# ISO 27001. “Un peligro diagnosticado es un peligro evitado”: Diagnóstico de la Seguridad de la Información

Un diagnóstico de la Seguridad de la Información es un proceso mediante el cual se evalúa y analiza el estado de seguridad de los sistemas, redes y datos de una organización o entidad. El objetivo principal de este diagnóstico es identificar y evaluar los riesgos y vulnerabilidades existentes en el entorno de seguridad de la información.

Durante el proceso de diagnóstico, se realizan diversas actividades, como la revisión de políticas y procedimientos de seguridad, la evaluación de controles de seguridad implementados, la identificación de posibles brechas de seguridad, la revisión de la configuración de los sistemas y redes, y la evaluación de la capacitación y concienciación del personal en materia de seguridad.

El diagnóstico de seguridad de la información se basa en estándares y buenas prácticas reconocidas en el campo de la seguridad, como ISO 27001, NIST Cybersecurity Framework o COBIT. También puede incluir pruebas de penetración, análisis de vulnerabilidades y evaluaciones de riesgos.

Una vez completado el diagnóstico, se generan informes detallados con los hallazgos, recomendaciones y un plan de acción para abordar las deficiencias identificadas. Estos informes ayudan a la organización a tomar decisiones informadas sobre cómo mejorar su postura de seguridad y proteger sus activos de información.

En resumen, un diagnóstico de seguridad de la información es un proceso crítico para evaluar la efectividad de las medidas de seguridad existentes y para identificar áreas de mejora en la protección de la información sensible de una organización.

El diagnóstico de la seguridad de la información es el acto de investigar y analizar los riesgos asociados a los procesos del propio negocio y su entorno.

Un diagnóstico eficaz va a permitir:

- Conocer los **activos y recursos a proteger**, los puntos vulnerables de cada proceso y las amenazas asociadas.
- Evaluar la **viabilidad y efectividad de los controles** de reducción a la exposición de amenazas que se están desarrollando.
- Identificar el **nivel de riesgo aceptable** para que la organización pueda existir.
- Calcular el **coste del impacto de materialización** de las amenazas identificadas.
- Valorar la **capacidad de recuperación** frente a incidentes y la probabilidad de continuidad de los procesos del negocio.
- Elaborar **planes de acción** para la mejora y solución de los puntos críticos.

**¿Qué se debe diagnosticar?**

Las organizaciones se estructuran en sistemas con el fin de alcanzar unos objetivos mediante la aplicación de procesos. Por ello, para el diagnóstico eficiente de

seguridad de la información se recomienda el análisis funcional de la organización, considerando las siguientes áreas:

- Sistema de gestión, políticas, planes de seguridad y base reglamentaria.
- Inventario de Hardware, Software y la evaluación de su valor real y de pérdida.
- Seguridad de la red e Internet.
- Accesos remotos y uso de servicios de acceso a aplicaciones de la organización.
- Publicaciones de la organización.
- Ordenadores de mesa y estaciones de trabajo en red.
- Seguridad física y ambiental de la Edificación.
- Fronteras de responsabilidades y disciplina tecnológica de la red.

Todas ellas deben estar identificadas e inventariadas. Así mismo, de cada una de ellas deben verificarse diferentes aspectos básicos relacionados con la normativa vigente, la aplicabilidad al caso real de la organización, la eficiencia del control ejercido, el valor económico, la empleabilidad y la formación del personal encargado.

**¿Cómo se debe realizar el diagnóstico?**

El diagnóstico de la seguridad de la información propone un enfoque sistémico y por objetivos, aplicado a los principios básicos de evidencia, análisis, síntesis y de control. El procedimiento para acometer el diagnóstico se puede resumir en las siguientes fases:

- Presentar el **programa de diagnóstico** con la definición de los objetivos, identificación de activos y recursos, técnicas a aplicar, recursos disponibles y temporalización.
- Contar con **personal formado y cualificado** oficialmente que sea capaz de verificar y revisar los equipos y aplicaciones informáticas, la red y el personal a cargo.
- Establecer un **expediente que registre evidencias**, organice la documentación solicitada, recopile actas y material relacionados con las pruebas realizadas.
- Presentar un **informe con los resultados** del diagnóstico que recoja la identificación del sistema, las fechas de ejecución, el equipo encargado, los criterios de medición y objetivos comprobados, los resultados finales, los elementos no conformes, una conclusión final y una serie de recomendaciones de mejora.

**ISOTools** es la plataforma tecnológica que permite ejecutar el diagnóstico de seguridad desde el momento cero, aplicando el enfoque a procesos para evaluar globalmente todas las áreas de la organización.

**ISOTools** cumple los objetivos del diagnóstico, facilita determinar el **GAP** de la organización con respecto a los niveles de madurez requeridos, evaluar los riesgos, analizar los controles y poder determinar un **Plan de Acción**, para comenzar a trabajar en los procesos críticos para la organización.

Las **ventajas** que ofrece la automatización del proceso de diagnóstico con ISOTools son:

- Fácil identificación de **activos y recursos** a diagnosticar.
- Permite una **evaluación individual** intuitiva, mediante un cuestionario equilibrado en alcance y precisión.
- Aplicabilidad para **diferentes diagnósticos** basados en modelos contrastados y la participación de expertos.
- Fomenta el **entorno colaborativo** mediante el uso de herramientas para gestionar y alcanzar una evaluación consensuada.

**ISOTools** ofrece un conjunto de potentes aplicaciones parametrizables que ayudan a alas organizaciones en todas las fases del diagnóstico de la Seguridad de la Información: **evaluación del riesgo, evaluación de la eficacia de controles, check list, incidentes TI, gestión de reports e indicadores.**