53

Fecha de presentación: julio, 2021
Fecha de aceptación: agosto, 2021
Fecha de publicación: septiembre, 2021

AUTOMATIZACIÓN

DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN BASADO EN LA NORMA ISO/IEC 27001

AUTOMATION OF AN INFORMATION SECURITY MANAGEMENT SYSTEM BASED ON THE ISO / IEC 27001 STANDARD

Tonysé de la Rosa Martín[1]
E-mail: tdelarosa@umet.edu.ec
ORCID: https://orcid.org/0000-0002-0881-6034
[1] Universidad Metropolitana. Ecuador.

Cita sugerida (APA, séptima edición)

De la Rosa Martín, T. (2021). Automatización de un sistema de gestión de seguridad de la informa-ción basado en la Norma ISO/IEC 27001. *Revista Universidad y Sociedad*, 13(5), 495-506.

RESUMEN

El presente trabajo tiene como objetivo describir los requisitos para la implementación y la docu-mentación necesaria de un Sistema de gestión de seguridad de la información (SGSI). La automati-zación consiste en la disponibilidad de una plantilla con preguntas de control internas enfocadas en los 3 pilares de la seguridad de la información (confidencialidad, integridad, disponibilidad) que permita realizar un "Gap-Analysis" para medir el nivel de madurez actual respecto a los requisitos del estándar internacional ISO/IEC 27001:2013, con un diagrama de radar y así instaurar un SGSI o realizar el proceso de la certificación ISO 27001 que garantice minimizar el riesgo y proteger la información en las computadoras o en los sistemas interconectados, ya que es uno de los activos más importantes de las organizaciones, asegurar la confidencialidad e integri-dad de los datos y de la información de determinados procesos críticos o sensibles, cuya pérdida, fuga o no disponibilidad de la información pongan en problemas a la organización.

Palabras clave: ISO, seguridad, información, automatización, riesgo, sistema.

ABSTRACT

The present work aims to describe the requirements for the implementation and the necessary documentation of an Informa-tion Security Management System (ISMS). Automation consists of the availability of a template with internal control questions focused on the 3 pillars of information se-curity (confidentiality, integrity, availability) that allows a "Gap-Analysis" to be carried out to meas-ure the level of current maturity with respect to the requirements of the international standard ISO / IEC 27001: 2013, with a radar diagram and thus establish an ISMS or carry out the ISO 27001 certification process that guarantees to minimize risk and protect information on computers or in interconnected systems, since it is one of the most important assets of organizations, ensuring the confidentiality and integrity of the data and information of certain critical or sensitive processes, whose loss, leakage or unavailability of information puts problems in the organization.

Keywords: ISO, security, information, automation, risk, system.

INTRODUCCIÓN

La información es un medio intangible. García (2020), menciona que *"la inversión en activos intangibles conduce a un gasto con retorno a futuro, contribuyendo a la llamada economía del conocimiento"* (p.1). Los activos intangibles generar mucho valor económico para las empresas, en la era de los datos, la información tiene mucho valor ya que generan productividad, amplían las ventas y disminuyen los costos por reducir el tiempo de utilidad de dicha información en la producción.

De acuerdo a Bosch & Bosch-Sijtsema (2010), el Sistema de Gestión de Seguridad de la Información (SGSI) es *"el elemento más importante de la norma ISO 27001, que unifica los criterios para la evaluación de los riesgos asociados al manejo de la información institucional".* El SGSI pretende salvaguardar la confidencialidad, integridad y disponibilidad de la información.

Toda organización y persona natural valora los datos y toda la información acumulada a lo largo de su trabajo o actividad económica, es por eso que, para su manejo, mal uso o posible pérdida es imprescindible el uso de mejoras continuas y normativas que eviten o restrinjan los riesgos.

Las normativas deben estar al alcance no solo de las organizaciones, sino también de las personas que a diario podemos estar expuestas a riesgos de mal uso de nuestra privacidad, cuentas electrónicas, redes sociales, etc.

En el presente trabajo se describen los lineamientos de la norma ISO 27001 para implementar un Sistema de Gestión de Seguridad de la Información y el desarrollo de una herramienta digital que permita medir el grado de madurez de seguridad con respecto a la norma ISO 27001.

La seguridad es un instinto natural Lucio Vásquez (2020), menciona que *"el deseo de seguridad de los hombres frente a los peligros que representan la naturaleza, sus semejantes, los estados y últimamente la tecnología, han sido una base fundamental en la formación de entidades políticas".* La seguridad en la actualidad necesita ser altamente eficiente, una mayor conciencia sobre los riesgos ayuda en la toma de decisiones, los riesgos pueden ser identificados, evaluados y atenuados. El conocimiento es la clave para mantener políticas de seguridad efectivas y buenas prácticas de prevención de riesgos con enfoques de mejora continua y por ello la implementación un Sistema de Gestión de la Seguridad de la Información es imprescindible en las organizaciones.

Los riesgos y los delitos informáticos han evolucionado al mismo ritmo de la tecnología. Por lo cual el manejo de seguridad de la información es un compromiso de las organizaciones altamente comprometidas y responsables con sus datos y prestigio. Por tanto, se plantea como objetivo es diseñar y desarrollar plantillas digitales de una Matriz de riesgos, un Gap-Analysis o análisis de brechas y un Modelo de Control, mediante un estudio de campo adecuado en empresas que mantienen buenas prácticas de mejora continua sobre Sistemas de Gestión de Seguridad de la Información de acuerdo a la normativa ISO 27001.

MATERIALES Y MÉTODOS

La seguridad de la información de acuerdo a Disterer (2013), *"el Sistema de Gestión de Seguridad ISO 27001 busca proteger la información y de los sistemas de información del acceso, divulgación o destrucción no autorizada".*

La seguridad y la privacidad es muy importante y para TECON (2019), *"por seguridad de la información se entiende el conjunto de medidas preventivas y reactivas que permiten resguardar y proteger la información".* El tratamiento adecuado de los datos y de la información es muy imprescindible en la actualidad, ya que la información es un bien inmaterial invaluable y por lo tanto su tratamiento, manejo aseguramiento tiene que ser prioritario en cualquier organización. La tríada de seguridad de la información se muestra en la Figura 1.

Figura 1. Tríada CIA.

Confidencialidad: de acuerdo a Digital Guide (2020), *"solo los usuarios y procesos autorizados pueden acceder y modificar los datos"* (p.1). La información no debe llegar a personas que no estén autorizadas.

Integridad: los datos deben mantenerse en un estado correcto y nadie debe poder modificarlos de manera incorrecta, ya sea accidental o maliciosamente". Proteger la información frente a vulnerabilidades externas o internas o posibles errores humanos.

Disponibilidad: la disponibilidad es para *"los usuarios autorizados pueden acceder a los datos siempre que lo necesiten".* Acceso a la información por personal autorizado, tomando en cuenta la privacidad.

Petersen, et al. (2015), plantean que *"según los profesionales en seguridad de ISACA (Information Systems Audit and Control Association) la ciberseguridad se define como una capa de protección para los archivos de información".* Es la seguridad informática y busca proteger la información digital en los sistemas interconectados.

La seguridad informática asocia temas en un contexto menor tales como: ataques informáticos, virus, Spam, análisis de vulnerabilidad, Firewall, contraseñas, entre otros. Este concepto es fundamentalmente técnico, dando importancia a los sistemas de información, las redes y la infraestructura netamente tecnológica, así como a los ordenadores. La vulnerabilidad de un sistema de información, computadoras, redes y equipos se indica en la Figura 2**.**

Figura 2. Diagrama de Vulnerabilidad.

Sistema operativo: es importante actualizar el sistema operativo de manera periódica, de acuerdo a Sites (2019), *"se recomienda activar las actualizaciones automáticas para poder recibir los parches de seguridad de forma automática".* Las actualizaciones pueden solucionar pequeños daños o defectos e incluso problemas graves de seguridad.

Antivirus: Sites (2019), afirma que *"se recomienda instalar solo un Antivirus, así como un Anti-Spam en su ordenador, actualizarlo semanalmente, y analizar las unidades locales y externas periódicamente".* Los antivirus protegen los equipos o sistemas informáticos.

Copias de seguridad: de acuerdo a Silva, et al. (2016), *"la copia de seguridad, también llamada respaldo o backup, se refiere a la copia de archivos físicos o virtuales o bases de datos a un sitio secundario para su preservación en caso de falla del equipo u otra catástrofe".* La información digital es más valiosa para las empresas, ya que constituyen los respaldos de su actividad e información vital para su razón de ser. Por tal motivo realizar copias de seguridad de manera regular garantiza el resguardo de dicha información. La rapidez de la generación de los respaldos, depende de la información más crítica o relevante.

La frecuencia de pruebas de copias de seguridad debe alinear sus pruebas de copia de seguridad con la frecuencia de los respaldos. Entonces la información constituye un activo de TI, el cual estará listo para su utilización en una emergencia.

Seguridad de software: según Petersen, et al. (2015), *"la seguridad de software se utiliza para proteger el software contra ataques maliciosos de hackers y otros riesgos, de forma que nuestro software siga funcionando correctamente con este tipo de riesgos potenciales".* En el año 2001 los expertos en seguridad recién investigaron de manera ordenada como construir un sistema seguro. Además, existen defectos de software que es importante también evaluar al momento de optar por software, ya que existe mayor riesgo en aplicaciones que tienen salida a internet.

Es importante aplicar seguridad en el ciclo de vida del desarrollo del software a nivel de seguridad, debemos considerar a los productos software como entes vivos en constante cambio para corregir vulnerabilidades, añadir controles y adaptarse a las regulaciones y amenazas cambiantes.

Actualmente los negocios y actividades digitales generan millones de dólares en ganancias a través del uso de software apropiados para el uso estratégico, pero a la vez también pierden mucho dinero por robos y daños por ataques criminales, por lo tanto, es altamente importante garantizar que el negocio siga siendo rentable. En las distintas fases del ciclo de vida de desarrollo del software se debe cumplir un marco legal, así como también ciertas políticas de seguridad. El desarrollo de un software también debe ser seguro durante su ciclo de vida, se muestra en la Figura 3.

Figura 3. Ciclo de vida de Desarrollo Seguro de Software.

Seguridad de red: de acuerdo a Cisco Umbrella (2020), la seguridad de la red es *"cualquier actividad diseñada para proteger el acceso, el uso y la integridad de la red y los datos corporativos".* La seguridad de la red, requiere la seguridad de cada capa y se lo debe hacer tanto en software como en hardware, el software tendrá que ser actualizado de manera frecuente para proteger los datos de diversas amenazas, entonces un sistema de seguridad de red tiene muchos componentes.

Para mejorar la seguridad, los componentes trabajan de manera conjunta. Algunos de esos componentes son:

- Antivirus y antispyware.
- Cortafuegos, para bloquear el acceso no autorizado a la red.
- Sistemas de Prevención de intrusiones (IPS).
- Redes privadas virtuales (VPN).

Navegación en Internet: actualmente la navegación en internet es tan común por cualquier dispositivo y para Cisco Umbrella (2020), *"cuándo navegamos siempre queremos e intentamos en toda medida conservar nuestra privacidad y nuestros datos intactos".* Se recomienda evitar sitios web de confiabilidad dudosa, uso de tarjetas en compras por internet, Descargar aplicaciones en sitios oficiales, evitar enlaces poco confiables.

Contraseñas: en el ordenador, en las redes sociales y en otros servicios en línea se guarda mucha información personal. Bosch & Bosch-Sijtsema (2010), mencionan que *"no sólo guardamos fotos y videos de nuestros viajes, sino que también almacenamos allí muchos datos privados de índole comercial, como números de tarjetas de crédito y demás. Es por ello que las contraseñas deben ser seguras y fuertes".* Las contraseñas permiten autentificar a los usuarios en cualquier servicio que lo requiera. Entonces se recomienda crear una buena contraseña que contenga letras, números y símbolos.

Correo electrónico: para Digital Guide (2020), *"los spambots, o programas "caza-correos", recorren Internet de forma incesante a la búsqueda de direcciones de correo que más tarde podrán utilizar para acciones de publicidad agresiva, para enviar phishing o para distribuir todo tipo de malware"* (p.1). Es evidente que nuestra información cada vez está más expuesta y puede ser utilizada en otros beneficios, entonces será necesario implementar mayores controles de seguridad.

Firewall: de acuerdo a Cisco Umbrella (2020), un cortafuegos es *"un sistema de seguridad para bloquear accesos no autorizados a un ordenador mientras sigue permitiendo la comunicación de tu ordenador con otros servicios autorizados. También se utilizan en redes de ordenadores, especialmente en intranets o redes locales".* Constituye una de las primeras medidas en cuanto a seguridad y su creación e implementación se dio tras el origen del internet, ya que se necesitaba un mayor desarrollo de seguridad de acuerdo a la evolución de la tecnología.

Redes Sociales: a consecuencia de la pandemia ocasionada por el Covid-19 las redes sociales han tenido un uso masivo y no solamente para pasar el tiempo, sino también para trabajar, estudiar y para impulsar los negocios. Muchos han descubierto internet a consecuencia de la COVID, para bien o para mal, o bien se han visto obligados a usar la red de redes. Con el uso global de las redes es necesario estar preparados ante las amenazas y no compartir información confidencial, ya que los fraudes y suplantaciones de identidad son las principales amenazas con las que se puede encontrar.

Red LAN: las redes LAN brindan soluciones eficientes en la transmisión de información entre ordenadores. Las redes inalámbricas son bastante populares en la actualidad, siendo muy atractivas para los atacantes, ya que es muy fácil intentar conectarse silenciosamente.

En la figura 4 se muestra la seguridad de una Red LAN.

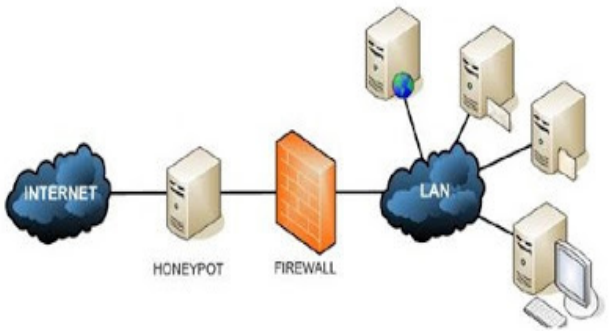

Figura 4. Seguridad de una Red LAN.

Luego de haber identificado y clasificado los riesgos, es importante analizarlos según explica Disterer (2013), *"se estudian la posibilidad y las consecuencias de cada factor de riesgo con el fin de establecer el nivel de riesgo de nuestro proyecto".* El análisis del riesgo determina los factores de riesgo potencialmente peligrosos y con mayor efecto en nuestros datos o información, por lo cual deberán ser gestionados de manera prioritaria.

Hangzhou Hikvision Digital Technology Co. (2016), afirma que para *"el análisis y gestión de los riesgos previene a las empresas de este tipo de situaciones negativas para su actividad y recoge una serie de factores fundamentales para su consecución"* (p.1). Para eso será indispensable identificar todos los activos de la empresa, en los cuales se incluyen los recursos afines a la gestión de la información en la empresa (software, hardware, comunicación, documentación digital, manuales y recursos humanos).

Cuando se identifican todos los activos de la información que tenga la empresa, es necesario identificar las amenazas a las que se puede estar expuestos como se muestra en la figura 5.

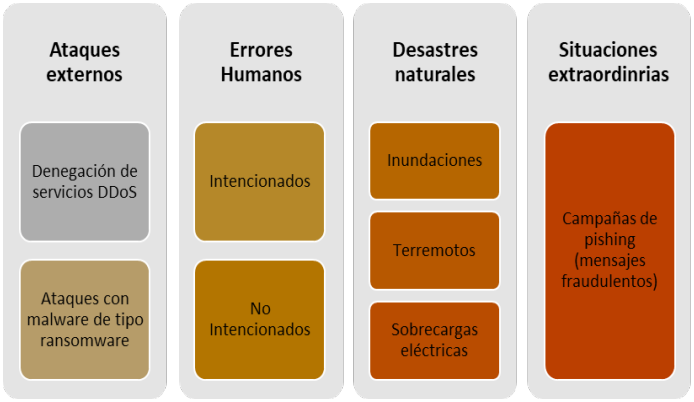

Figura 5. Riesgos y amenazas.

Las ventajas de la transformación digital también están acompañadas de amenazas que ponen en riesgo la seguridad y además la privacidad se ve altamente afectada. Los ciberdelincuentes siguen evolucionando con el objetivo de robar información.

Las empresas siempre deben analizar los riesgos informáticos para tomar medidas que logren evitar efectos negativos o a su vez mitigar los efectos. El diagrama de análisis de riesgos se muestra en la Figura 6.

Figura 6. Análisis de riesgos.

Con la globalización y con las nuevas tecnologías nuestros datos personales circulan por la red sin ningún tipo de control. Es por eso que en Europa se ha publicado el Reglamento General de Protección de Datos (RGPD), que es una normativa a seguir para el tratamiento de datos personales y cuyo objetivo es proteger el derecho de las personas físicas, con el fin de preservar su información (Bosch & Bosch-Sijtsema, 2010).

Razones para realizar el análisis. – Los avances tecnológicos y los delitos informáticos son cada vez más frecuentes y la información personal, así como los datos empresariales son vulnerables.

Describir flujos de información:es el proceso que debe seguirse para establecer las medidas de seguridad.

Identificar los riesgos: es el plan de gestión de riesgos, en el cual se pueden incluir: alcance, cronograma, costos, nivel de calidad. En este proceso la identificación puede ser temprana, reiterada, emergente, extensa y proporcionada.

Establecer soluciones: una vez que hemos identificado los riesgos para la privacidad, tal y como hemos descrito en el punto anterior, lo más lógico es desarrollar las medidas correspondientes para eliminar o mitigar dichos riesgos.

Implementar soluciones: luego de obtener las conveniencias necesarias que garanticen la privacidad, es momento de tomar la decisión cuáles de ellas implementamos, ya que como se ha comentado anteriormente, no necesariamente hay que poner en funcionamiento todas. La empresa puede adjudicarse determinados riesgos, siempre y cuando sean considerados como tolerables. Sin embargo, pueden existir riesgos que no se puedan eliminar.

Participación de los agentes implicados: en cualquier fase del análisis de riesgos debe fluir la información en todos los niveles de la organización. Interno y externo, para saber la opinión de los afectados y dar transparencia a la información entre usuarios y consumidores.

Integrar análisis de riesgos: para garantizar la privacidad de productos y servicios. "*Todas las empresas, sin excepción, deben analizar las vulnerabilidades informáticas y potenciales brechas de seguridad lógica con el fin de seleccionar e implementar las mejores soluciones informáticas destinadas a impedir, bloquear o neutralizar los ataques"*. También se puede implementar un Plan Director de Seguridad (PDS) que consta de 6 fases como se indica en Figura 7.

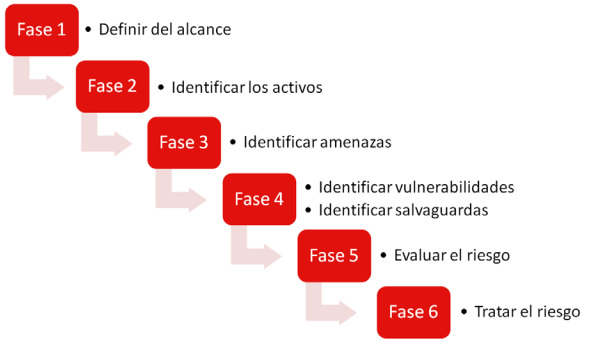

Figura 7. Etapas de un Análisis de Riesgo.

Velando (2019), afirma que la Organización Internacional de Normalización, está *"integrada por más de 160 países"* (p.15). La función de ISO es normar productos y servicios, las normas son optativas.

El uso de un Sistema de Gestión de Seguridad de la Información (SGSI), es para "a través de un enfoque sistémico… preservar la confidencialidad, integridad y disponibilidad de la información". (Velando, 2019)

El Anexo SL proporciona una nueva estructura, denominada de Alto Nivel, para los sistemas de gestión ISO- sustituye a la histórica Guía 83 de la ISO (Conislla, 2020). El anexo SL fue creada para implantar un texto base idéntico con cláusulas y definiciones comunes. Con SL permite:

Optimizar las normas.

Fomentar la certificación.

Facilitar la integración de los sistemas de gestión.

La estructura alineada a Anexo SL se muestra en la figura 8.

Figura 8. Etapas de un Análisis de Riesgo.

De acuerdo al ciclo de mejora continua, un Sistema de Gestión está formado por 4 fases, para reducir al mínimo los riesgos de la información es necesario la implementación de forma constante. En la Figura 9 se muestra las fases del sistema de gestión.

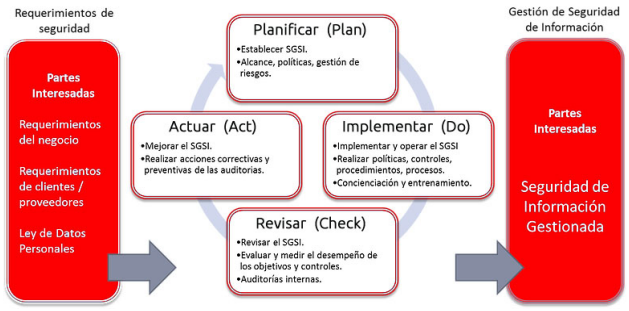

Figura 9. Fases del Sistema de Gestión.

» **Planificar**: establecer los objetivos de seguridad de la información, para determinar los controles adecuados (catálogo de posibles controles).

» **Implementar**: aplicar todo lo establecido en la fase anterior.

» **Revisar**: comprobar y verificar si el funcionamiento y los resultados cumplen lo determinado.

» **Actuar**: para mejorar los incumplimientos que han sido detectados en la fase de revisión.

Disterer (2013), menciona que *"el cumplimiento de esta norma es una decisión estratégica apoyada por la dirección, debe existir un compromiso firme para establecer una política y asignar recursos necesarios para su cumplimiento".* El principal objetivo es proteger la información para evitar que caiga en las manos equivocadas o se pierda, ya que las amenazas pueden ser externas o internas y pueden ser de maliciosas o accidentales.

La Organización Internacional de Estandarización acopia un número extenso de normas en la familia ISO 27000, como se muestra en la Tabla 1.

Tabla 1. Familia ISO.

N°	ISO	Función
1)	27000:2018	Fundamentos y Vocabulario
2)	27001:2013	Norma Principal
3)	27002:2013	Buenas Prácticas
4)	27003:2017	Guía de Implementación
5)	27004:2016	Métricas y Mediciones
6)	27005:2018	Gestión de Riesgos
7)	27006:2015	Esquema de Certificación
8)	27007:2017	Guía de Auditoría al SGSI
9)	27008:2011	Guía de Auditoría a los Controles
10)	27032:2012	Lineamientos de Ciberseguridad

La ISO 270001 es la norma ISO que establece los requerimientos para implementar, mantener y mejorar un SGSI y en la actualidad es el único estándar aceptado a nivel internacional para la gestión de la Seguridad de la Información.

La ISO actualmente ha ido evolucionando gracias a normas y buenas prácticas que han permitido a las empresas administrar apropiadamente la seguridad de la información. ***"La ISO 27001 como la conocemos hoy en día, ha sido resultado de la evolución de otros estándares relacionados con la seguridad de la información".*** (Petersen, et al., 2015).

Un sistema de Gestión de Seguridad de la Información (SGSI) constituye ***"el medio más eficaz de minimizar los riesgos, al asegurar que se identifican y valoran los activos y sus riesgos, considerando el impacto para la organización"*** (Valdez, 2015). La estrategia de negocio consiste en adoptar controles y procedimientos eficaces para la empresa.

ISO/IEC 27001:2013 = NTP ISO/IEC 27001:2014. Permite reforzar la seguridad de la información y disminuir los riesgos de fraude, así como la pérdida o filtración de información.

Algunos beneficios de la Norma ISO/IEC 27001

» Identificar los riesgos y establecer controles para gestionarlos o eliminarlos.

» Confidencialidad, asegurando que sólo quienes estén autorizados puedan acceder a la información.

» Flexibilidad para adaptar los controles a todas las áreas de la empresa o solo a algunas seleccionadas.

» Conseguir que las partes interesadas y los clientes confíen en la protección de los datos.

» Demostrar conformidad y conseguir el estatus de proveedor preferente.

» Alcanzar las expectativas demostrando conformidad.

En las normas para la evaluación de la seguridad de la información se incluye dos partes:

ISO/IEC 27001:2013, describe los requisitos para la implementación y la documentación necesaria de un Sistema de Gestión de Seguridad de la Información (SGSI). Constituye:

» Tecnología de la Información.

» Técnicas de Seguridad.

» Sistemas de Gestión de Seguridad de la Información.

» Requisitos.

ISO/IEC 27002:2013, es el documento de referencia para las mejores prácticas de un SGSI, en donde contienen las instrucciones para la implementación.

La propuesta

Objetivo: Facilitar la comprensión de los requerimientos necesarios para la implementación de un Sistema de Gestión de la Seguridad de la Información mediante el uso de un repositorio digital.

Diseño de plantillas

Objetivo:

Fomentar el trabajo colaborativo a través del intercambio de información que permita desarrollar la capacidad reflexiva de los estudiantes de TI sobre la importancia de la implementación de un SGSI en una organización.

Matriz de Riesgos

La plantilla de la Matriz de riesgos se la realizó en Excel, tomando en cuenta las características necesarias de diseño sencillo, flexible para documentar y evaluar los diversos procesos, así como los riesgos de manera general. En la Figura 10 se muestra un ejemplo de plantilla para Matriz de riesgos.

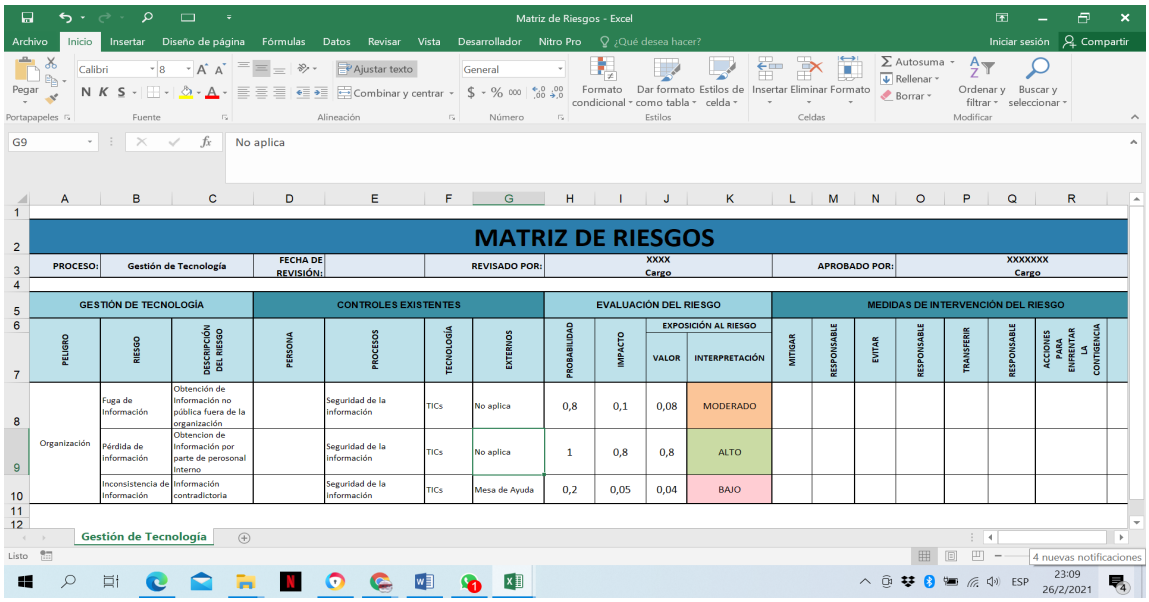

Figura 10. Matriz de Riesgos.

GAP Analysis

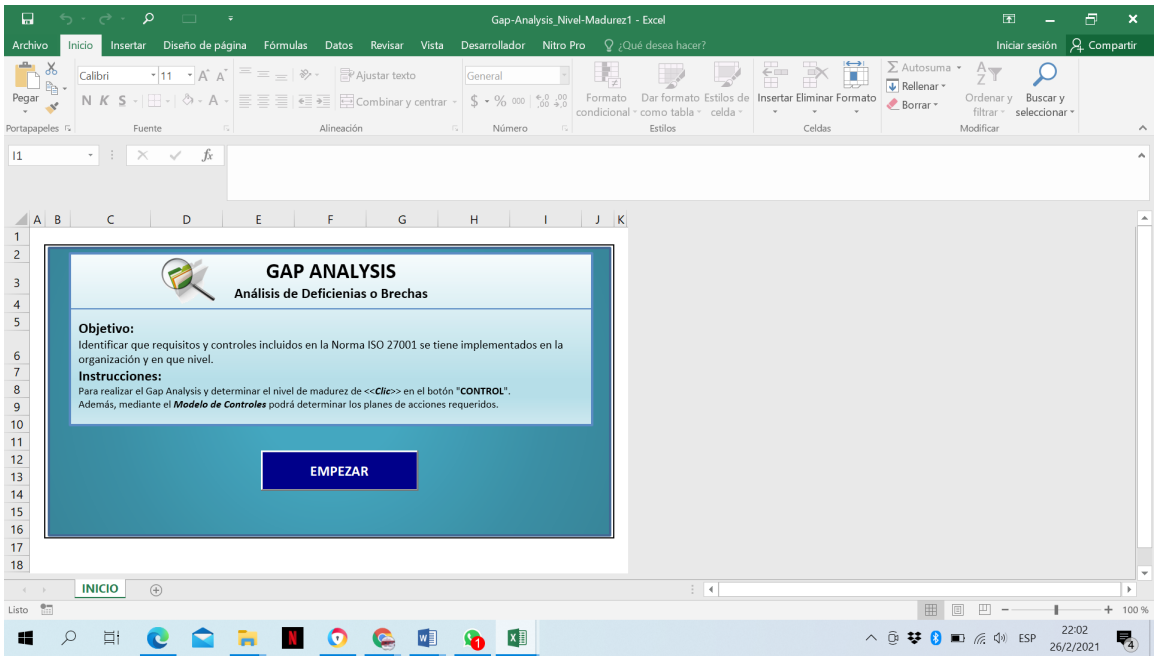

Figura 11. Plantilla de GAP-Analysis.

La plantilla del Gap-Analysis o análisis de brecha se los realizó en Excel mediante macros con un menú y botones de navegación. es un servicio que permite identificar la distancia existente entre la organización actual de la seguridad de la información en la empresa y las buenas prácticas más reconocidas en la industria. En la Figura 11 se muestra el Menú de la plantilla ejemplo para realizar un Gap Analysis.

Al dar <<Clic>> en el botón "Empezar" inmediatamente irá a la hoja "Control" en donde encontrará una tabla con preguntas de control acordes a Anexo A de ISO 27001, el cumplimiento se mide en 5 niveles:

0 “Inexistente”

1 “Inicial”.

2 “Ejecutado”.

3 “Definido”.

4 “Administrado”.

5 “Optimizado”.

Una vez que se haya llenado todas las celdas al dar <<Clic>> en el botón “Resultados” le dirigirá a la siguiente hoja. En la figura 12 se muestra la plantilla ejemplo de la matriz de control.

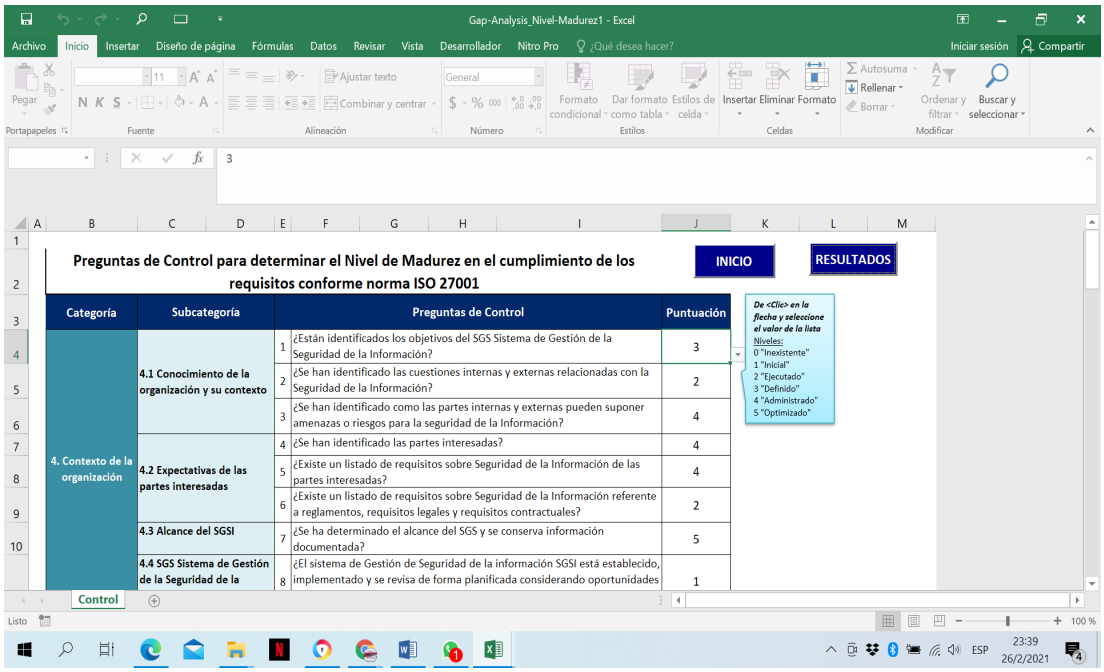

Figura 12. Preguntas de Control.

La siguiente hoja de la plantilla muestra el resumen y los resultados de acuerdo a las respuestas de la Matriz de Control, además en la hoja “Resultados” se encuentran los botones:

“Inicio” para volver a la pantalla “Menú”

“Gráfico” para mostrar el gráfico de resultados

“Control” para volver a la matriz de control

“Gap Analysis” para mostrar los resultados del análisis de brechas.

En la figura 13 se muestra la hoja “Resultados”.

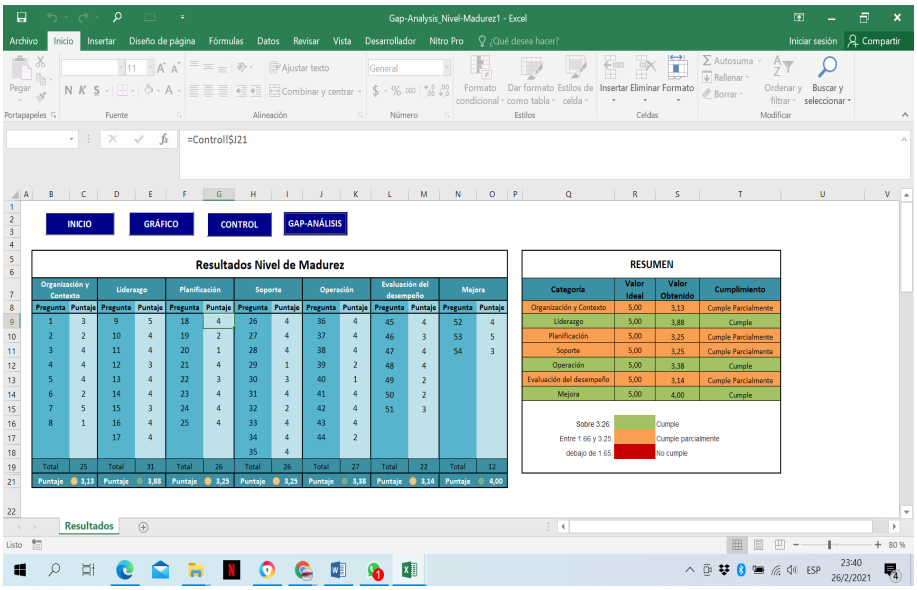

Figura 13. Resultados y Resumen.

Al dar <<Clic>> en "Gráfico" inmediatamente se visualiza el gráfico del análisis de brechas, como se muestra en la Figura 14.

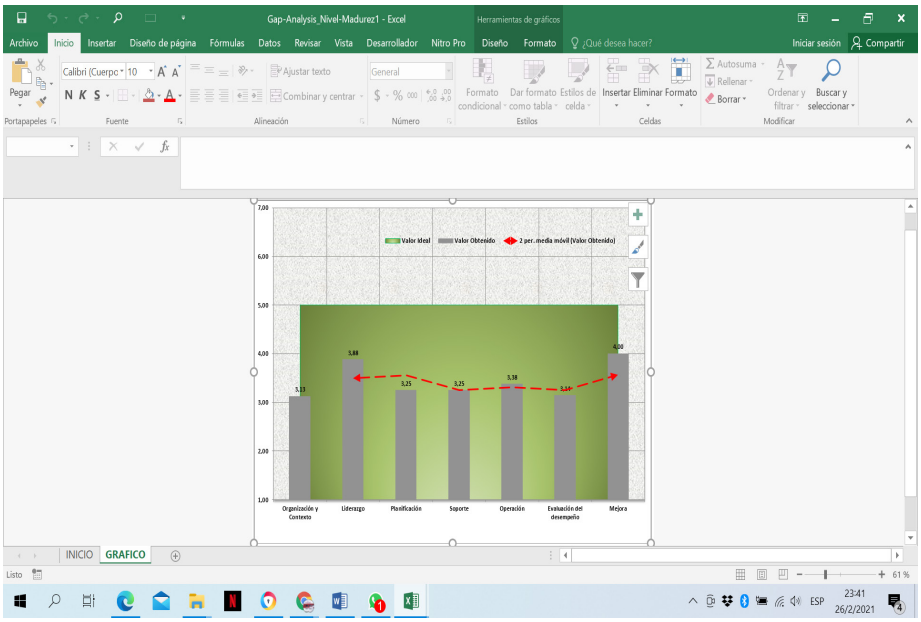

Figura 14. Gráfico de Análisis de Brechas.

Al dar <<Clic>> en "Gap Análisis" inmediatamente se visualiza el análisis de brechas y las acciones a realizar acorde a los resultados obtenidos, los resultados del nivel de madurez se evalúan de la siguiente manera:

» Sobre 3,26 "Cumple"

» Entre 1,66 y 3,25 "Cumple Parcialmente"

» Bajo de 1,66 "No Cumple"

De acuerdo al nivel de madurez las acciones a considerar serán:

» No Cumple Acción: “Superar”

» Cumple Parcialmente Acción: “Mejorar”

» Cumple Acción: “Potenciar”

En la figura 15 se muestra un gráfico en Radar con los valores ideales y reales, además las acciones generales que deberían realizarse en los planes de acción o estrategias de mejora continua.

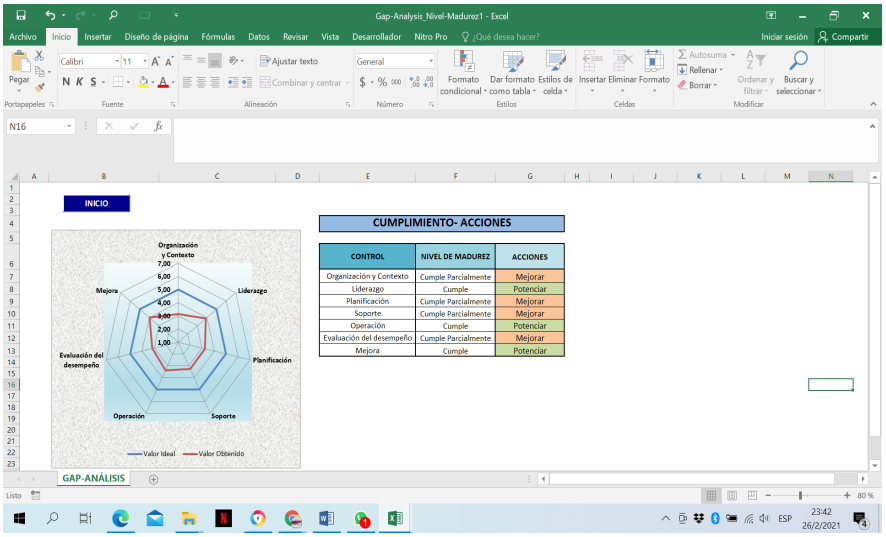

Figura 15. Gráfico en radar del Análisis de Brechas.

Modelo de Controles

La plantilla de modelo de Controles se realizó en Excel tomando en cuenta los pilares de ISO27001, el modelo de controles permite establecer planes de acción como estrategias de mejora continua. En la figura 16 se muestra la plantilla ejemplo del Modelo de Controles.

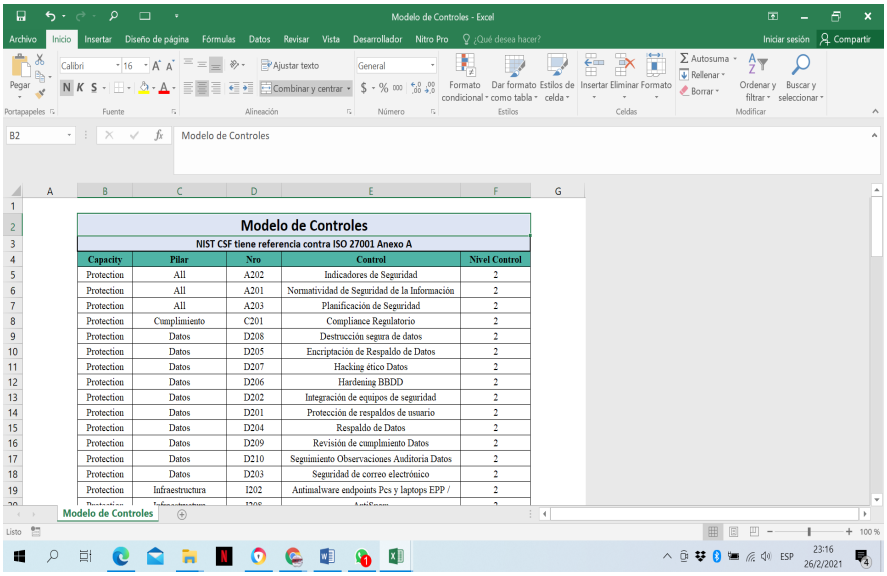

Figura 16. Modelo de Controles.

CONCLUSIONES

En el estudio se recopiló información sobre ISO/ SGSI y estructura estándar internacional ISO/IEC 27001 para implementar un SGSI (Sistema de Gestión de Seguridad de la información). Esto se verifica en el marco teórico en el cual se consideran 10 fases.

En la página Web: https://bryangsk8.wixsite.com/my-site se presentó las plantillas de Matriz de Riesgos, Gap Análisis y Modelo de Control de un SGSI basado en la normativa ISO 27001. Entonces se concluye que se cumplió con el segundo objetivo específico.

Se diseñaron y desarrollaron 3 plantillas en Excel sobre matriz de riesgos, Gap Análisis y Modelo de Control de un SGSI basado en la normativa ISO 27001.

REFERENCIAS BIBLIOGRÁFICAS

Bosch, J., &. Bosch-Sijtsema, P. (2010). From integration to composition: On the impact of software product lines global development and ecosystems. ***Journal of Systems and Software***, 83(1), 67-76.

Cisco Umbrella. (2020). ***¿Qué es la seguridad de red?*** https://www.cisco.com/c/es_mx/products/security/what-is-network-security.html

Digital Guide. (2020). ***Correo electrónico: asegura tu información - IONOS.*** https://www.ionos.es/digitalguide/correo-electronico/seguridad-correo-electronico/

Disterer, G. (2013). ISO/IEC 27000 27001 and 27002 for information security management. ***Journal of Information Security***, 4, 92-100.

García, G. (2020). ***Activos intangibles: qué son y cómo ayudan a tu empresa?*** https://www.sage.com/es-es/blog/activos-intangibles-ayudar-empresa/

Google Sites. (2019). ***Reglas Básicas de Seguridad Informática - Seguridad Informatica y Web.*** https://sites.google.com/site/seguridadinformaticayweb/reglas-basicas-de-seguridad-informatica

Lucio Vásquez, A. G. (2020). Evolución del concepto de seguridad en la República del Ecuador: desde una perspectiva de seguridad nacional hacia la seguridad integral. ***Relaciones Internacionales***, (43), 171–188.

Petersen, K., & Vakkalanka, S., & Kuzniarz, L. (2015). Guidelines for conducting systematic mapping studies in software engineering: An update. ***Information and Software Technology***, 64.

Silva, L., Hsu, C., Backhouse, J., & McDonnell, A. (2016). Resistance and power in a security certification scheme: the case of c: cure. ***Decision Support Systems, 92, 68-78.***