27002 para los requisitos de escritorio y pantalla despejados.

3.6 Garantizar que la organización pueda demostrar diligencia debida y preparación para auditorías sin requerir infraestructura de nivel corporativo.

4. Funciones y responsabilidades

4.1 Dirección General (DG)

4.1.1 Es responsable de esta política y garantiza que se comunique adecuadamente, se entienda y se cumpla por todos los empleados y contratistas.

4.1.2 Es responsable de aprobar cualquier excepción, responder a incumplimientos y supervisar la formación relacionada con prácticas de trabajo seguras.

4.1.3 Debe realizar o delegar comprobaciones periódicas, al menos trimestrales, para confirmar que los espacios de trabajo físicos y digitales cumplen lo establecido en la política.

4.2 Miembro del personal designado, si procede

4.2.1 Se le podrá asignar la responsabilidad de implantar configuraciones técnicas (p. ej., ajustes de tiempo de espera de pantalla) o distribuir elementos de almacenamiento físico (p. ej., cajones con cerradura).

4.2.2 Apoya al DG notificando incumplimientos, gestionando recordatorios sobre la seguridad del espacio de trabajo y realizando el seguimiento de las medidas correctivas cuando se identifiquen incidencias.

4.2.3 Ayuda a garantizar que todos los empleados tengan acceso, cuando sea viable, a mecanismos de cierre adecuados o a espacios de almacenamiento seguro.

[... 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 El DG debe revisar esta política al menos una vez al año y tras cualquiera de los siguientes eventos:

9.1.1 Incorporación de nuevos espacios de oficina, dispositivos o sistemas compartidos

9.1.2 Cambios en los requisitos legales o de certificación aplicables

9.1.3 Hallazgos de auditorías, evaluaciones de riesgos o incidentes de seguridad

9.2 Las actualizaciones intermedias deben comunicarse a todos los empleados por correo electrónico, requiriéndose acuse de recibo.

9.3 Las versiones anteriores de esta política deben almacenarse de forma segura y ser auditables para demostrar la alineación continua con ISO/IEC 27001 y marcos relacionados.

10. Políticas relacionadas y vinculaciones

10.1 P2S – Política de funciones y responsabilidades de gobernanza: aclara la autoridad del DG para aplicar y auditar el comportamiento en espacios de trabajo físicos y digitales.

10.2 P4S – Política de control de acceso: respalda la implantación técnica de las prácticas de bloqueo de pantalla e inicio de sesión seguro en puestos de trabajo.

10.3 P8S – Política de concienciación y formación en seguridad de la información: refuerza la formación conductual necesaria para el cumplimiento de la política.

10.4 P17S – Política de protección de datos y privacidad: define las obligaciones para la gestión de datos y la protección de datos personales y sensibles de conformidad con el RGPD de la UE.

10.5 P30S – Política de respuesta a incidentes: proporciona el marco de escalado y respuesta si un incumplimiento da lugar a exposición de datos o a una brecha de seguridad.

11. Normas y marcos de referencia

11.1 ISO/IEC 27001

11.1.1 La cláusula 7.2 exige que todo el personal conozca sus responsabilidades en materia de seguridad, incluidas las medidas de protección físicas.

11.1.2 La cláusula 8.1 exige que los controles operativos garanticen protecciones físicas y lógicas adecuadas.

11.2 ISO/IEC 27002

11.2.1 El control 7.7 proporciona orientación detallada sobre el establecimiento, la comunicación y la aplicación de requisitos de escritorio y pantalla despejados.

11.3 NIST SP 800-53 Rev. 5

11.3.1 PE-2 establece expectativas de control de acceso físico, incluido el comportamiento del personal dentro de entornos seguros.

11.3.2 AC-11 exige la funcionalidad de bloqueo de sesión en puestos de trabajo para evitar la visualización o interacción no autorizadas.

11.4 RGPD de la UE

11.4.1 El artículo 32 exige a las organizaciones proteger los datos personales mediante medidas de protección físicas y técnicas, incluidos los puestos de trabajo y los documentos.

11.5 Directiva NIS2 de la UE

11.5.1 El artículo 21(2)(d) exige a las organizaciones implantar políticas de acceso físico y lógico basadas en el riesgo.

11.6 DORA de la UE

11.6.1 El artículo 9(2)(f) exige políticas de seguridad de las TIC, incluida la higiene segura del espacio de trabajo, para operadores del sector financiero y sus cadenas de suministro.

11.7 COBIT 2019

11.7.1 DSS01.06 exige prácticas de protección de activos, incluidos controles físicos sobre espacios de trabajo y soportes.

11.7.2 DSS05.02 respalda la aplicación de prácticas de seguridad para usuarios finales en todos los entornos operativos.