Seguridad de la información: aplicación de IRAM-ISO/IEC 27001

Tres casos de éxito de la certificación de la Norma IRAM-ISO/IEC 27001, aplicada por diversas organizaciones con el objetivo proteger la confidencialidad, integridad y disponibilidad de los datos que manejan.

IRAM
www.iram.org.ar

La seguridad de la información (SI) ya no es un aspecto privativo de las empresas vinculadas a la tecnología. Se trata de un pilar fundamental tenido en cuenta por todo tipo de organizaciones, independientemente de su tamaño o rubro. En esta línea, la adopción de un sistema de gestión de seguridad de la información (SGSI o ISMS, por sus siglas en inglés) se convierte en una decisión estratégica.

La norma internacional cuyo cumplimiento garantiza una adopción adecuada es la IRAM-ISO/IEC 27001. Las organizaciones que implementan este documento logran planificar, operar, medir, revisar y mejorar la seguridad de la información mediante un enfoque basado en riesgos, alineando los objetivos de seguridad con los objetivos de negocio y con los requisitos de seguridad de las partes interesadas (clientes, entes reguladores, accionistas, la sociedad en su conjunto).

Entre otras ventajas, el estándar permite priorizar las inversiones en función de los riesgos asociados, que sean de mayor relevancia para la organización

Entre otras ventajas, el estándar permite priorizar las inversiones en función de los riesgos asociados, que sean de mayor relevancia para la organización, pudiendo, a su vez, demostrar su retorno y justificar nuevas cuando sean necesarias.

Diversas organizaciones de relevancia han adoptado el estándar, entre ellas, se pueden destacar Nosis Laboratorio de Investigación y Desarrollo, el Grupo MSA SA y Conexia.

Aplicación en un laboratorio de investigación y desarrollo

Según testimonio de la propia gerencia, en Nosis la seguridad de la información ha sido siempre abordada, y ya solía identificar circunstancias para mejorar de índole cultural y de procesos.

Por ejemplo, la seguridad de la información se trataba como algo aislado, propio de las áreas de Desarrollo y Tecnología, y la responsabilidad recaía estrictamente en ellas. Además, existía escasa documentación formal sobre los procesos relacionados con la temática; los análisis de riesgo no eran algo común, como así tampoco la evidencia de los controles realizados.

El proceso de certificación requirió de tiempo, esfuerzo y un cambio en la cultura organizacional. Permitió dar cuenta de que la seguridad de la información merecía un enfoque distinto, y entender que es un proceso de mejora continua que debe ser sostenido y enriquecido.

Como consecuencia, la aplicación de un sistema de gestión de seguridad de la información ayudó a la empresa a organizarse de una manera ordenada y auditable, con documentación más detallada sobre los procesos, identificando sus riesgos y posibles acciones de mitigación.

Su integración con el resto de los aspectos de la organización se ha realizado de manera natural, impulsado por el compromiso de las distintas áreas de la empresa y de la alta dirección.

Se ha elaborado y difundido la Política de Seguridad de la Información de la empresa, la cual dicta los estándares de seguridad de la información que deben cumplir todas las partes interesadas. Sobre dicha política, hoy existe un esquema de concientización continua.

Asimismo, el sistema evoluciona permanentemente y es una herramienta eficaz a la hora de implementar cambios en toda la organización que puedan impactar en la seguridad de la información. Además, la certificación generó un impacto positivo en los clientes, quienes ahora perciben a Nosis como una empresa sólida en el tratamiento de los datos.

La aplicación de un sistema de gestión de seguridad de la información ayudó a la empresa a organizarse de una manera ordenada y auditable, con documentación más detallada sobre los procesos

Aplicación en un grupo empresario

Sin importar a qué se dedique una organización, la correcta gestión de la seguridad de la información es central, en tanto que el mundo actual demanda mantenerse actualizado en las buenas prácticas seguridad de la información. Así lo entendió el Grupo MSA, que nuclea empresas a fin de ofrecer soluciones innovadoras de software.

Antes de la certificación, la tarea requería esfuerzos que hoy salvaguarda gracias a la formalización y gestión eficiente alcanzadas. El proceso permitió formalizar formas de trabajo, brindó orden y ayudó a comunicar e involucrar a todos los colaboradores en la gestión diaria de la información.

Asimismo, entre los mayores beneficios que impactaron positivamente en la empresa se encuentra el involucramiento de todos los equipos en la gestión de la seguridad de la información en sus procesos y operaciones diarias; en ampliar su impacto fuera de los equipos IT, que siempre lo tienen en su top de prioridades, y en la formalización de las capacitaciones a todos los sectores. Con ISO 9001, la empresa ya trataba el tema de forma transversal, pero con 27001, logró profundizar y gestionar la seguridad de la información con una mirada crítica.

Vale destacar que el Grupo MSA hace ya más de 25 años que lleva adelante procesos tecnológicos de misión crítica en Latinoamérica, por lo que valora tener una construcción de confianza apoyada en su trayectoria, integridad y credibilidad. La seguridad es, sin duda, un factor clave en sus proyectos y en esa construcción de confianza. En este sentido, la certificación es un aval de su compromiso con la seguridad de la información y la calidad en todos sus procesos.

Con ISO 9001, la empresa ya trataba el tema de forma transversal, pero con 27001, logró profundizar y gestionar la seguridad de la información con una mirada crítica.

Aplicación en una empresa de tecnología

En el caso de Conexia, la empresa no contaba con procesos definidos y/o controles de seguridad monitoreados regularmente con el objetivo de apalancar la protección de los datos de acuerdo con su nivel de sensibilidad y criticidad.

Tener un ente que la regule, monitoree y apoye con regularidad con base en sus recomendaciones y mejoras en temas de seguridad, en cuanto al diseño y ejecución de los controles de seguridad de la información, está entre los mayores beneficios que la empresa reconoce tras la aplicación de IRAM-ISO/IEC 27001.

Tener un sistema de gestión de seguridad de la información certificado apalancó la implementación de procesos clave de seguridad, como la gestión de riesgos proactiva, de incidentes, de continuidad, etc.; y esto se vio luego reflejado en mejoras a nivel gobierno organizacional, que respaldan la satisfacción de los clientes internos y externos.

Tener un sistema de gestión de seguridad de la información certificado apalancó la implementación de procesos clave de seguridad, como la gestión de riesgos proactiva, de incidentes, de continuidad, etc.