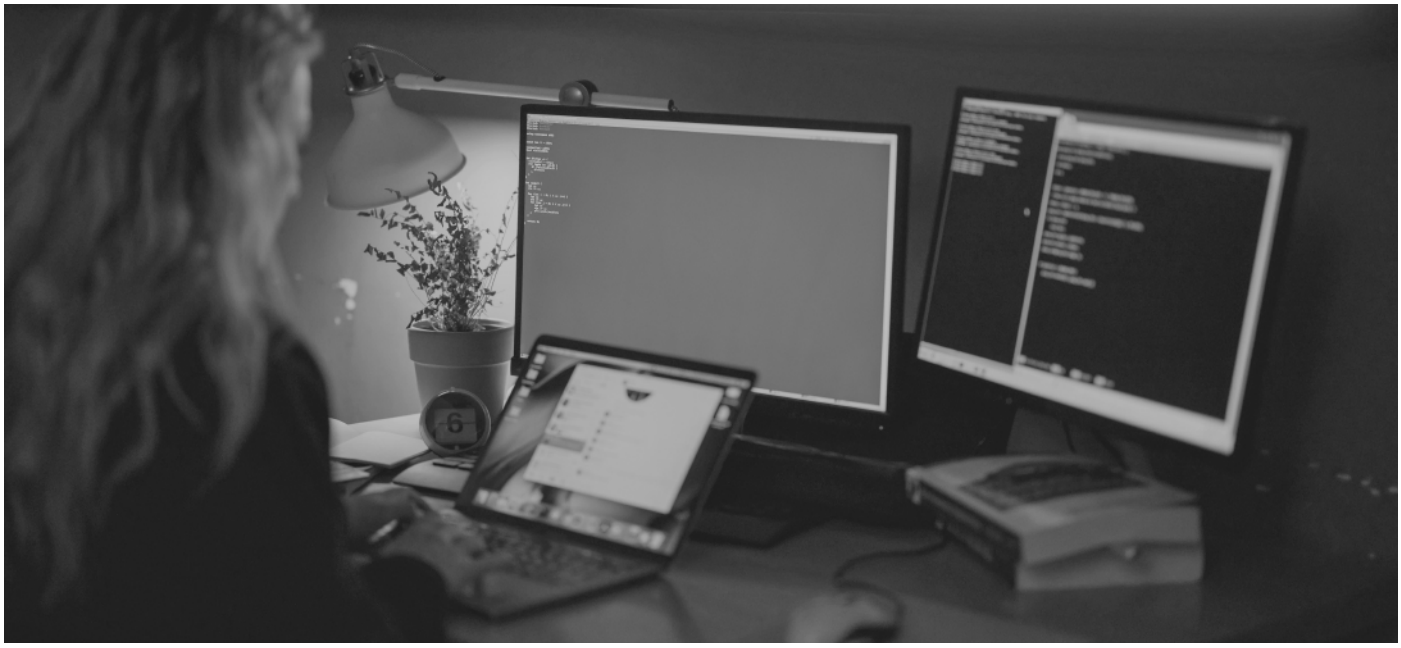
Importancia de la organización bajo el esquema de la ISO 27001:2013



América Latina sufrió más de 91,000 millones de intentos de ciberataques durante el primer semestre del año 2021. En la región, los países más afectados por el aumento de los ataques cibernéticos fueron México, con 60,800 millones; Brasil, con 16,200 millones; Perú, con 4,700 millones posicionándose en la tercera ubicación; y Colombia, con 3,700 millones (Gestión, 2021).

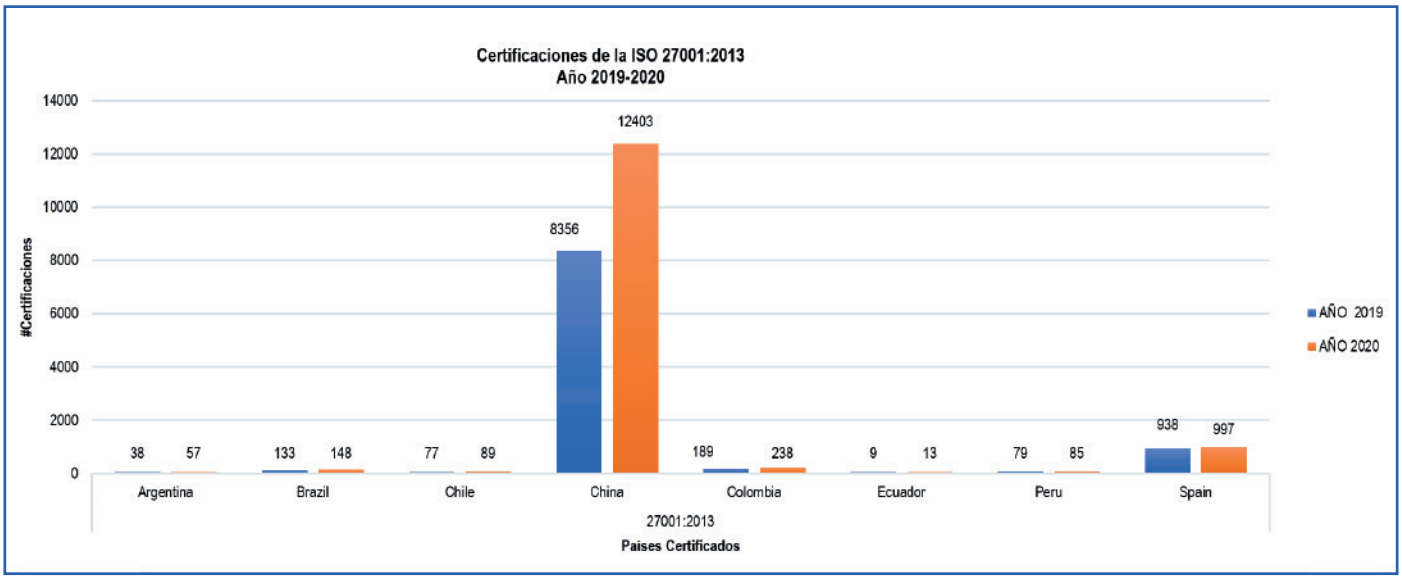
Ante una sociedad cada vez más digitalizada y ante las nuevas necesidades que han surgido a raíz de la crisis sanitaria por COVID-19, se ha desarrollado diversas amenazas que pueden perjudicar a una organización. Tales como el acceso a la red, al sistema de información por personas no autorizadas, incumplimiento de relaciones contractuales con el cliente o partes interesadas, infracción legal, fuga de información debido al termino de contrato, errores de software entre otros; dando lugar a situaciones comprometedoras para las empresas ya sean pequeñas corporaciones o grandes multinacionales.

Por ello, se debe tener en cuenta que la información, los sistemas informáticos y procesos, forman activos de información que la organización debería mantener adecuadamente, la ISO 27001 menciona que estos son algo que una organización valora y por lo tanto protege. Además, esto se pueden clasificar en datos y/o información, software, hardware, dispositivos móviles, redes de comunicación, los colaboradores, entre otros.

De acuerdo al informe publicado por la ISO, en el año 2019 y 2020 se ha incrementado en todo el mundo la implementación y por ende la certificación de la ISO 27001:2013 (ver figura 1), debido a que esta norma establece una metodología la cual permite gestionar la seguridad de la información de forma clara y concisa, minimizando los riesgo de incidentes de seguridad de la información como pérdidas y/o robos de información y de esta manera establece medidas de control para que los propios clientes, colaboradores, proveedores y partes interesadas puedan acceder a la información de forma segura y controlada, de esta manera ofrece a los clientes y socios estratégicos un compromiso, ya que muestra a la empresa como un organismo preocupado por la confidencialidad, la integridad y la seguridad de la información (Tech Consulting, 2020).

Figura 1

Certificación ISO 27001:2013



La ISO 27001 se basa en el ciclo PHVA, también conocido como ciclo de Deming. El ciclo PHVA puede aplicarse no solo al sistema de gestión sino también a cada elemento individual para proporcionar un enfoque en la mejora continua (Gómez, 2018).

- **Planear:** Se define la política de seguridad y competencias, se asigna las autoridades y responsabilidades, se establece el alcance del SGSI, se realiza el análisis de riesgo y se selecciona los controles.
- **Hacer:** Se implementa el plan de gestión de riesgos y los controles establecidos.
- **Verificar:** se controla y mide los procesos para establecer el rendimiento de la política, objetivos, requisitos y actividades planificadas además de informar de los resultados.
- **Actuar:** Se implementa las mejoras identificadas adoptando las acciones correctivas y preventivas como acciones de mejora para contribuir al rendimiento del sistema de gestión de la seguridad de la información.

La seguridad de la información está ocupando un valor importante para las organizaciones y la adopción de la ISO 27001:2013 es cada vez más usual. La mayoría de las organizaciones reconocen que los incidentes de seguridad pueden suceder, solo es cuestión de tiempo para verse afectado por alguno de ellos.

Por ello, se debe tener en cuenta que la tecnología solo es un apoyo para llegar a minimizar ciertas amenazas, el sistema de gestión de seguridad de la información es un trabajo continua y conlleva a un trabajo en equipo.
Como dice Bruce Schneier (2008):

> "Si piensas que la tecnología por sí misma puede resolver los problemas de seguridad, entonces no entiendes los problemas y por ende la tecnología".

El entender ello, permite que la organización optimice el funcionamiento de los procesos de información y por lo tanto una reducción de costos. Además, se convierte en una ventaja competitiva frente a la competencia, pues el contar con un SGSI incrementa su imagen a nivel nacional e internacional.

Referencias:

Gestión (2021, septiembre 21). *Perú es el tercer país con más ciberataques en América Latina: Sufrió más de 4,700 millones de intentos nndc* | ECONOMIA. Gestión; NOTICIAS GESTIÓN. https://gestion.pe/economia/peru-es-el-tercer-pais-con-mas-ciberataques-en-america-latina-sufrio-mas-de-4700-millones-de-intentos-nndc-noticia/

Gómez Galindo, D. M. (2018). *Desarrollo del sistema de gestión de seguridad de la información (SGSI) alineado con el estándar ISO 27001 y sus requisitos básicos en la aplicación del ciclo PHVA*. 11.

NQA-ISO-27001-Guia-de-implantación. (s. f.). Recuperado 17 de enero de 2022, de https://www.nqa.com/medialibraries/NQA/NQA-Media-Library/PDFs/Spanish%20QRFs%20and%20PDFs/NQA-ISO-27001-Guia-de-implantacion.pdf

Schneier, U. A.. (2008). *Bruce Schneier, experto en seguridad informática*. UABDivulga Barcelona Investigación e Innovación. http://www.uab.cat/web/detalle-noticia/bruce-schneier-experto-en-seguridad-informatica-1345680342040.html?articleId=1212474376342

Tech Consulting. (2020, octubre 7). Ventajas de implantar un Sistema de Gestión de Seguridad de la Información (SGSI) en tu empresa. *TechConsulting - Ciberseguridad en Murcia y Alicante*. Recuperado de https://techconsulting.es/ventajas-de-implantar-un-sistema-de-gestion-de-seguridad-de-la-informacion-sgsi-en-tu-empresa/

Lucero Arana Walde
Procesos SIG
larana@corebusinesscorp.com

Core Business Corp.