					Introduzca aquí la denominación de la entidad jurídica registrada							
Número de documento: P10					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**

Alineada con normas y reglamentos

Norma/Reglamento	Cláusula/Artículo	Comentario
ISO/IEC 27001:2022	Cláusula 6.1.3, cláusula 8	Plan de tratamiento de riesgos, planificación y control operacional para espacios de trabajo seguros
ISO/IEC 27002:2022	Control 7	Controles de comportamiento y ambientales para proteger la información física desatendida
NIST SP 800-53 Rev.5	PE-2, PS-7, MP-6, AC-11, CM-6, IA-5	Acceso físico, seguridad del personal externo, destrucción segura de soportes, bloqueo de sesión, controles de configuración y autenticación
RGPD de la UE	Artículos 5(1)(f), 32; considerando 39	Integridad y confidencialidad de los datos, y salvaguardas físicas para los datos
Directiva NIS2 de la UE	Artículos 21(2)(d), 21(3)	Políticas de seguridad física, comportamiento de los usuarios y prevención de fugas de información
DORA de la UE	Artículos 5, 8, 9	Gobierno interno, TIC y gestión de incidentes que involucran seguridad física
COBIT 2019	DSS01, DSS05, MEA	Operaciones gestionadas, servicios de seguridad y supervisión del cumplimiento

1. Propósito

1.1 Esta política establece controles obligatorios para proteger la información sensible mediante la exigencia de una gestión segura de documentos físicos, puestos de trabajo, pantallas y soportes extraíbles, tanto en oficinas como en entornos de trabajo compartidos.

1.2 Esta política respalda el control 7.7 del anexo A de ISO/IEC 27001 al imponer prácticas de comportamiento y técnicas que mitiguen el riesgo de divulgación no autorizada, robo o pérdida de datos debido a información visible o desatendida.

1.3 Esta política refuerza la seguridad física y de la información en las operaciones diarias y respalda el cumplimiento de las obligaciones regulatorias, contractuales y legales aplicables.

2. Alcance

2.1 Esta política se aplica a todo el personal que opere en espacios de trabajo físicos o acceda a ellos, incluidos:

2.1.1 Empleados permanentes y temporales

2.1.2 Contratistas, consultores, proveedores y becarios

2.1.3 Proveedores de servicios externos y visitantes presenciales con acceso a información sensible

2.2 Los requisitos se aplican en:

2.2.1 Oficinas individuales, cubículos y espacios de trabajo diáfanos

2.2.2 Salas de reuniones y zonas compartidas de colaboración

2.2.3 Áreas de impresoras, mostradores de recepción y salas de copiado

2.2.4 Áreas en las que se utilicen puestos de trabajo remotos o terminales compartidos

2.3 Esta política también se aplica a entornos de trabajo temporales o híbridos (p. ej., puestos no asignados) y a entornos abiertos al público donde exista riesgo de observación por encima del hombro o de datos desatendidos.

3. Objetivos

3.1 Prevenir el acceso no autorizado a información confidencial, sensible o regulada expuesta en formato físico o digital.

3.2 Promover una postura de seguridad estandarizada en todos los entornos de trabajo mediante el uso de salvaguardas físicas, la configuración de los puestos de trabajo y el comportamiento del usuario final.

3.3 Reducir el riesgo de brechas de privacidad, pérdida de propiedad intelectual y exfiltración de datos causadas por negligencia o descuido.

3.4 Integrar las prácticas de escritorio limpio y pantalla despejada en la cultura de la organización, reforzando la disciplina operativa, la trazabilidad de auditoría y la capacidad de defensa jurídica.

3.5 Respaldar el cumplimiento de ISO/IEC 27001, el artículo 32 del RGPD de la UE, el artículo 15 de la Directiva NIS2 de la UE y otros requisitos de seguridad física aplicables a datos críticos o personales.

4. Funciones y responsabilidades

4.1 Alta Dirección

4.1.1 Aprueba esta política y promueve una cultura de concienciación en seguridad en todas las unidades de negocio.

4.1.2 Asigna los recursos adecuados para la aplicación de la política, las campañas de concienciación y los mecanismos de control físico.

4.2 Director de Seguridad de la Información / Responsable del SGSI

4.2.1 Es responsable de esta política y garantiza su alineación con ISO/IEC 27001:2022, los requisitos de auditoría y las estrategias de tratamiento de riesgos.

4.2.2 Desarrolla programas de concienciación y controles para garantizar una implantación coherente en instalaciones y entornos de trabajo híbridos.

4.2.3 Coordina con Instalaciones y TI para asegurar que existan salvaguardas físicas adecuadas.

[... 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 Calendario de revisión de la política

9.1.1 Esta política se revisará:

9.1.1.1 Al menos una vez al año

9.1.1.2 Tras cualquier no conformidad de auditoría relacionada con la exposición de espacios de trabajo o pantallas

9.1.1.3 Después de cualquier incidente físico o ambiental (p. ej., robo de dispositivos, acceso no autorizado por seguimiento indebido, vigilancia)

9.1.1.4 Cuando se implanten nuevos diseños de oficina, políticas de instalaciones o modelos de espacio de trabajo (p. ej., puestos no asignados, centros remotos)

9.2 Responsables

9.2.1 El propietario de esta política es el Director de Seguridad de la Información o el Responsable del SGSI designado.

9.2.2 El proceso de revisión deberá implicar a:

9.2.2.1 Equipos de Instalaciones y Seguridad Corporativa

9.2.2.2 TI e Infraestructura para la aplicación relacionada con dispositivos

9.2.2.3 Recursos Humanos y Asuntos Jurídicos para la aplicación de normas de comportamiento y su alineación disciplinaria

9.2.3 Todas las actualizaciones de la política deben estar sujetas a control de versiones, ser aprobadas por el Comité Directivo de Seguridad de la Información y redistribuirse con un nuevo acuse de recibo cuando sea necesario.

9.3 Comunicación de cambios

9.3.1 Los usuarios serán informados de las actualizaciones sustanciales a través de:

9.3.1.1 Centro o portal de políticas en la intranet

9.3.1.2 Comunicaciones dirigidas por correo electrónico

9.3.1.3 Recordatorios durante la incorporación y sesiones informativas trimestrales

9.3.1.4 Solicitudes obligatorias de acuse de recibo para cualquier nueva cláusula crítica de aplicación

10. Políticas relacionadas y vinculaciones

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

10.1.1 P1 – Política de Seguridad de la Información: establece las expectativas sobre comportamiento del usuario y seguridad física que sirven de base a esta política.

10.1.2 P3 – Política de Uso Aceptable: aborda la responsabilidad proactiva del usuario en la protección de datos y sistemas, incluidos los entornos físicos.

10.1.3 P6 – Política de gestión de riesgos: incorpora los riesgos de los espacios de trabajo físicos como parte del análisis integral de riesgos de información.

10.1.4 P12 – Política de gestión de activos: respalda el seguimiento y la gestión segura de dispositivos y soportes dejados sobre escritorios.

10.1.5 P13 – Política de clasificación y etiquetado de datos: se vincula a la aplicación del escritorio limpio para documentos físicos etiquetados como Confidencial o Interno.

10.1.6 P14 – Política de conservación y eliminación de datos: orienta la conservación de documentos físicos, su destrucción y la gestión de contenedores.

10.1.7 P22 – Política de registro de eventos y supervisión: podrá utilizarse para supervisar el estado de bloqueo de los puestos de trabajo, el tiempo de inactividad o las cámaras del espacio de trabajo cuando esté permitido.

10.2 Estas políticas relacionadas establecen una cultura de seguridad integrada que combina la concienciación del usuario, las salvaguardas físicas y la responsabilidad proactiva para garantizar espacios de trabajo resilientes.

11. Normas y marcos de referencia

11.1 Esta política está alineada con normas reconocidas internacionalmente y requisitos legales que exigen la protección de la información sensible en entornos físicos y mediante el comportamiento de los usuarios.

11.2 ISO/IEC 27001

11.2.1 Cláusula 6.1.3 – Plan de tratamiento de riesgos: respalda la implantación de controles para mitigar riesgos físicos y ambientales, incluidos los vinculados al comportamiento de los usuarios en espacios de trabajo abiertos.

11.2.2 Cláusula 8.1 – Planificación y control operacional: establece salvaguardas operativas para gestionar espacios de trabajo seguros y el uso de equipos.

11.3 ISO/IEC 27002:2022 – Control 7

11.3.1 Este control exige protecciones de comportamiento y ambientales para prevenir el acceso no autorizado a la información a través de soportes desatendidos, pantallas o materiales impresos. Esta política impone prácticas de orden en el espacio de trabajo físico, uso del bloqueo de pantalla y eliminación de documentos sensibles.

11.4 NIST SP 800-53 Rev.5

11.4.1 PE-2 (Autorizaciones de acceso físico): vinculado mediante restricciones de espacio de trabajo y la aplicación de almacenamiento con llave en entornos de alto riesgo.

11.4.2 PS-7 (Seguridad del personal externo): aplicado mediante requisitos de escritorio limpio y pantalla despejada extendidos a contratistas y usuarios terceros.

11.4.3 MP-6 (Descontaminación de soportes) y AC-11 (Bloqueo de sesión): implantados mediante procedimientos de eliminación segura y temporizadores obligatorios de bloqueo de pantalla.

11.4.4 CM-6 (Ajustes de configuración) e IA-5 (Gestión de autenticadores): respaldan la aplicación técnica del bloqueo de pantalla y el control de sesión en endpoints.

11.5 RGPD de la UE (2016/679)

11.5.1 Artículo 5(1)(f): exige la integridad y confidencialidad de los datos personales, incluidas las protecciones frente a la exposición física o la visualización por personas no autorizadas.

11.5.2 Artículo 32 – Seguridad del tratamiento: exige medidas físicas y organizativas adecuadas para proteger los datos personales frente a su destrucción accidental o ilícita, pérdida o divulgación no autorizada, lo que se logra mediante controles de escritorio y pantalla.

11.5.3 Considerando 39: exige limitar el acceso a los datos personales a personas autorizadas; ello incluye protegerlos en formato físico cuando quedan sin supervisión.

11.6 Directiva NIS2 de la UE (2022/2555)

11.6.1 Artículo 21(2)(d): exige políticas y procedimientos relacionados con la seguridad física y ambiental, incluidas protecciones de seguridad de la información a nivel del puesto de trabajo.

11.6.2 Artículo 21(3): promueve una cultura de seguridad que incorpore un buen comportamiento del usuario, concienciación y prevención de fugas de datos no intencionadas, respaldada por los controles de comportamiento de esta política.

11.7 DORA de la UE (2022/2554)

11.7.1 Artículo 5 – Gobierno interno y control: exige que todos los riesgos relacionados con las TIC, incluidas las amenazas humanas y ambientales, se rijan mediante políticas exigibles.

11.7.2 Artículo 8 – Gestión del riesgo de las TIC: exige salvaguardas tanto en contextos digitales como físicos, garantizando que los usuarios remotos, de sucursales y en las instalaciones no generen exposición no gestionada.

11.7.3 Artículo 9 – Gestión de incidentes: exige que las deficiencias ambientales o de comportamiento que den lugar a exposición de datos se registren, clasifiquen y traten con acciones correctivas apropiadas.

11.8 COBIT 2019

11.8.1 DSS01 – Operaciones gestionadas: garantiza disciplina operativa en la protección de espacios de trabajo físicos y sistemas mediante controles repetibles.

11.8.2 DSS05 – Gestionar los servicios de seguridad: respalda la protección de datos, dispositivos y endpoints de acceso mediante medidas de aplicación basadas en el comportamiento, como las prácticas de escritorio limpio.

11.8.3 MEA03 – Supervisar, evaluar y valorar el cumplimiento: promueve la auditoría de salvaguardas físicas y de la adopción de políticas en las prácticas diarias de la organización.