					Introduzca aquí la denominación de la entidad jurídica registrada							
Número de documento: P07					Título del documento: **Política de incorporación y cese**							
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	Cláusula 7.2, Cláusula 6	Competencia del personal, incorporación segura y aplicación de responsabilidades en caso de cese o cambio.
ISO/IEC 27002:2022	Controles 6.2, 6.5, 5	Incorporación, acceso y controles del ciclo de vida del personal.
NIST SP 800-53 Rev.5	PS-4, PS-5, AC-2, AC-6, IA-4, IA-5, CM-5, AU-2, AU-6	Transición y cese del personal, mínimo privilegio, registro de auditoría y gestión de accesos durante y después de cambios de personal.
RGPD de la UE	Artículos 5(1)(f), 25, 32; Considerando 39	Limitación del acceso, confidencialidad, protección y controles adecuados para los datos del personal.
Directiva NIS2 de la UE	Artículo 21(2)(b, c, d)	Medidas de seguridad del personal y operativas; mitigación de amenazas internas; procesos del ciclo de vida.
DORA de la UE	Artículos 5, 8, 9	Gobierno, control interno de las TIC, riesgo de las TIC y gestión de incidentes durante la transición del personal.
COBIT 2019	APO07, BAI08, DSS05, MEA03	Recursos humanos, gestión del conocimiento, seguridad y cumplimiento en la incorporación y el cese.

1. Propósito

1.1 Esta política establece procedimientos normalizados para gestionar la incorporación, los traslados internos y los ceses de todo tipo de usuarios.

1.2 Garantiza el aprovisionamiento y desaprovisionamiento oportunos y seguros de los accesos, tanto físicos como lógicos, al tiempo que refuerza la confidencialidad, la rendición de cuentas y la recuperación de activos.

1.3 Esta política mitiga los riesgos asociados al acceso no autorizado, la fuga de datos y la no devolución de activos mediante la integración de controles de incorporación y cese en los procesos de Recursos Humanos, TI y Seguridad.

1.4 Da soporte al control 6.5 del Anexo A de ISO/IEC 27001:2022 al garantizar que las obligaciones de seguridad del personal se apliquen durante y después de la relación laboral o contractual.

2. Alcance

2.1 Esta política se aplica a todos los empleados, contratistas, consultores, proveedores y otros terceros a quienes se conceda acceso a los sistemas, redes, instalaciones o datos de la organización.

2.2 Regula el ciclo de vida completo de:

2.2.1 el proceso de incorporación (contratación, formalización contractual o vinculación temporal)

2.2.2 los traslados internos o cambios de puesto

2.2.3 la desvinculación (renuncia, jubilación, despido o finalización del contrato)

2.3 La política abarca:

2.3.1 acceso lógico (sistemas, aplicaciones, nube, VPN)

2.3.2 control de acceso físico (tarjetas, llaves, sistemas de entrada al edificio)

2.3.3 activos asignados (portátiles, teléfonos, tokens de acceso, credenciales)

2.3.4 acuse de recibo de la política y obligaciones de confidencialidad

2.4 Todos los departamentos (Recursos Humanos, TI, Instalaciones, Seguridad y Dirección) son responsables de ejecutar su función en los flujos de trabajo de incorporación y desvinculación.

3. Objetivos

3.1 Garantizar que a todo el personal se le conceda acceso únicamente tras el cumplimiento de los requisitos previos de seguridad, formación y contratación.

3.2 Revocar los derechos de acceso y recuperar los activos de la organización de forma inmediata cuando se produzca un cambio de puesto o un cese.

3.3 Preservar la confidencialidad, integridad y disponibilidad de los activos de la organización durante las transiciones del personal.

3.4 Respaldar la trazabilidad de auditoría y la defensa jurídica mediante registros completos de los eventos de incorporación y cese.

3.5 Reducir la exposición a amenazas internas mediante la validación y documentación de todos los eventos de acceso relacionados con el personal.

3.6 Alinear el ciclo de vida del personal de la organización con prácticas de seguridad basadas en riesgos y requisitos normativos.

4. Funciones y responsabilidades

4.1 Dirección ejecutiva

4.1.1 Aprueba esta política y asigna autoridad y recursos para los procesos de incorporación, desvinculación y control de acceso.

4.1.2 Garantiza que las transiciones del personal no expongan a la organización a riesgos de seguridad o legales indebidos.

4.2 Recursos Humanos (RR. HH.)

4.2.1 Inicia los flujos de trabajo de incorporación y cese para los empleados y notifica los cambios a los departamentos pertinentes.

4.2.2 Garantiza que las verificaciones de antecedentes, contratos, acuerdos de confidencialidad y acuses de recibo de la política se completen antes de conceder el acceso.

4.2.3 Informa a TI e Instalaciones de las salidas del personal de acuerdo con el acuerdo de nivel de servicio de notificación.

4.2.4 Se coordina con el área Jurídica para aplicar las obligaciones posteriores a la finalización de la relación laboral o contractual (por ejemplo, cláusulas de no divulgación).

[... 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 de la política

9.1.1 Esta política debe revisarse:

9.1.1.1 anualmente, o

9.1.1.2 después de cualquier incidente material relacionado con uso indebido de accesos, pérdida de activos o fallo procedimental

9.1.1.3 cuando se implanten cambios importantes en plataformas de Recursos Humanos o IAM

9.1.1.4 tras actualizaciones normativas o legales que afecten a los datos del personal o a sus obligaciones

9.2 Proceso de revisión y titularidad

9.2.1 El Responsable del SGSI y el Director de Recursos Humanos coordinarán la revisión, con aportaciones de Seguridad de TI, Jurídico y Cumplimiento.

9.2.2 Todos los cambios deben ser aprobados por la Dirección ejecutiva y el Comité de Dirección de Seguridad de la Información.

9.2.3 Las versiones revisadas deben redistribuirse a los departamentos y al personal afectados para un nuevo acuse de recibo.

9.3 Control documental y conservación

9.3.1 Esta política debe incluir:

9.3.2 control de versiones, historial de versiones y fecha de entrada en vigor

9.3.3 propietario responsable y revisor(es)

9.3.4 clasificación de la política y registro de aprobación

9.3.5 Las versiones obsoletas deben archivarse durante un mínimo de 3 años de acuerdo con la Política de Gestión Documental.

10. Políticas relacionadas y vinculaciones

10.1.1 Esta política se integra directamente con:

10.1.2 P1 – Política de Seguridad de la Información: establece los objetivos de seguridad de la organización, incluida la gobernanza del acceso del personal.

10.1.3 P4 – Política de Control de Acceso: establece los requisitos operativos para asignar y revocar accesos a sistemas y accesos físicos sobre la base de los desencadenantes de incorporación y cese.

10.1.4 P3 – Política de Uso Aceptable: exige su acuse de recibo durante la incorporación y respalda su aplicación tras el cese.

10.1.5 P6 – Política de Gestión de Riesgos: garantiza que los riesgos de acceso y transición de usuarios se evalúen y mitiguen conforme a los principios del SGSI.

10.1.6 P11 – Política de Gestión de Cuentas de Usuario y Privilegios: regula los controles técnicos de aprovisionamiento y desaprovisionamiento de accesos en apoyo de esta política.

10.2 Estas políticas forman un sistema de control integrado para gestionar de forma segura y responsable los eventos del ciclo de vida del personal.

11. Normas y marcos de referencia

11.1 Esta política está alineada con marcos reconocidos internacionalmente en materia de seguridad, privacidad y gobierno de TI para garantizar que los procesos de incorporación y cese sean seguros, trazables y conformes con los requisitos legales y organizativos.

11.2 ISO/IEC 27001:

11.2.1 Cláusula 7.2 – Competencia y cláusula 6.2 – Objetivos de seguridad de la información: esta política respalda el establecimiento de la competencia del personal y la incorporación segura de las personas en funciones que influyen en los objetivos del SGSI.

11.2.2 Anexo A, control 6.5 – Responsabilidades tras el cese o cambio de empleo: esta política aplica plenamente controles sobre derechos de acceso residuales, custodia de datos y obligaciones contractuales al producirse la salida.

11.2.3 Anexo A, control 5.9 – Verificación de antecedentes y 6.2 – Términos y condiciones del empleo: los procedimientos de incorporación incorporan mecanismos de verificación de antecedentes y acuse de recibo de la política coherentes con estas cláusulas.

11.3 NIST SP 800-53 Rev.5:

11.3.1 PS-4 (cese del personal) y PS-5 (traslado del personal): esta política aplica la retirada o modificación estructurada de derechos de acceso, tarjetas de acceso y activos físicos.

11.3.2 AC-2 (gestión de cuentas) y AC-6 (mínimo privilegio): las disposiciones garantizan que el acceso esté alineado con el puesto y se revoque con prontitud cuando deje de ser necesario.

11.3.3 IA-4 (gestión de identificadores) e IA-5 (gestión de autenticadores): da soporte a la gestión segura de credenciales durante y después de los cambios de personal.

11.3.4 CM-5 (restricciones de acceso para cambios): evita cambios no autorizados tras el cese mediante la revocación de derechos de acceso elevados.

11.3.5 AU-2 y AU-6: el registro y la trazabilidad de los eventos de acceso se refuerzan mediante la integración de IAM y del registro de auditoría.

11.4 RGPD de la UE (2016/679):

11.4.1 Artículo 5(1)(f): protege los datos personales frente a accesos no autorizados, lo que aquí se aplica mediante la revocación del acceso del usuario durante la desvinculación.

11.4.2 Artículo 32: exige controles técnicos y organizativos adecuados para proteger los datos personales durante el ciclo de vida laboral.

11.4.3 Artículo 25 – Protección de datos desde el diseño: garantiza que la incorporación y el cese integren minimización de datos, conservación y controles de acceso lícito.

11.4.4 Considerando 39: hace hincapié en la limitación del acceso y la confidencialidad, respaldadas por la estructura de esta política.

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

11.5.1 Artículo 21(2)(b, c, d): exige medidas de seguridad del personal y operativas para abordar el control de acceso, la mitigación de amenazas internas y los procesos del ciclo de vida, todos ellos reflejados en esta política.

11.6 DORA de la UE (2022/2554):

11.6.1 Artículo 5 – Gobierno y control interno: esta política respalda el gobierno interno de las TIC relacionado con el riesgo humano y la gestión de accesos.

11.6.2 Artículo 8 – Gestión de riesgos de las TIC: aplica controles a las transiciones del personal que podrían exponer activos críticos o entornos regulados.

11.6.3 Artículo 9 – Clasificación y gestión de incidentes: garantiza que las brechas de seguridad relacionadas con ceses sean notificables y se mitiguen mediante un desaprovisionamiento de accesos adecuado y la correcta gestión de activos.

11.7 COBIT 2019:

11.7.1 APO07 – Gestionar los recursos humanos: define las funciones, responsabilidades y acciones del ciclo de vida para incorporación y cese alineadas con los objetivos de gobernanza.

11.7.2 BAI08 – Gestionar el conocimiento: refuerza la documentación de procedimientos, la conservación del conocimiento y la transferencia de control al final de la relación laboral.

11.7.3 DSS05 – Gestionar los servicios de seguridad: aplica la desactivación de usuarios, el control de activos y la responsabilidad durante las transiciones de puesto.

11.7.4 MEA03 – Supervisar, evaluar y valorar el cumplimiento: garantiza que los controles de incorporación y desvinculación se evalúen durante auditorías internas y externas.