THE ADECCO GROUP

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Grupo Adecco | España

Control del documento

Versión	Fecha	Autor	Aprobado por
2026	03/09/2026	Responsable de Seguridad	Presidente Adecco España

Índice

1. Aprobación y entrada en vigor

Esta Política es efectiva desde la fecha de su aprobación y firma por la Dirección y permanecerá vigente hasta que sea sustituida por una nueva versión.

El documento será revisado periódicamente y siempre que se produzcan cambios relevantes en el contexto, los requisitos aplicables, los riesgos, los servicios o los sistemas incluidos en su alcance.

2. Misión y compromiso

El Grupo Adecco trabaja cada día para crear un futuro mejor en todo el mundo, ayudando a optimizar el talento de las empresas y a transformar sus plantillas, así como a fomentar la empleabilidad de todas las personas.

En su relación con personas candidatas o trabajadoras, contratistas, clientes y proveedores, el Grupo Adecco recopila, procesa, almacena e intercambia **información**. El Grupo Adecco asume el compromiso de protegerla y de proporcionar los recursos necesarios para gestionar su seguridad de forma eficaz.

Los sistemas y servicios deben ser gestionados con diligencia para preservar la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de la información, asegurar la continuidad de los servicios y reaccionar con presteza ante los incidentes.

3. Alcance

Esta Política se aplica a los activos de información dentro del alcance del Sistema de Gestión de Seguridad de la Información (SGSI) del Grupo Adecco; lo que incluye a personas, procesos, instalaciones, proveedores, soportes y sistemas de información.

Para los servicios y proyectos destinados al sector público que requieran la aplicación del Esquema Nacional de Seguridad (ENS), serán exigibles además los principios, requisitos y medidas aplicables a dicho marco normativo.

El personal externo deberá cumplir las obligaciones de seguridad establecidas contractualmente y las normas internas que le sean de aplicación.

4. Objetivos y valores

El objetivo de esta Política es establecer el marco de gobierno y los principios necesarios para proteger los activos de información y prestar servicios seguros y resilientes, de acuerdo con los valores del Grupo Adecco:

- Garantizar la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de la información.
- Prevenir incidentes de seguridad de la información en la medida que sea técnica y económicamente viable, reduciendo la probabilidad de materialización de amenazas y limitando su impacto.

- Reforzar la resiliencia y asegurar una recuperación eficaz ante interrupciones o desastres.
- Aplicar seguridad por diseño y por defecto durante todo el ciclo de vida de los sistemas, servicios y proyectos.
- Cumplir los requisitos legales, regulatorios, contractuales y corporativos aplicables.
- Promover la concienciación, la responsabilidad individual, la colaboración y la mejora continua.

Valores Adecco aplicados a la seguridad de la información

Abordar nuestra misión con energía, evolucionando con un proceso de mejora continua.

Asegurar la privacidad de los datos personales, con una política de buenas prácticas en seguridad de la información.

Cumplir con la responsabilidad legal y ética en el manejo de la información.

Minimizar el impacto de cualquier amenaza de seguridad frente al nuevo reto digital.

Ofrecer soluciones seguras, fiables e interconectadas a clientes internos y externos.

5. Marco normativo

El SGSI mantendrá identificados y actualizados los requisitos legales, regulatorios, contractuales y corporativos aplicables. Entre las referencias principales se incluyen:

- Reglamento (UE) 2016/679, General de Protección de Datos.
- Ley Orgánica 3/2018, de Protección de Datos Personales y garantía de los derechos digitales.

- Real Decreto Legislativo 1/1996, por el que se aprueba el texto refundido de la Ley de Propiedad Intelectual, y normativa que lo modifica.
- Ley 34/2002, de servicios de la sociedad de la información y de comercio electrónico.
- Real Decreto 311/2022, por el que se regula el Esquema Nacional de Seguridad.
- Leyes 39/2015 y 40/2015, cuando sean aplicables a los servicios prestados al sector público.
- Legislación laboral y demás normativa aplicable a las relaciones con el personal, incluida la que afecte a deberes, medidas disciplinarias y derechos digitales.
- Políticas globales del Grupo Adecco, obligaciones contractuales y compromisos con clientes.
- Normas y buenas prácticas aplicables, incluida ISO/IEC 27001 y las guías CCN-STIC cuando correspondan.

6. Sistema de Gestión de Seguridad de la Información

El Grupo Adecco mantiene un SGSI basado en riesgos, orientado al cumplimiento y alineado con las políticas corporativas globales. El SGSI se mantiene actualizado, se adapta a los objetivos de la organización y es objeto de auditorías internas y externas.

La documentación del SGSI se organiza de forma controlada en normativa, políticas, procedimientos, estándares, guías, registros y evidencias.

Las políticas corporativas desarrollan, entre otras materias, la clasificación y manejo de la información, cumplimiento y auditoría, seguridad en desarrollo y gestión de proyectos, riesgos, identidad y acceso, terceros, recursos humanos, seguridad física, operaciones (incluye gestión de incidentes), recuperación ante desastres y copias de seguridad, criptografía y enmascaramiento de datos.

7. Organización y gobierno de la seguridad

La Dirección es responsable última del gobierno de la seguridad de la información, de aprobar esta Política, asignar responsabilidades y facilitar los recursos necesarios.

Las funciones de seguridad se ejercerán con la debida segregación de responsabilidades. Las designaciones nominales, suplencias y relaciones de dependencia se mantendrán en el registro de responsables, roles y responsabilidades y en el acta vigente del Comité de Seguridad de la Información.

Función / Rol	Responsabilidades principales
Dirección	Aprobar la Política, liderar el SGSI, proporcionar los recursos necesarios y resolver las cuestiones elevadas por el Comité.
Responsable de la Información (comité)	Determinar los requisitos y aprobar los niveles de seguridad de la información tratada.
Responsable del Servicio (comité)	Determinar los requisitos y aprobar los niveles de seguridad y continuidad de los servicios prestados.

Responsable de Seguridad (comité)	Coordinar el SGSI corporativo, apoyar la gestión de riesgos e incidentes, supervisar el cumplimiento de los requisitos de seguridad y determinar la idoneidad de las medidas, manteniendo independencia respecto de la operación del sistema.
Responsable del Sistema (comité)	Desarrollar, operar y mantener el sistema, coordinar la implantación de medidas y gestionar su mejora técnica.
Todo el personal	Cumplir esta Política, proteger la información y comunicar incidentes o debilidades sin demora.

8. Comité de Seguridad de la Información

Órgano de coordinación y seguimiento del SGSI y de la seguridad de los sistemas sujetos al ENS. Su composición, designación, renovación, cese, periodicidad y reglas de funcionamiento se establecerán en su acta o norma de constitución vigente.

Impulsa la estrategia de seguridad de la información, revisa riesgos e incidentes relevantes, supervisa planes de tratamiento y mejora, propone prioridades de actuación y mejora en materia de seguridad de la información y riesgo y eleva a la Dirección las decisiones que excedan sus atribuciones. Los conflictos de responsabilidad o criterio se documentarán y escalarán a la Dirección para su resolución.

9. Gestión de riesgos

Todos los sistemas y servicios incluidos en el alcance deberán someterse a un análisis de riesgos proporcionado a su criticidad. El análisis considerará amenazas, vulnerabilidades, impacto, probabilidad, dependencias y controles existentes.

El análisis se revisará al menos anualmente y cuando se produzcan cambios significativos en la información, los servicios, la tecnología, los terceros o el contexto; cuando ocurra un incidente grave; o cuando se identifiquen vulnerabilidades graves. Los riesgos se tratarán, aceptarán y supervisarán por los responsables competentes conforme a la metodología aprobada.

10. Seguridad de las personas

La seguridad se integra en todo el ciclo de vida de las personas trabajadoras, desde la selección e incorporación hasta los cambios de función y la finalización de la relación laboral o contractual.

- Informar de las obligaciones de seguridad y confidencialidad y reflejarlas en contratos, compromisos y descripciones de puesto.
- Proporcionar formación inicial obligatoria y concienciación periódica, al menos anual, adaptada a las funciones y riesgos.

- Formar antes de asumir responsabilidades de uso, operación o administración de sistemas cuando sea necesario.
- Gestionar de forma oportuna las altas, cambios y bajas de acceso.
- Aplicar el régimen disciplinario y contractual conforme a la legislación y normativa interna aplicables.
- Facilitar canales para comunicar incidentes, debilidades y sospechas de incumplimiento.

11. Control de acceso

El acceso a la información, los sistemas y los servicios se basará en necesidad de negocio, mínimo privilegio, segregación de funciones y autorización formal. La identidad de los usuarios deberá verificarse mediante mecanismos de autenticación adecuados al riesgo.

Los derechos de acceso se revisarán periódicamente y tras cambios de función. Las cuentas privilegiadas, accesos remotos, conexiones con terceros y actividades críticas estarán sujetos a controles reforzados, registro y supervisión. Cada persona es responsable del uso adecuado de sus credenciales y dispositivos.

12. Seguridad física y ambiental

Las instalaciones, equipos, cableado y soportes de información (incluido la documentación en papel) se protegerán frente a accesos no autorizados, daños, interferencias y amenazas ambientales mediante controles proporcionales al riesgo.

Se definirán y revisarán los niveles de acceso físico a zonas restringidas. Se aplicarán medidas para equipos fuera de las instalaciones, mantenimiento y traslado de activos, así como las normas de escritorio limpio y pantalla bloqueada.

13. Adquisición y desarrollo seguro

Los requisitos de seguridad, privacidad, continuidad y cumplimiento se identificarán desde la planificación de proyectos, adquisiciones, desarrollos y contrataciones, y se incorporarán a solicitudes de oferta, contratos, criterios de aceptación y actividades de mantenimiento.

Los cambios y desarrollos se someterán a controles de aprobación, pruebas, segregación de entornos y revisión de riesgos. Los proveedores y subcontratistas deberán cumplir requisitos de seguridad proporcionales al servicio y estarán sujetos a seguimiento.

14. Seguridad por diseño y por defecto

La seguridad de la información y la protección de datos se integrarán como requisitos transversales durante todo el ciclo de vida de procesos, productos, servicios y sistemas. Las configuraciones iniciales deberán ser

seguras, limitar la exposición innecesaria y habilitar únicamente las funciones, accesos y comunicaciones requeridos.

15. Integridad, cambios y actualización

La integridad de los sistemas se protegerá mediante procesos documentados de gestión de cambios, configuración, vulnerabilidades, actualizaciones y parches. Los cambios con impacto relevante requerirán evaluación previa de seguridad, autorización, pruebas y, cuando proceda, un plan de reversión.

Se realizarán revisiones periódicas del estado de seguridad teniendo en cuenta recomendaciones de fabricantes, vulnerabilidades conocidas, obsolescencia y actualizaciones aplicables.

16. Protección de la información

La información se clasificará y tratará de acuerdo con su sensibilidad, requisitos legales, valor y criticidad. Se aplicarán controles adecuados durante su creación, acceso, uso, almacenamiento, transmisión, archivo y eliminación.

La información almacenada o transmitida a través de entornos de riesgo, incluidos equipos portátiles, teléfonos móviles, medios extraíbles, servicios en la nube, redes abiertas o conexiones de terceros, se protegerá mediante cifrado, control de acceso, gestión de dispositivos y otros mecanismos proporcionales al riesgo.

17. Interconexión y seguridad de red

Las interconexiones con redes públicas, privadas, servicios en la nube y sistemas de terceros deberán estar autorizadas, documentadas y protegidas. Antes de su puesta en servicio se analizarán los riesgos, se definirán responsabilidades y se controlarán los puntos de unión.

La arquitectura de red aplicará segmentación, filtrado, monitorización y protección perimetral de acuerdo con el riesgo, y la criticidad según la naturaleza de los servicios.

18. Continuidad, recuperación y copias de seguridad

El Grupo Adecco mantendrá capacidades de continuidad y recuperación que permitan responder a interrupciones y restablecer los servicios dentro de los objetivos aprobados. Los planes se basarán en el análisis de impacto en el negocio y en el análisis de riesgos.

Las copias de seguridad se protegerán, supervisarán y probarán. Los planes de continuidad y recuperación se ejercitarán periódicamente, se registrarán los resultados y se corregirán las desviaciones identificadas.ç

19. Gestión de incidentes

Todo el personal y los terceros deberán comunicar sin demora los incidentes, eventos o debilidades de seguridad a través de los canales establecidos. Los incidentes se registrarán, clasificarán, investigarán, contendrán, resolverán y cerrarán conforme al procedimiento vigente.

El Responsable de Seguridad coordinará el tratamiento y el reporte al Comité de Seguridad de la Información y a los responsables afectados. Cuando proceda, se activarán los procesos de continuidad, notificación regulatoria, comunicación a terceros, conservación de evidencias y aprendizaje posterior.

20. Cumplimiento, auditoría y mejora continua

El cumplimiento de esta Política será objeto de seguimiento mediante indicadores, revisiones, auditorías internas y externas, evaluaciones de riesgos, pruebas y seguimiento de acciones correctivas.

El SGSI aplicará un proceso de mejora continua alineado con ISO/IEC 27001 y, cuando corresponda, con el ENS. Las excepciones deberán justificarse, evaluarse, aprobarse por la autoridad competente, quedar registradas y revisarse dentro de un plazo definido.

Aprobación

La presente Política será aprobada y firmada por el **Presidente de Adecco España**. La identificación de la persona firmante y la fecha de aprobación se incorporarán en la versión definitiva controlada.