



Política de Seguridad de la Información

Referencia:

DQA-POL-07

Edición: 01

19/09/2025

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Elabora	Revisa	Aprueba
Manuel Ángel Lombó Álvarez	José Antonio Díaz Pérez	Fernando Casariego
Dtr. Tecnología e Innovación	Dtr. Auditoría y QHSE	Dtr. General

CONTROL DE MODIFICACIONES

Ed.	Fecha	Apartado modificado	Descripción
01	19/09/2025	Edición inicial	

DQA-FRM-01 Ed.02





Política de Seguridad de la Información

Referencia:

DQA-POL-07

Edición: 01

19/09/2025

La Dirección de DiagnóstiQA Consultoría Técnica SL (“**DiagnóstiQA**”), en el marco de sus competencias para establecer las políticas y estrategias de la organización, ha aprobado la presente Política de Seguridad de la Información (en adelante, la “**Política**”).

El objetivo de esta Política, dirigida a todos los grupos de interés, es definir y establecer los principios, criterios y objetivos de mejora que rigen las actuaciones en materia de seguridad de la información en línea con las directrices marcadas por la norma ISO27001.

1 FINALIDAD

DiagnóstiQA asume la seguridad de la información asociada a sus servicios como uno de los factores clave en la realización de sus actividades con objeto de garantizar la confidencialidad, integridad y disponibilidad, protegiendo los datos personales, la privacidad de la información y los sistemas de información contra accesos indebidos y modificaciones no autorizadas.

Forma parte de la política estratégica de DiagnóstiQA la implantación y el desarrollo de un Sistema de Gestión de Seguridad de la Información basado en la identificación, protección, detección, respuesta y recuperación de los sistemas de información, aportando para ello la Dirección de la compañía, los recursos necesarios para su consecución.

DiagnóstiQA, consciente de la necesidad de integrar todas las herramientas y los medios necesarios para prestar sus servicios con eficiencia, calidad y en un entorno seguro de gestión de la información, incidirá en todas aquellas medidas y actuaciones que logren reducir, minimizar, transferir o evitar los Riesgos y permitan aprovechar las Oportunidades para su Sistema de Gestión.

A tal efecto, la Dirección de DiagnóstiQA se compromete a mejorar continuamente el Sistema de Gestión de Seguridad de la Información implantado, en las revisiones periódicas que mantiene anualmente y mediante el establecimiento de objetivos y acciones de mejora.

2 PRINCIPIOS GENERALES

Mediante esta Política, DiagnóstiQA asume y promueve los siguientes principios generales que deben guiar todas sus actividades:

- a. Dirigir nuestros esfuerzos a la prevención de errores, así como a su corrección, control y gestión.
- b. Fomentar la participación de todos para conseguir los objetivos establecidos por DiagnóstiQA, lo que redundará en el bien de nuestros empleados, clientes y otras partes interesadas.
- c. Tomar la formación continua y la concienciación como uno de los principales pilares en los que se sustenta la seguridad de la información.
- d. Asegurar que la empresa cumple con todos los requisitos exigibles por parte de los clientes, las distintas administraciones y organismos públicos, así como todos los requisitos legales y reglamentarios aplicables, poniendo especial énfasis en aquellos establecidos por la legislación en materia de seguridad de la información.
- e. Establecer los procedimientos que sean necesarios para el control, monitorización y prevención de incidentes.
- f. Dotarse de herramientas y procedimientos que permitan adaptarse con agilidad a las condiciones cambiantes del entorno.
- g. Garantizar la confidencialidad, integridad, disponibilidad, así como la debida protección de los datos y los sistemas de información contra accesos indebidos, ciberataques y modificaciones no autorizadas.
- h. Garantizar la continuidad del negocio, en cuanto a seguridad de la información se refiere, protegiendo los procesos críticos contra fallos o desastres significativos.
- i. Realizar una adecuada evaluación, gestión y tratamiento del riesgo de seguridad de la información para alcanzar un nivel madurez elevado y minimizar el riesgo, priorizando las medidas y controles a implantar acordes con los riesgos identificados y objetivos de negocio.
- j. Actuar de manera adecuada y conjunta para prevenir, detectar y responder a los ciberincidentes que pudieran afectar a la seguridad de la información.



Política de Seguridad de la Información

Referencia:

DQA-POL-07

Edición: 01

19/09/2025

- k. Mejorar la eficiencia de los controles de seguridad implantados para adaptarse a la evolución de los riesgos y los nuevos entornos tecnológicos.
- l. Gestionar de manera adecuada los usuarios mediante procedimientos de autenticación robustos y el establecimiento de políticas de contraseñas fuertes, garantizando el acceso solo a aquellos usuarios debidamente autorizados.
- m. Proteger de forma integral los sistemas de correo electrónico, servidores y endpoints mediante mecanismos avanzados de seguridad que aseguren la confidencialidad, integridad y disponibilidad de la información.
- n. Implementar copias de seguridad periódicas con mecanismos específicos de protección contra ransomware, asegurando la capacidad de recuperación de datos ante incidentes de seguridad.
- o. Realizar actualizaciones y parcheos periódicos de todo el software, con el fin de corregir vulnerabilidades y adaptarse a nuevas amenazas de seguridad.
- p. Revisar y evaluar la seguridad de la información periódicamente, tomando las medidas necesarias para corregir las desviaciones que se pudieran detectar.

Esta Política de Seguridad de la Información fue aprobada el 19 de septiembre de 2025 por la Dirección de DiagnósticoQA.

