Revista Logos Ciencia & Tecnología, 16(3), 62-87 | Septiembre-diciembre, 2024
https://revistalogos.policia.edu.co:8443/index.php/rlct

Artículos de investigación

Revista Logos Ciencia & Tecnología
ISSN 2422-4200 (en línea)

Implementación de un *roadmap* para asegurar la información en los desarrollos de aplicaciones en línea

Implementation of a roadmap to ensure information in the development of online applications

Implementação de *roadmap* para proteger informações em desenvolvimentos de aplicativos on-line

José Luis Unás Gómez [a] | Royer David Estrada Esponda [b, *] | Luis Germán Toro Pareja [c]

a https://orcid.org/0000-0001-6359-3104 Universidad del Valle, Tuluá, Colombia

b https://orcid.org/0000-0002-6849-1278 Universidad del Valle, Cali, Colombia

c https://orcid.org/0000-0002-4916-7536 Universidad del Valle, Tuluá, Colombia

- Fecha de recepción: 21/06/2024
- Fecha concepto de evaluación: 30/08/2024
- Fecha de aprobación: 22/09/2024
https://doi.org/10.22335/rlct.v16i3.1967

Para citar este artículo/To reference this article/Para citar este artigo: Unás, J. L., Estrada, R. D., & Toro, L. G. (2024). Implementación de un roadmap para asegurar la información en los desarrollos de aplicaciones en línea. *Revista Logos Ciencia & Tecnología, 16*(3), 62-87. https://doi.org/10.22335/rlct.v16i3.1967

RESUMEN

Este artículo presenta un *roadmap* para el control de los datos de la información en los ámbitos de desarrollo de aplicaciones de software para las grandes, medianas y pequeñas empresas de desarrollo de aplicaciones en línea, las cuales son vulnerables por la falta de controles o políticas que permitan la protección de la información de ataques no deseados y exposición de información sensible. Se implementó una metodología de investigación con base en la norma de la Organización Internacional de Estandarización ISO 27001; las características de Objetivos de Control para la Información y Tecnologías Relacionadas con las metodologías COBIT y Magerit para el diseño de un Sistema de Gestión de la Seguridad de la Información (SGSI), que asegure la información de los clientes en los desarrollos de aplicaciones en línea. Con la presentación de la metodología de desarrollo se han utilizado datos de control y experimentales para asegurar la información, logrando elevar su nivel de seguridad y madurez de la empresa, y se busca con ello garantizar los tres pilares de la seguridad de la información: integridad, disponibilidad y confidencialidad.

Palabras clave: gestión de la seguridad, COBIT, asegurar información, sistemas en línea, *roadmap*.

ABSTRACT

This article presents a roadmap for the control of information and data in the areas of software application development for large, medium, and small online application development companies, which are vulnerable due to the lack of controls or policies that allow the protection of information from unwanted attacks and the exposure of sensitive information. A research methodology was implemented based on the International Organisation for Standardisation ISO 27001, the characteristics of Control Objectives for Information and Related Technologies COBIT and the Magerit methodology for the design of a Computer Security Management System (ISMS),

*Autor de correspondencia. Correo electrónico: royer.estrada@correounivalle.edu.co

which protects customer information in online application developments. With the presentation of the development methodology, control and experimental data have been used to secure information, managing to raise the level of security and maturity of the company, thereby seeking to guarantee the three pillars of information security: integrity, availability, and confidentiality.

Keywords: Security management, COBIT, securing information, online systems, roadmap.

RESUMO

Este artigo apresenta um *roadmap* para o controle de dados de informações nos domínios de desenvolvimento de aplicativos de software para grandes, médias e pequenas empresas de desenvolvimento de aplicativos on-line, as quais são vulneráveis devido à falta de controles ou políticas que permitam a proteção das informações contra os ataques indesejados e exposição de informações confidenciais. Uma metodologia de pesquisa foi implementada com base na norma ISO 27001 da Organização Internacional de Normalização; nas características dos objetivos de controle para informações e tecnologias relacionadas com as metodologias COBIT e Magerit para o projeto de um Sistema de Gestão da Segurança da Informação (ISMS), que protege as informações dos clientes no desenvolvimento de aplicativos on-line. Com a apresentação da metodologia de desenvolvimento, foram utilizados dados de controle e experimentais para proteger as informações, conseguindo elevar seu nível de segurança e a maturidade da empresa, e assim busca garantir os três pilares da segurança da informação: integridade, disponibilidade e confidencialidade.

Palavras-chave: gestão da segurança, COBIT, proteção de informações, sistemas on-line, *roadmap.*

Introducción

En la actualidad, las organizaciones de desarrollo de aplicaciones en línea manejan datos o información de tipo sensible y no sensible que pueden estar expuestas a las diferentes amenazas, que de materializarse pueden lograr un impacto negativo en cuestiones económicas, debido a demandas por parte de los afectados, multas por incumplimiento de requisitos legales y pérdida de la credibilidad. Las empresas están cada vez más preocupadas por este aspecto y su aplicabilidad en los procesos en cuanto a la seguridad de la información, "hacen enormes esfuerzos e inversiones económicas en plataformas o sistemas de información con el objetivo de ser más eficientes, más seguras, cumplir con su misión y con los aspectos claves de su planeación estratégica" (Muñoz Periñán & Ulloa Villegas, 2011, p. 24). De ser un gasto innecesario, se ha convertido en una inversión para las diferentes organizaciones, con el objetivo de proteger y asegurar el activo más importante: la información de los clientes.

En el tiempo actual, las amenazas se han posicionado como elementos de la cotidianidad y de la existencia organizacional, las cuales se pueden ver reflejadas en diferentes formas: físicas (robo hormiga) y en entornos digitales como virus que ponen en peligro la identidad de las personas o sistemas, a través de ataques como el secuestro de datos (en inglés, *ransomware*) y día cero (en inglés, *zero-day attack*).

Hoy en día, las organizaciones y sus sistemas de información están expuestos a diferentes números de amenazas, "causa un incidente no esperado u ocasionado y puede resultar en un daño o deterioro de un sistema u organización y/o activos"(Bautista Torres, 2012, p. 5). Tal es el caso, los ataques son muy transversales y podrían afectar el desarrollo de aplicaciones en línea, como son: técnica de propagación de códigos maliciosos conocidos como gusanos (*worm*), ingeniería social y amenazas relacionadas con fenómenos naturales que existen mediante el uso de actividades malintencionadas que se aprovechan de cualquier tipo de vulnerabilidades existentes, personal no capacitado en el tratamiento y protección de datos personales (Ley 1581 de 2012) y falta de validación de datos que afecta los diferentes activos sensibles en diversas situaciones de fraude, pérdida, fuga y desorganización de la información, que conlleva pérdidas económicas para el usuario y de credibilidad para la organización.

Además de lo anterior, se suman diferentes elementos que propician que los sistemas de información no sean seguros, dando como resultado que los datos propios y de terceros se vean involucrados en fugas de información o sean expuestos, convirtiéndolos en piezas fundamentales de vulnerabilidades por los virus informáticos, ingeniería social, el acceso ilegal, o los ataques de inyección "SQL", que son algunos de los ejemplos conocidos recientemente que podrían afectar a los desarrollos de software en línea. No obstante, se menciona que existen eventualidades de seguridad causados voluntaria o involuntariamente dentro de la organización o, en su defecto, por aquellos que son provocados por catástrofes naturales o fallas técnicas.

Por tanto, el flujo de información de los clientes por medio del uso de las tecnologías de la información y la comunicación (TIC), procesada en los diferentes ámbitos laborales, servicios transaccionales y uso de las redes sociales, puede ser susceptible de riesgos de seguridad como la extracción no autorizada de la información, la adulteración de datos y la presencia de entropía de acuerdo con la teoría de la información. Por ello, la oportuna implementación de un roadmap (hoja de ruta) que extraiga lo mejor de ISO 27001, COBIT y Magerit para la seguridad y las políticas operacionales correctas de esta, "[…] permite preservar la información para minimizar el impacto de la pérdida de confidencialidad, integridad y disponibilidad"(Andrés & Gómez, 2012, p. 10).

Por consiguiente, la seguridad de la información permite en su estilo poder mantener niveles aceptables de riesgos, tanto físicos como digitales, en los diferentes dispositivos tecnológicos que admiten cualquier tipo de clase de datos, desde la conectividad, el procesamiento, el acceso, la actualización, el almacenamiento, la transferencia y la presentación de la información.

En los más recientes estudios sobre el estado de la ciberseguridad a nivel mundial, se encontró un aumento del 48% al 53% de empresas que sufrieron ataques en el 2023 a escala mundial (Hiscox, 2023), registrándose con preocupación el aumento de ataques a empresas pequeñas (10 o menos empleados). Para el caso de América Latina, el *phishing* se sextuplicó y los troyanos bancarios aumentaron en 50%; Colombia se encuentra en el cuarto puesto en Latam de ataques, con 30 900 000 ataques en el 2023 (Kaspersky, 2023).

Durante la investigación, se relacionó la importancia de generar un roadmap de implementación que genere la protección de la información en los desarrollos de software para las empresas en aplicaciones en línea y sus pilares (confidencialidad, integridad y disponibilidad), implicando sus controles o políticas con el estándar según la norma ISO/IEC 27001; que es un marco de la gestión de seguridad con el objetivo de desarrollar reglas, guías de normalización en los diferentes ámbitos, en este caso la informática, en donde se establecen ciertas medidas de protección necesarias.

Estado del arte

En la investigación se utilizarán los estándares de la norma ISO/IEC 27001:2013, que definen los requisitos para un Sistema de Gestión de Seguridad Informática (SGSI). Asimismo, se continúa con la norma en el sistema de gestión para los documentos de la ISO 30301, y se considerará la ley de protección de datos colombiana, que menciona que los datos sensibles "[…] afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación"(Ley 1581 de 2012). Además, se aplicará la metodología COBIT (Objetivos de Control para la Información y las Tecnologías Relacionadas), cuyos principios o características incluyen: "efectividad, eficiencia, confidencialidad, integridad, disponibilidad, cumplimiento y confiabilidad de la información" (COBIT, 1996, p. 6). Esta metodología se basa en los recursos de la tecnología de la información (TI) para el conjunto de procesos que reúnen datos pertinentes en las organizaciones, con el fin de alcanzar las metas y la determinación del riesgo y su control, mediante la valoración de vulnerabilidades, amenazas y riesgos sobre la protección de los activos.

La norma ISO/IEC 27001:2013 establece las especificaciones para la creación, implementación, funcionamiento, supervisión, revisión, mantenimiento y mejora continua de un SGSI, con el propósito de preservar la confidencialidad, integridad y disponibilidad de los datos mediante un proceso de gestión de riesgo operados en las empresas.

Roadmap

Surgió de la industria y ha evolucionado a lo largo de las décadas, a través de mejoras y refinamientos realizados tanto por profesionales como por grupos de investigación, para convertirse en un método establecido y ampliamente implementado. Los roadmap, según Kerr y Phaal (2022), son populares para ayudar a transmitir y comunicar la esencia de las estrategias, los planes, las iniciativas organizacionales, las rutas de programas y perspectivas futuras mediante vías de acción. Pero ¿qué constituye realmente una hoja de ruta? ¿qué son los atributos únicos que los distinguen de otros mapas de viajes, enfoques y documentos comerciales con visión de futuro?

Aprovechando la participación en compromisos industriales, investigación aplicada, el desarrollo de herramientas y respaldado por la literatura, una hoja de ruta ahora se ha definido como una cronología visual estructurada de intención estratégica. Además, se ha determinado como la aplicación de una lente estratégica estructurada temporal y espacialmente.

Magerit

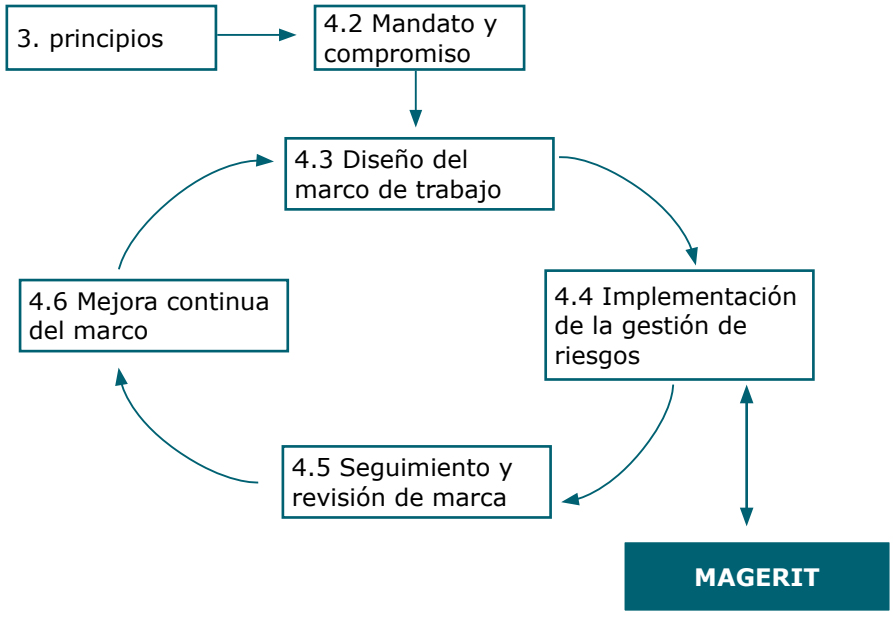
La metodología de análisis y gestión de riesgos (Ministerio de Hacienda y Administraciones Públicas, 2012) es un marco de trabajo (véase Figura 1), que tiene como objetivo tomar decisiones según los diferentes órganos de gobierno para minimizar los riesgos que son originados mediante el uso de las diferentes tecnologías de la información.

Con el ánimo de encontrar habilidades que ayuden a mejorar y gestionar de manera segura los sistemas de información en línea, la metodología Magerit permite mitigar o minimizar los diferentes riesgos que puede enfrentar en este nuevo reto de la protección de datos personales del siglo XXI.

Por tanto, para la investigación, se siguen ciertos elementos de la estructura de análisis de riesgos (identificación de activos y su clasificación, valoración de los activos, las amenazas, las vulnerabilidades y la probabilidad del peligro) que se alinean en la calificación y cuantificación, con el fin de conocer la realidad del estado de las empresas, a nivel de seguridad informática y los riesgos latentes a los que están expuestas. Y en función del autor Botero Vega (2016), se plantea que sigue ciertos elementos de la metodología Magerit y disminuye el impacto en relación con la variable y confirma que el problema funcionó.

Figura 1

ISO 310000. Marco de trabajo para la gestión de riesgo



Nota. El gráfico representa el marco de trabajo según Ministerio de Hacienda y Administraciones Públicas (2012)

Ciclo de Deming

La norma internacional para la seguridad de información ISO/IEC 27001:2013 realiza el respectivo análisis de procesos con el apoyo del ciclo PHVA (planificar, hacer, verificar y actuar), que es "una herramienta de mejora de larga trayectoria, muy utilizada, dado que la mejora continua no es solo un método para la resolución de problemas, sino también una forma de pensar orientada a los procesos" (Trías et al., 2019, pp. 22-23). El círculo de Deming para la mejora continua (véase Figura 2) se implementa aplicando las siguientes cuatro fases que se explican a continuación:

Planificar: realizar la planeación, establecer los objetivos y definir sus actividades.

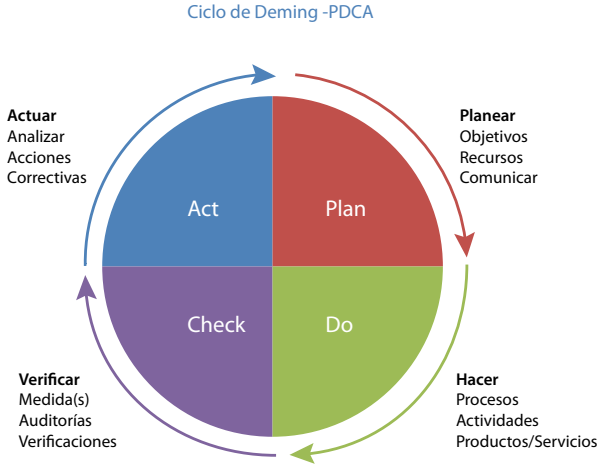
Hacer: llevar a cabo las acciones planeadas (actividades) para alcanzar los objetivos propuestos.

Verificar: seguimiento para conocer el avance y verificar su correcto funcionamiento en la consecución de los objetivos planeados.

Actuar: luego de analizar la verificación de las actividades, se examina si las mejoras son permanentes y se aplican las acciones correctivas que sean necesarias en caso de que los resultados no sean satisfactorios, con el fin de cumplir los objetivos.

Figura 2

Gestión por procesos del ciclo Deming

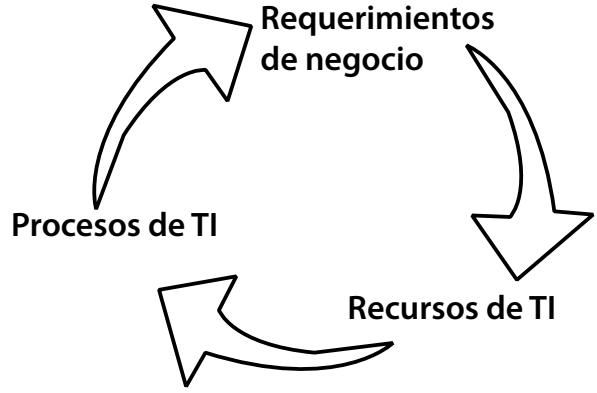


Nota. Adaptado del ciclo Deming, por (Ingeniería de Calidad, 2024)

Provee de un marco de trabajo integral que ayuda a las empresas a alcanzar sus objetivos para el Gobierno y la gestión de las tecnologías de la información (TI) corporativas. Ayuda a las empresas u organizaciones a crear el valor óptimo desde las TI, manteniendo el equilibrio entre la generación de beneficios y la optimización de los diferentes niveles de riesgo y el uso adecuado de los recursos. Este marco de trabajo COBIT 3 se basa en cinco principios claves para el Gobierno y de las TI empresariales (véase Figura 3).

Figura 3

Principios COBIT 3



Nota. Tomado de COBIT (1996, p. 14).

Dentro del marco de referencia de COBIT 3 edición, se hace alusión a siete características (efectividad, eficiencia, confidencialidad, integridad, disponibilidad, cumplimiento y confiabilidad de la información) para la protección de datos personales, tratados por la organización a nivel de codificación o desarrollo de software en recursos o sistemas en línea de la siguiente manera.

Para el proyecto, se tendrán en cuenta las características o principios de COBIT 3 para la protección de los datos personales que se procesarán en los recursos en línea. Las cuales son: efectividad, eficiencia, confidencialidad, integridad, disponibilidad, cumplimiento y confiabilidad de la información.

Trabajos relacionados

Así pues, se reseñan los principales documentos con sus autores de referencias en la construcción del roadmap; que sirvieron en el debido

proceso de la planificación y desarrollo en el componente metodológico de la investigación.

Mitigar las vulnerabilidades del software mediante el desarrollo de software seguro con un modelo en cascada basado en políticas

Este es un referente clave en las actividades de ingenieros y profesionales del software, ya que les permite crear aplicaciones de software seguras, utilizando el modelo en cascada impulsado por políticas (PDWM) y el ciclo de vida del desarrollo del software (SDLC); así pues, los autores Hussain et al. (2024) señalan que "el desarrollo seguro que pueda conducir a un software que tenga la capacidad de detectar programa maligno y anomalías en el proceso" (p. 2).

Asimismo, los autores presentan un enfoque dirigido a pequeñas y medianas empresas que desarrollan software en línea. A lo anterior, describen cómo el PDWM aborda los requisitos de seguridad y las prácticas específicas que se limitan en cada fase del SDLC, proporcionando orientación para mejorar la seguridad del software. Esto permite a las organizaciones identificar riesgos y vulnerabilidades, con el objetivo de reducir la exposición de los activos sensibles y lograr un sistema más confiable y seguro.

Metodología para la implementación de un SGSI en la Fundación Universitaria Juan de Castellanos, bajo la norma ISO 27001:2005

El presente trabajo de Alemán-Novoa (2015) consiste en aplicar la metodología PDCA ("planificar-hacer-verificar-actuar") para la construcción de un SGSI enfocado en los procesos universitarios en línea, con el objetivo de proteger los activos y salvaguardar los sistemas informáticos, tanto a nivel de software como de hardware, evitando con ello pérdidas económicas, sanciones o el cierre temporal o total de la organización. Esta metodología se apuntala bajo la norma ISO 27001, y busca obtener la certificación de calidad conforme a la norma ISO 91001.

A continuación, se describen las fases del ciclo según la metodología PDCA:

Fase 1. Se identifican los elementos del SGSI, incluidas las políticas, la evaluación de riesgos, el inventario de activos, las amenazas, las vulnerabilidades y su impacto en la organización. También se lleva a cabo el análisis de riesgos y la selección de los diferentes controles.

Fase 2. Se establece el plan y la implementación del tratamiento de riesgo. Adicional, se utilizan los controles, y se lleva a cabo el proceso de la concientización del personal y se aplica el SGSI.

Fase 3. Se revisa el SGSI y los controles. Asimismo, se efectúan auditorías y se registran los diferentes eventos y acciones relacionadas.

Fase 4. En la última etapa, se implementan las mejoras del SGSI, se toman las acciones correctivas y preventivas de los eventos, adicional se comprueba la eficacia de las acciones involucradas.

En conclusión, es importante destacar que la implementación de la metodología PDCA permitió establecer un SGSI con el objetivo de evaluar el estado de los sistemas informáticos, y aplicar las medidas de seguridad adecuadas con relación a la norma ISO 91001. Esto facilitó la certificación institucional de los procesos y servicios de alta calidad ante el organismo correspondiente.

Protección de los datos personales de la historia clínica en Argentina y Uruguay e IHE XDS

Los autores de este artículo, Giudice et al. (2011), presentan una perspectiva o experiencia de poder compartir información sensible bajo elementos o estándares de protección de datos, lo que permite involucrar el uso de las tecnologías de la información entre dos países. Estos autores muestran la preexistencia de un Sistema de Gestión de Seguridad y de la Información (SGSI) para la protección de los datos personales de la historia clínica del paciente entre ambos países de Argentina y Uruguay e IHE XDS en referencia a la ley de protección de datos personales (PDP) y a la familia de estándares ISO/IEC 27000. En el uso compartido de documentos entre los países, se acopla la arquitectura XDS (*cross-enterprise document sharing*) con base en el modelo de los perfiles IHE (*integrating the healthcare enterprise*) de

las transacciones sobre la información clínica o escenario del flujo del trabajo y sus debidos estándares para conseguir compartir información entre los diferentes actores.

Luego, los autores presentan una metodología en cuatro grupos, en la que destacan los principios para compartir documentos de historias clínicas con el consentimiento del paciente y los estándares de protección de datos de la siguiente manera:

- Grupo A: instalar el PDP en la historia clínica del paciente.
    - Consentimientos.
    - Datos patronímicos de pacientes (identificar y ubicar a las personas).
    - Datos comunes y sensibles.
    - Datos de registro en bitácoras.
- Grupo B: encontrar los actores del IHE respecto al grupo de los datos personales.
- Grupo C: estudiar la flexibilidad de BPPC (*basic patient privacy consent*) y registrar los posibles consentimientos informados de los pacientes mediante formularios debidamente firmados y disponibles para su consulta.
- Grupo D: realizar los accesos de la información de pacientes, familiares, médicos, personal administrativo y médicos externos, asegurando que cualquier trabajo investigativo se realice bajo los principios establecidos en la norma ISO 27000.

Finalmente, este trabajo recalca el compromiso del trabajo en línea para compartir información de gran alcance a modo sensible en el tratamiento de los datos de cada paciente y su posible manejo para eventos de investigación. El diseño y mejora continua del SGSI, permite asegurar la confidencialidad, la disponibilidad de los datos, la integridad de los documentos, la imputabilidad ("accountability") de los profesionales y auditabilidad de las transacciones en cada caso.

Diseño del Sistema de Gestión de Seguridad Informática y de la Información (SGSI) para la empresa Belisario Ltda. de Bogotá, D. C.

En el trabajo de Botero Vega (2016) se analiza el estudio de implementación de la norma ISO 27001 de seguridad de la información para la empresa en Bogotá, D. C., con el objetivo de reducir la pérdida de información y mejorar la seguridad informática. Esto se logra mediante el control de las condiciones y las variables del entorno, así como la adecuada protección de los objetivos de la naturaleza del negocio. De esta manera, se asegura que la información del cliente se encuentre protegida frente a posibles intrusiones que pongan en riesgo o que puedan comprometer su confidencialidad, integridad y disponibilidad.

El proyecto se enfoca específicamente, según el autor, en la infraestructura tecnológica de la organización y en el personal involucrado que forma parte del proceso de gestión tecnológica. Para llevar a cabo su desarrollo, se emplea la metodología Magerit versión 3.0, en combinación con el modelo PDCA ("planificar-hacer-verificar-actuar").

Objetivos

El objetivo general es implementar un roadmap para asegurar la información en el desarrollo de aplicaciones en línea que permitan evaluar el nivel de madurez de la seguridad informática y la mejora continua del negocio, que garantice el correcto tratamiento de los datos.

Los objetivos específicos son:

1. Identificar los dominios con sus respectivos controles de acuerdo con la norma ISO/IEC 27001 y los activos para asegurar la información mediante técnicas de recolección de datos.
2. Analizar los dominios con sus respectivos controles y los resultados del ambiente de pruebas para asegurar los contenidos de acuerdo con la norma ISO/IEC 27001.

3. Diseñar controles y mecanismos de la gestión de seguridad para resguardar los datos que puedan ser aplicables a empresas en desarrollos de software en recursos en línea.

4. Configurar los controles alineados a las metodologías del estado del arte para la protección de datos.

5. Preparar un ambiente de pruebas con los controles definidos en la Figura 10) para recopilar datos por el área de pruebas.

6. Valorar los resultados y hacer una mejora continua mediante el ciclo Deming.

7. Clasificar los datos o activos como sensibles y no sensibles de la muestra (17 activos tratados).

8. Capacitar al recurso humano o personal de la empresa en temas de seguridad respecto a los datos.

9. Desarrollar la metodología para garantizar la información de acuerdo con los controles aceptados o comprobados.

Metodología

La presente investigación se clasifica como documental, informativa y experimental. La estructura del documento incluye una introducción, seguida del estado del arte con un análisis de las diferentes metodologías existentes, cuyo objetivo era seleccionar de manera meticulosa el material de investigación que permita contribuir en la correcta definición en el diseño y la implementación del roadmap propuesto y poder someterlos a los procesos de exploración, descripción y el respectivo análisis, que se dividen en las siguientes fases o etapas:

1. Investigación exhaustiva de diferentes metodologías, dominios y controles similares como aporte del estado del arte.

2. Se analizan las diferentes metodologías en el estado del arte y se revisa el aporte que puede contribuir en el alcance de la investigación.

3. Se genera un roadmap para los desarrollos de aplicaciones en línea, con base en los resultados obtenidos en la revisión del estado del arte.

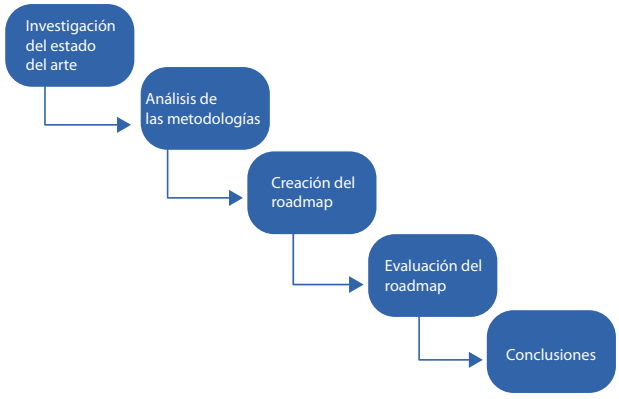
4. Se evalúa el roadmap, se utilizan los instrumentos de medición y se obtienen los resultados. Se examinan las diferentes conclusiones sobre la metodología en el contexto de las aplicaciones en línea.

5. Por último, se elaboran las diferentes conclusiones derivadas en la evaluación del roadmap, proporcionando una visión completa de los hallazgos y contribuciones de la investigación.

Es relevante analizar los pasos distintivos que permiten identificar los momentos claves del roadmap apropiados en el artículo, según la Figura 4.

Figura 4

Metodología del trabajo



A continuación, se define la implementación de un roadmap aplicable a las pequeñas y medianas empresas en el desarrollo de software en línea para facilitar la ejecución adecuada de un SGSI, con el fin de minimizar los costos económicos de inversión y el tiempo de desarrollo, de la siguiente manera:

1. Rapidez, definida en tres fases: evaluación de las características COBIT, análisis de riesgos y resultados.

2. Uso correcto de los controles definidos e identificados (véase Tabla 9).

3. Se procede al registro de un inventario con base en información clasificada y no clasificada.

4. Reporte y entrega de la plantilla completa de análisis de riesgos y el cálculo preciso de la probabilidad de ocurrencia de los eventos.

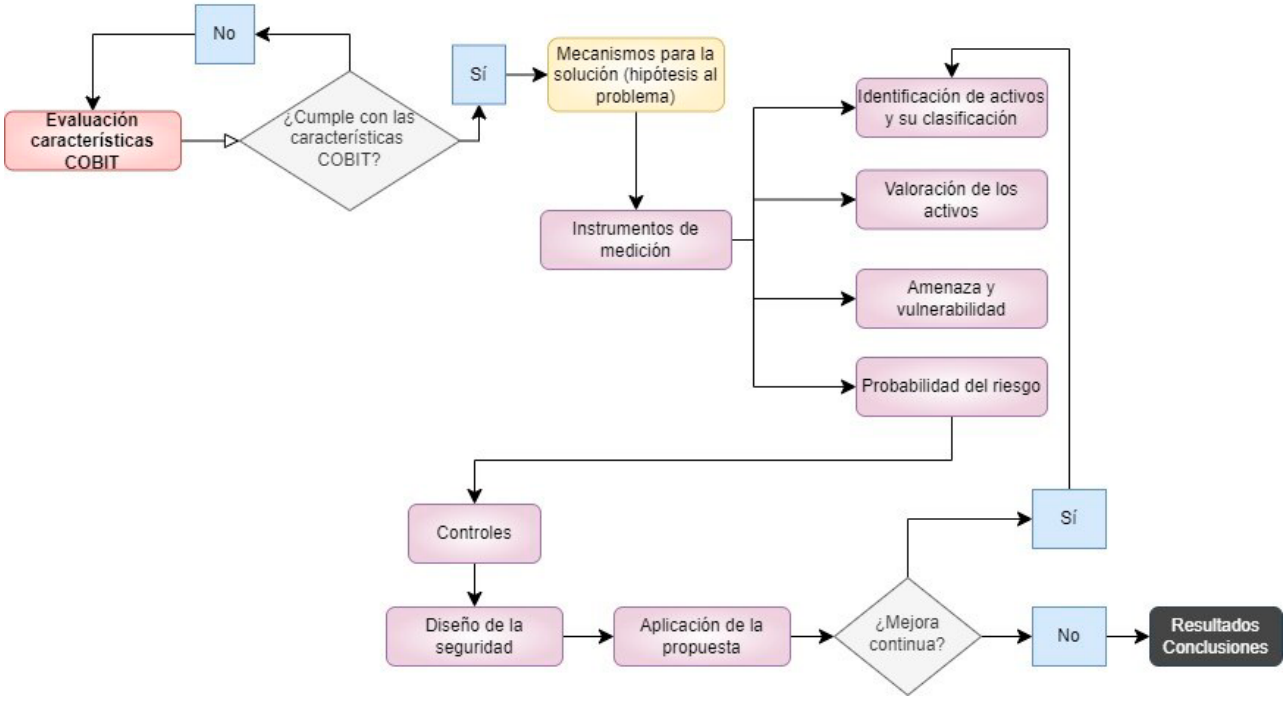
Es un tipo de desarrollo metodológico que identifica los procesos y los beneficios en las organizaciones: desde la planeación, los activos, las vulnerabilidades, las amenazas, los requisitos legales, identificar controles, calcular riesgos y plan de tratamiento del riesgo. Se debe conservar la integridad, confidencialidad, disponibilidad, compatibilidad y la legibilidad del contenido, durante y después de la producción del desarrollo.

Las organizaciones que requieren una estructura de pruebas y bases de datos antes de la producción, lo hacen bajo políticas de seguridad en el manejo y confidencialidad de la información, especialmente en aquellas que desarrollan software en sistemas en línea. Estas empresas deben estar dotadas de reglas, controles y políticas de seguridad que se encuentran en el manejo de datos personales con terceros, con el objetivo de garantizar las características utilizadas para la investigación según la metodología COBIT, las cuales son: "[…] efectividad, eficiencia, confidencialidad, integridad, disponibilidad, cumplimiento y confiabilidad de la información" (COBIT, 1996). La protección de la información, la optimización de los niveles de riesgo y la utilización correcta de los recursos son fundamentales. Además, para las organizaciones, esto proporciona roles y responsabilidades claras. Para ello, se aplica utilizando el filtro de la norma ISO 27001:2013, con los controles definidos y una política de control de acceso.

Por consiguiente, se describen en detalle los ítems en el desarrollo del modelo de investigación, como se observa en la Figura 5.

Figura 5

Modelo de investigación

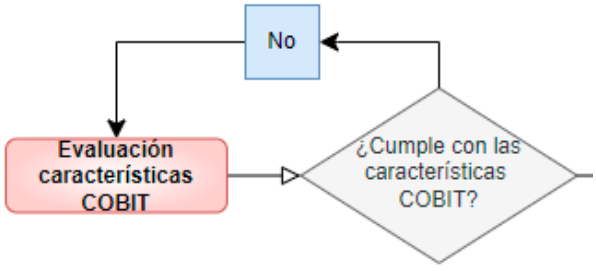


Fase 1. Evaluación de las características COBIT (véase Figura 6)

Dentro del marco de referencia de COBIT 3 edición, se hace alusión a las siete características para la protección de los datos personales tratados por la organización en los procesos de codificación o desarrollo de software en línea, según la Tabla 1.

Figura 6

Proceso fase 1 - Evaluación de las características COBIT



Para llevar a cabo el proceso de la revisión de las características según el marco de la metodología COBIT 3, se hará la evaluación mediante una plantilla de registros, la cual es una práctica que permite incluir los principios específicos de los elementos que se están revisando, junto con el espacio para registrar los indicadores. Por consiguiente, se dispone de un universo de datos a probar y evaluar, los cuales incluyen documentos, registros e información importante relacionados en el proceso de los principios e indicadores, para poder aplicar las posibles mejoras según sea necesario. En caso contrario, se empieza con el análisis de riesgos como paso siguiente del procedimiento.

Fase 2. Mecanismos para la solución

La solución se plantea a partir de la evaluación correcta de las características COBIT, las cuales son personalizadas para los procesos de desarrollo de aplicaciones en línea. El objetivo principal es conocer los niveles de riesgo que puedan afectar los activos más importantes de las empresas. A través de la implementación del roadmap, se busca minimizar o solucionar ciertos riesgos latentes que afecten la integridad, la disponibilidad y la confidencialidad de la información empresarial.

El proceso inicia con los instrumentos de medición (véase Figura 7) destinados a obtener información relevante o de gran impacto para su respectivo análisis. Por medio del modelo de investigación que se está empleando, se busca agilizar la identificación y análisis de los diferentes elementos, como los activos, las amenazas, las vulnerabilidades y la probabilidad de riesgos asociados. La eficacia de este enfoque es fundamental, ya que la falta de cobertura de estos aspectos, previamente mencionados, podría llegar a presentar un riesgo de alto impacto que afecte tanto los servicios operacionales como la imagen de las organizaciones.

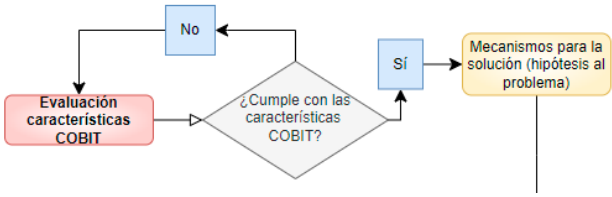
Tabla 1

Características COBIT

Característica Metodológica COBIT 3										
Nombre de la empresa:										
Responsable:										
Lugar y Fecha:										
			Principios						Indicadores	
Clasificación	Activo	Descripción del activo	Efectividad	Eficiencia	Confidencialidad	Integridad	Disponibilidad	Cumplimiento	Confiabilidad de la información	Ítems	Nivel de Seguridad

Figura 7

Proceso fase 2 - Mecanismos para la solución



Fase 3. Instrumentos de medición

Para la recolección de información dentro de las empresas pymes, se usan las siguientes técnicas bajo la metodología empleada y aplicada de la siguiente manera (véase Figura 8):

Entrevistas: se realizan reuniones en el sitio o de manera virtual (experiencia y funciones) con el personal idóneo de los diferentes procesos, con el objetivo de obtener datos útiles para la valoración de los riesgos.

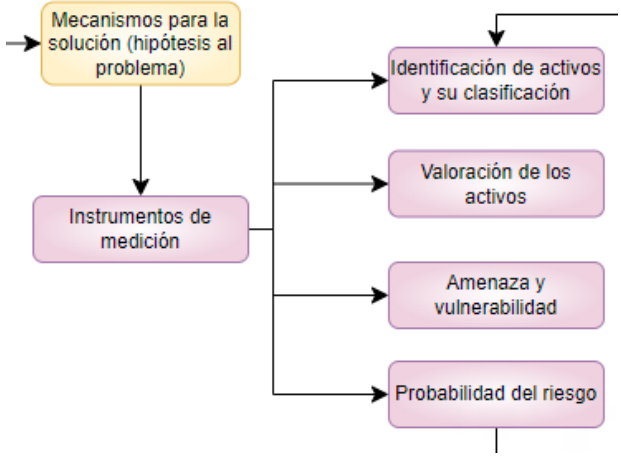
- Durante la entrevista se recopila contenido del cliente (qué datos), de los procesos, del objetivo de la empresa (misión, visión, servicios y productos). Se conoce el dominio, frecuencia y volumen de los datos informativos.
- Se realiza la identificación de los activos y su inventario de la organización.
- Se analizan las posibles amenazas, vulnerabilidades y riesgos de la información.
- Se clasifican los activos más importantes en el flujo de los datos relevantes.

Revisión de documentos: documentación de procesos, normas, directrices, formatos, bitácoras, informes de auditorías previas, inventarios de equipos, matriz de cumplimiento de requisitos legales, hojas de vida de los activos informáticos y plantilla de controles planeados por la organización.

- Se procede a la revisión de los documentos originales, en la cual se estima una fecha de valoración de los procesos de los registros para su estudio en formato .pdf (*portable document format* documentos digitales-Adobe Reader) y .ppt (MS-PowerPoint). Durante esta revisión, se verifican los elementos claves en cada documento, asegurando que tenga un título, membrete de la empresa para su legalidad, folio, ley de protección de datos personales y cumplimiento legal.
- Se inspeccionan los documentos legales de representación de ley para el respectivo funcionamiento de la organización en el desarrollo y la codificación de productos de software en el uso comercial.
- Documento de la Cámara de Comercio.
- Documento de la Industria y Comercio.
- Documento de la actividad económica, Registro Único Tributario (RUT).

Figura 8

Proceso fase 3 - Instrumentos de medición



Identificación de activos y clasificación

Un activo, según García (2013), "[…] el valor de la información aumenta cada día siendo el activo más importante de las empresas u organizaciones", gestionado por cualquier entidad o persona. Este autor destaca el valor fundamental de la información como ente primordial que debe protegerse.

En el marco de la identificación de activos y su clasificación, se emplea la metodología de análisis de riesgos Magerit, la cual expresa activos generales. Esta elección se propone como un aporte específico y valioso para las

empresas de desarrollo de aplicaciones en línea, ya que se ajusta, de manera precisa, a la identificación de activos relacionados en este contexto particular.

Como parte de esta iniciativa, se ha generado una plantilla personalizada diseñada para la clasificación de los activos, que se aplica para facilitar el proceso de organización por parte de los diferentes entes relacionados o involucrados en el contexto de los activos. El desarrollo de esta plantilla se lleva a cabo mediante la utilización de la popular herramienta Excel, la cual brinda a los usuarios flexibilidad y accesibilidad en su manejo, con base en los siguientes elementos: clasificación, tipo, activo, sensible o no sensible, definición conceptual y operacional (véase Tabla 2).

Valoración de los activos

En el proceso de la valoración, se ha establecido un análisis detallado de las dimensiones, características o atributos que posibilitan encontrar un valor específico a los activos de la organización. Esta información se establece y se presenta en tres pilares fundamentales en la seguridad de los datos: confidencialidad, integridad y disponibilidad. La estructuración de este inestimable contenido se visualiza en las Tablas 3, 4 y 5, las cuales reflejan y relacionan las dimensiones críticas con respecto a la seguridad de la información. Estas tablas sirven como una herramienta referencial para comprender y evaluar los activos desde diferentes aspectos claves de la organización, permitiendo facilitar la toma de decisiones fundamentadas y la ejecución de estrategias de seguridad destinada a proteger los activos identificados como críticos o de gran relevancia para las partes involucradas.

Tabla 2

Clasificación de los activos

CLASIFICACIÓN DE LOS ACTIVOS INFORMÁTICOS APLICACIONES EN LÍNEA						
Nombre de la empresa:						
Responsable:						
Lugar y Fecha:						
Definición conceptual	**Definición operacional**	**Clasificación**	**Tipo**	**Activo**	**Sensibles**	**No sensibles**

Tabla 3

Niveles de confidencialidad

Confidencialidad (C)		Indicador	
Definición conceptual	**Definición operacional**	**Ítem**	**Dimensión**
Advertir la no divulgación de los datos personales o activos de la información (ESGinnova Group, 2015).	Actividad que permite identificar el nivel de impacto en la confidencialidad de la información o los datos de la organización en sistemas en línea.	1-2	Libre
		3-5	Restringida
		6-8	Protegida
		9-10	Confidencial
		N/A	No aplica

Tabla 4

Niveles de integridad

Integridad (I)		Indicador	
Definición conceptual	**Definición operacional**	**Ítem**	**Dimensión**
Capacidad para garantizar la no modificación o pérdida de la información (ESGinnova Group, 2015).	Proceso que permite identificar el nivel de impacto en la integridad de la información o los datos de la empresa en sistemas en línea.	1-2	Baja
		3-5	Normal
		6-8	Alta
		9-10	Crítica
		N/A	No aplica

Tabla 5

Niveles de disponibilidad

Disponibilidad (D)		Indicador	
Definición conceptual	**Definición operacional**	**Ítem**	**Dimensión**
La información debe estar protegida con relación a la negación de los accesos no autorizados a los sistemas (ESGinnova Group, 2015).	Menos de una hora	1-2	Baja
	Hasta un día de labor	3-5	Normal
	Hasta una semana	6-8	Alta
	Más de una semana	9-10	Crítica
	No aplica	N/A	No aplica

Amenazas y vulnerabilidades

En este punto, el objetivo es identificar las posibles amenazas que afectan a los activos informáticos dentro de la organización y vulnerabilidades que pueden ser materializadas o explotadas por el peligro latente. Se lleva a cabo el reconocimiento de las posibles amenazas en función de los activos informáticos relacionados, desglosando los subconjuntos y personalizando los elementos que sean necesarios.

Para el proceso de evaluar las amenazas, se contemplan las siguientes condiciones de tratamiento sobre el activo en riesgo:

1. Cada amenaza es excluyente una de otra; por ende, si hay un error de usuario, no es necesario que exista una fuga de información y a la vez es uso previsto de los recursos.

2. Se basa en las distribuciones parejas según el número de factores que implica para el proyecto. Si se tienen diez amenazas por activo, se deben dividir entre el cálculo de probabilidad de ocurrencia de eventos excluyentes de la cantidad de amenazas que existan por activo

3. Para el debido proceso de análisis estadístico en la evaluación de las amenazas, se utilizó el cálculo de ocurrencia de eventos excluyentes en relación con la suma. Esto implica que la probabilidad de que ocurra cualquiera de los riesgos, representados por , se determina por la unión o la suma de las probabilidades de que suceda cada amenaza de manera individual, es decir, .

El modelo de cálculo de la probabilidad de ocurrencia para orientar el proceso de evaluación correspondiente se muestra en la Ecuación 1.

$$PA = \frac{100\%}{\sum_{i=1}^{n} Yi} \quad (1)$$

Donde:

Donde:

PA = probabilidad de amenaza

*Amenaza*1 = Y_1

*Amenazas*2 = Y_2

*Amenazas*3= Y_3

$$n-ésimas\ amenazas = \sum_{i=1}^{n} Yi = Y_1 + Y_2 + Y_3 + ... + Y_n$$

La probabilidad del riesgo por amenazas (*PR*), se puede calcular mediante una regla de tres simple como se muestra en la Ecuación 2.

$$\frac{X}{PR} + \frac{100\%}{PA}$$

Despejando:

$$PR = \frac{PA * X}{100\%} \quad (2)$$

Donde:

PR = probabilidad del riesgo por amenazas

Total activo = *X*

Al conseguir la probabilidad del riesgo por cada amenaza relacionada a un activo y sumar los resultados mediante el álgebra, se obtiene el valor total de la probabilidad del riesgo (Ecuación 3).

TPRAn = total probabilidad del riesgo por activo, es una sucesión de sumas parciales.

$$TPRA_n = \sum_{i=1}^{n} PR_i = PR_1 + PR_2 + ... + PR_n \quad (3)$$

Probabilidad del riesgo que afecta el activo: es la suma de las probabilidades de los factores de cada amenaza sobre el activo según su clasificación. Los datos se muestran en porcentaje (%).

Probabilidad del riesgo

El riesgo se define como la medida del daño o afectación potencial sobre un activo de información cuando se materializa una amenaza. Este impacto se evalúa en términos de probabilidad de ocurrencia (baja, normal, alta y crítica), según la Tabla 6. Es importante destacar que en este análisis no se consideran las salvaguardas o controles implementados, por lo que no se ha realizado ningún control sobre el riesgo identificado. "Pueden derivarse de las diferentes amenazas de los activos, por lo que se debe construir un vínculo entre los activos, las amenazas y lo relevante para las empresas, con el fin que proporcionan una base de cómo analizar los riesgos"(Mujica & Álvarez, 2009, p. 35).

Tabla 6

Nivel del riesgo

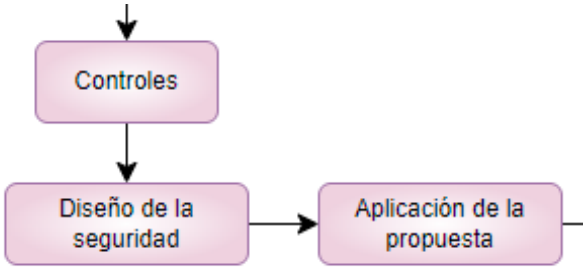
Nivel del riesgo		**Indicador**	
Definición conceptual	**Definición operacional**	**Ítem**	**Dimensión**
Representa el nivel de probabilidad del riesgo que pueda afectar el funcionamiento del sistema o procesos (Pinzón Parada, 2014).	Tiempo cumplido anual desde la última acción.	Elementos en el rango de 1%-25%	Baja
	Tiempo cumplido cada mes desde la última acción.	Elementos en el rango de 26%-50%	Normal
	Tiempo cumplido semanalmente desde la última acción.	Elementos en el rango de 51%-75%	Alta
	Tiempo cumplido diariamente desde la última acción.	Elementos en el rango de 76%-100%	Crítica

Fase 4. Controles

Después de realizar el análisis de cada riesgo, es importante identificar y clasificarlos de manera adecuada. Luego, se establecen los objetivos de control bajo la norma que ofrece un marco amplio con relación a la seguridad informática según la ISO/IEC 27002:2013. Estos objetivos de control se definen con sus 14 dominios, que contienen diversos elementos de seguridad de la información y sus 35 objetivos de control, que se distribuyen en 114 controles de manera específica. Para aplicar estos objetivos y controles, es relevante contar con políticas claras y definidas. Dichas políticas se crean mediante consultas y reuniones con el gerente de la empresa, personal de seguridad y otros empleados involucrados en el proceso. A continuación, se presenta el proceso ilustrado en la Figura 9.

Figura 9

Proceso fase 4 – Controles



A continuación, se presenta un listado de los controles que "son necesarios para asegurar datos sensitivos" (Fisher, 1988, p. 107), alineados a la metodología de investigación y establecidos en la norma del marco ISO 27002:2013. Estos controles se aplican luego de haber realizado el análisis de riesgos sobre el universo de los datos de las pymes que desarrollan aplicaciones en línea. En el contexto de las empresas pequeñas y medianas, se destacan algunos dominios y controles que las empresas a modo inicial podrían necesitar según la Figura 10, se resaltan en amarillo. Aunque es importante reconocer que la selección de los controles es determinada según la naturaleza y las necesidades de los procesos de cada organización. Se recomienda que las pymes adapten y amplíen estos controles en conformidad con las características y el entorno de trabajo. La debida implementación de estas medidas de seguridad contribuye significativamente a proteger la confidencialidad, integridad y disponibilidad de los datos sensibles de cada organización.

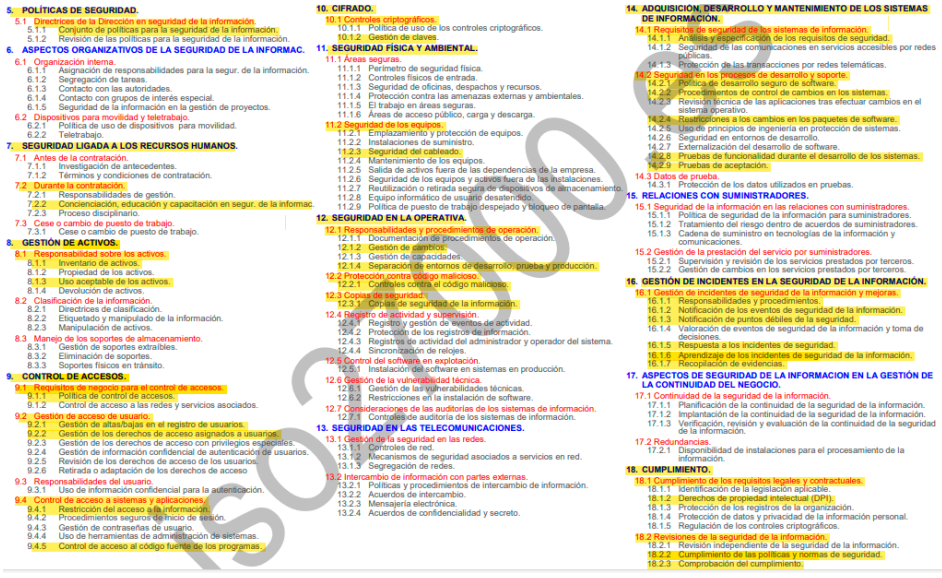
Diseño de la seguridad

Objetivo del SGSI

Los objetivos propuestos para la investigación en este documento sobre la metodología para el diseño del Sistema de Gestión de Seguridad Informática (SGSI) son los siguientes:

Figura 10

Controles identificados para las aplicaciones en línea


5. POLÍTICAS DE SEGURIDAD.
5.1 Directrices de la Dirección en seguridad de la información.
5.1.1 Conjunto de políticas para la seguridad de la información.
5.1.2 Revisión de las políticas para la seguridad de la información.
6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMAC.
6.1 Organización interna.
6.1.1 Asignación de responsabilidades para la segur. de la información.
6.1.2 Segregación de tareas.
6.1.3 Contacto con las autoridades.
6.1.4 Contacto con grupos de interés especial.
6.1.5 Seguridad de la información en la gestión de proyectos.
6.2 Dispositivos para movilidad y teletrabajo.
6.2.1 Política de uso de dispositivos para movilidad.
6.2.2 Teletrabajo.
7. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.
7.1 Antes de la contratación.
7.1.1 Investigación de antecedentes.
7.1.2 Términos y condiciones de contratación.
7.2 Durante la contratación.
7.2.1 Responsabilidades de gestión.
7.2.2 Concienciación, educación y capacitación en segur. de la informac.
7.2.3 Proceso disciplinario.
7.3 Cese o cambio de puesto de trabajo.
7.3.1 Cese o cambio de puesto de trabajo.
8. GESTIÓN DE ACTIVOS.
8.1 Responsabilidad sobre los activos.
8.1.1 Inventario de activos.
8.1.2 Propiedad de los activos.
8.1.3 Uso aceptable de los activos.
8.1.4 Devolución de activos.
8.2 Clasificación de la información.
8.2.1 Directrices de clasificación.
8.2.2 Etiquetado y manipulado de la información.
8.2.3 Manipulación de activos.
8.3 Manejo de los soportes de almacenamiento.
8.3.1 Gestión de soportes extraíbles.
8.3.2 Eliminación de soportes.
8.3.3 Soportes físicos en tránsito.
9. CONTROL DE ACCESOS.
9.1 Requisitos de negocio para el control de accesos.
9.1.1 Política de control de accesos.
9.1.2 Control de acceso a las redes y servicios asociados.
9.2 Gestión de acceso de usuario.
9.2.1 Gestión de altas/bajas en el registro de usuarios.
9.2.2 Gestión de los derechos de acceso asignados a usuarios.
9.2.3 Gestión de los derechos de acceso con privilegios especiales.
9.2.4 Gestión de información confidencial de autenticación de usuarios.
9.2.5 Revisión de los derechos de acceso de los usuarios.
9.2.6 Retirada o adaptación de los derechos de acceso
9.3 Responsabilidades del usuario.
9.3.1 Uso de información confidencial para la autenticación.
9.4 Control de acceso a sistemas y aplicaciones.
9.4.1 Restricción del acceso a la información.
9.4.2 Procedimientos seguros de inicio de sesión.
9.4.3 Gestión de contraseñas de usuario.
9.4.4 Uso de herramientas de administración de sistemas.
9.4.5 Control de acceso al código fuente de los programas.
10. CIFRADO.
10.1 Controles criptográficos.
10.1.1 Política de uso de los controles criptográficos.
10.1.2 Gestión de claves.
11. SEGURIDAD FÍSICA Y AMBIENTAL.
11.1 Áreas seguras.
11.1.1 Perímetro de seguridad física.
11.1.2 Controles físicos de entrada.
11.1.3 Seguridad de oficinas, despachos y recursos.
11.1.4 Protección contra las amenazas externas y ambientales.
11.1.5 El trabajo en áreas seguras.
11.1.6 Áreas de acceso público, carga y descarga.
11.2 Seguridad de los equipos.
11.2.1 Emplazamiento y protección de equipos.
11.2.2 Instalaciones de suministro.
11.2.3 Seguridad del cableado.
11.2.4 Mantenimiento de los equipos.
11.2.5 Salida de activos fuera de las dependencias de la empresa.
11.2.6 Seguridad de los equipos y activos fuera de las instalaciones.
11.2.7 Reutilización o retirada segura de dispositivos de almacenamiento.
11.2.8 Equipo informático de usuario desatendido.
11.2.9 Política de puesto de trabajo despejado y bloqueo de pantalla.
12. SEGURIDAD EN LA OPERATIVA.
12.1 Responsabilidades y procedimientos de operación.
12.1.1 Documentación de procedimientos de operación.
12.1.2 Gestión de cambios.
12.1.3 Gestión de capacidades.
12.1.4 Separación de entornos de desarrollo, prueba y producción.
12.2 Protección contra código malicioso.
12.2.1 Controles contra el código malicioso.
12.3 Copias de seguridad.
12.3.1 Copias de seguridad de la información.
12.4 Registro de actividad y supervisión.
12.4.1 Registro y gestión de eventos de actividad.
12.4.2 Protección de los registros de información.
12.4.3 Registros de actividad del administrador y operador del sistema.
12.4.4 Sincronización de relojes.
12.5 Control del software en explotación.
12.5.1 Instalación del software en sistemas en producción.
12.6 Gestión de la vulnerabilidad técnica.
12.6.1 Gestión de las vulnerabilidades técnicas.
12.6.2 Restricciones en la instalación de software.
12.7 Consideraciones de las auditorías de los sistemas de información.
12.7.1 Controles de auditoría de los sistemas de información.
13. SEGURIDAD EN LAS TELECOMUNICACIONES.
13.1 Gestión de la seguridad en las redes.
13.1.1 Controles de red.
13.1.2 Mecanismos de seguridad asociados a servicios en red.
13.1.3 Segregación de redes.
13.2 Intercambio de información con partes externas.
13.2.1 Políticas y procedimientos de intercambio de información.
13.2.2 Acuerdos de intercambio.
13.2.3 Mensajería electrónica.
13.2.4 Acuerdos de confidencialidad y secreto.
14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN.
14.1 Requisitos de seguridad de los sistemas de información.
14.1.1 Análisis y especificación de los requisitos de seguridad.
14.1.2 Seguridad de las comunicaciones en servicios accesibles por redes públicas.
14.1.3 Protección de las transacciones por redes telemáticas.
14.2 Seguridad en los procesos de desarrollo y soporte.
14.2.1 Política de desarrollo seguro de software.
14.2.2 Procedimientos de control de cambios en los sistemas.
14.2.3 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo.
14.2.4 Restricciones a los cambios en los paquetes de software.
14.2.5 Uso de principios de ingeniería en protección de sistemas.
14.2.6 Seguridad en entornos de desarrollo.
14.2.7 Externalización del desarrollo de software.
14.2.8 Pruebas de funcionalidad durante el desarrollo de los sistemas.
14.2.9 Pruebas de aceptación.
14.3 Datos de prueba.
14.3.1 Protección de los datos utilizados en pruebas.
15. RELACIONES CON SUMINISTRADORES.
15.1 Seguridad de la información en las relaciones con suministradores.
15.1.1 Política de seguridad de la información para suministradores.
15.1.2 Tratamiento del riesgo dentro de acuerdos de suministradores.
15.1.3 Cadena de suministro en tecnologías de la información y comunicaciones.
15.2 Gestión de la prestación del servicio por suministradores.
15.2.1 Supervisión y revisión de los servicios prestados por terceros.
15.2.2 Gestión de cambios en los servicios prestados por terceros.
16. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.
16.1 Gestión de incidentes de seguridad de la información y mejoras.
16.1.1 Responsabilidades y procedimientos.
16.1.2 Notificación de los eventos de seguridad de la información.
16.1.3 Notificación de puntos débiles de la seguridad.
16.1.4 Valoración de eventos de seguridad de la información y toma de decisiones.
16.1.5 Respuesta a los incidentes de seguridad.
16.1.6 Aprendizaje de los incidentes de seguridad de la información.
16.1.7 Recopilación de evidencias.
17. ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.
17.1 Continuidad de la seguridad de la información.
17.1.1 Planificación de la continuidad de la seguridad de la información.
17.1.2 Implantación de la continuidad de la seguridad de la información.
17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información.
17.2 Redundancias.
17.2.1 Disponibilidad de instalaciones para el procesamiento de la información.
18. CUMPLIMIENTO.
18.1 Cumplimiento de los requisitos legales y contractuales.
18.1.1 Identificación de la legislación aplicable.
18.1.2 Derechos de propiedad intelectual (DPI).
18.1.3 Protección de los registros de la organización.
18.1.4 Protección de datos y privacidad de la información personal.
18.1.5 Regulación de los controles criptográficos.
18.2 Revisiones de la seguridad de la información.
18.2.1 Revisión independiente de la seguridad de la información.
18.2.2 Cumplimiento de las políticas y normas de seguridad.
18.2.3 Comprobación del cumplimiento.

- Analizar e identificar los diferentes dominios y controles según la norma ISO 27001.

- Proteger los datos personales de terceros identificados como los activos de información dentro de la organización mediante el diseño de controles, preservando la disponibilidad, la integridad y la confidencialidad en recursos en línea.

- Minimizar el nivel de riesgo dentro de la organización, basado en las características de COBIT 3, "efectividad, eficiencia, confidencialidad, integridad, disponibilidad, cumplimiento y confiabilidad de la información" y capacitación del recurso humano.

- Evaluar los resultados obtenidos y realizar mejoras continuas.

- Garantizar el acceso a la información dentro de la organización según las diferentes políticas, procedimientos y controles conforme al estudio realizado y definido por la alta gerencia.

- En el universo de los datos proporcionados (muestra) para la investigación, clasificar los datos como sensibles y no sensibles.

- Preparar la metodología de investigación según los controles admitidos.

Alcance del Sistema de Gestión de Seguridad de la Información

Se determina mediante varios aspectos, como la estructura organizativa, ubicación física, los activos y tecnología relacionada. Este alcance implica el proceso integral de las tecnologías de la información y comunicación, con el objetivo de garantizar la seguridad y protección de los diferentes activos, especialmente los datos personales. Para cumplir con este propósito, se implementan políticas, procedimientos y controles de manera específica con fines de fortalecer la confidencialidad, integridad y disponibilidad de la seguridad en sistemas en línea.

Política de seguridad

La política del Sistema de Gestión de Seguridad de la Información se define como la directriz que representa la directiva o alta gerencia de la organización, en relación con la seguridad de la información para la protección de datos personales en desarrollo de aplicaciones en línea.

Con el propósito de cumplir con los objetivos estratégicos y teniendo como base sus valores corporativos, modelos de negocios, la participación e integración de sus consultores y las necesidades de atención a los clientes de tecnologías de información propias y de terceros, las entidades establecen la función de seguridad de la información en la organización de la siguiente manera:

- Ser adecuada al propósito de la organización.

- Incluir objetivos de seguridad de los datos.

- Compromiso de cumplir con los requisitos aplicables a la seguridad de la información.

- Establecer la mejora continua del SGSI.

- Estar disponible como información documentada.

- Comunicación dentro de la organización y estar disponible para las partes interesadas, como sea apropiado.

- Definir una estructura de políticas según la naturaleza de la empresa en desarrollo de software en línea.

Aplicación de la propuesta

En este ítem, tras un exhaustivo análisis de los diferentes activos, amenazas, seguido con su posible impacto, las empresas deben permitir implementar los diferentes controles y políticas correspondientes para garantizar la seguridad en la protección de los datos personales. La implementación propuesta es aplicarlas según los activos que presenten un nivel de riesgo determinado o, en su defecto, un nivel de riesgo

alto que se contemple entre el 76%-100%, con el objetivo de disminuir o mitigar los problemas que impactan en las variables críticas.

A continuación, se relacionan los elementos de la aplicación de la propuesta:

- Clasificación
- Tipo
- Activo
- Dominio
- Objetivos de control
- Control(es)

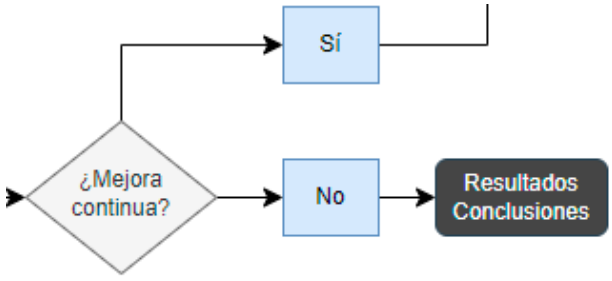
Estos elementos son esenciales para una correcta aplicación de la propuesta y para permitir hacer mejoras continuas con la identificación de los procesos de la metodología de investigación. Por consiguiente, se procede a analizar los resultados y conclusiones de lo recursivo del roadmap. Lo anterior proporciona una visión clara y precisa de los hallazgos encontrados, lo cual facilita la interpretación de mejores decisiones informadas y las acciones correspondientes de manera correctiva, si es requerido.

Fase 5. Resultados y conclusiones

En este punto se expresan los resultados de la medición de manera cuantitativa y cualitativa, donde se refleja una probabilidad de nivel del riesgo en los activos según los valores de la empresa con relación al desarrollo de aplicaciones en línea que se van a emplear. Por tanto, se analizan los niveles de riesgo o riesgos latentes asociados con este tipo de información. Se verifica si el roadmap implementado corrigió los problemas o si tuvo alguna falla o inconveniente de algunos de los controles o políticas presentadas. En caso de que exista algún activo que no estaba relacionado inicialmente, se procede a su identificación, análisis, aplicación de la metodología y se verifica si el problema se resolvió de manera apropiada, según Figura 11.

Figura 11

Proceso fase 5 - Resultados y conclusiones



Resultados

Con el objetivo de validar el roadmap propuesto, se selecciona una empresa de desarrollo de aplicaciones en línea para realizar la implementación; la empresa seleccionada es Bitsoft de Bogotá, D. C.

Evaluación de las características COBIT

Las características de la metodología COBIT (Objetivos de Control para la Información y las Tecnologías Relacionadas) indican las siguientes acciones en cada una de las fases para garantizar el flujo normal de los datos.

- Efectividad: los datos pertinentes o relevantes se encuentran disponibles para su procesamiento de manera oportuna.
- Eficiencia: se optimiza el tiempo para estandarizar el flujo de entrada y salida de datos, utilizando controles con base en la norma ISO 27001.
- Confidencialidad: una vez que se reciban los datos reales de pruebas, no pueden ser modificados ni comercializados, ya que están protegidos por un acuerdo de confidencialidad y no divulgación de registros personales de terceros.
- Integridad: se debe garantizar que los datos de entrada en el flujo de información sean los mismos que los de salida, sin ningún tipo de alteraciones.

- Disponibilidad: los datos de trabajo de pruebas están listos y disponibles para su tratamiento en las etapas de entrada, proceso y salida.

- Cumplimiento: una vez establecidos los procesos a desarrollar, las políticas, procedimientos, controles, los contratos y las leyes de protección de datos en Colombia, se da cumplimiento a la disposición de los registros.

- Confiabilidad de la información: los datos de entrada coinciden con los de salida sin ningún tipo de error, falla o alteración, con el objetivo de garantizar que no se pierdan los registros. En caso contrario, se debe reportar el incidente al departamento de sistemas o a la alta gerencia.

Con lo anterior, se llevó a cabo el proceso de la empresa Bitsoft en la evaluación de las características de la metodología COBIT y se obtuvieron los siguientes resultados, como se evidencia en la Tabla 7.

Tabla 7

Características COBIT

Característica Metodológica COBIT 3	
Nombre de la empresa: Bitsoft	
Responsable:	Carlos Mario
Lugar y Fecha:	Bogotá, ago-18

			Principios							**Indicadores**	
Clasificación	**Activo**	**Descripción del activo**	**Efectividad**	**Eficiencia**	**Confidencialidad**	**Integridad**	**Disponibilidad**	**Cumplimiento**	**Confiabilidad**	**Ítems**	**Dimensión**
Activo de información	Copia seguridad código probado semanalmente	Datos almacenados para el respaldo de la información de manera online	X	X	X	X	X	X	X	6-7	Alto
	Windows 10	Sistema Operativo (SO) asignadas el equipo TI	X	X	X					3-5	Medio

Mecanismos para la solución

Dado que la empresa Bitsoft no cuenta con un SGSI, puede suceder que los datos lógicos se pongan en riesgo: pérdida de los registros, fuga de los datos, la información se corrompa o desorganización de los archivos, permitiendo que las organizaciones estén expuestas a los diferentes riesgos. Tales situaciones pueden generar pérdidas tanto de datos como económicas para los clientes o empresas, lo que conlleva poner a disposición de personas malintencionadas o ataques relacionados en el desarrollo en línea como son los datos sensibles (número de tarjeta y cuenta, fecha de expedición y vencimiento, saldo, contraseña y código de seguridad - CVV, en *card verification value*, "valor de verificación de la tarjeta"). Lo anterior refleja las carencias de políticas de control de acceso para el respectivo manejo de los registros o el activo más importante en ambientes de desarrollo en línea.

El desarrollo de la presente investigación beneficiará a la empresa Bitsoft en la protección de datos personales de terceros y el uso de los activos, lo que permite una mejora continua en los procesos de gestión de la seguridad; "[…] así, el diseño y la implementación de la metodología con base en un SGSI será mejor acogido por las personas relacionadas, progresando de manera sucesiva y con un menor esfuerzo por obtener seguridad"(Gómez Fernández & Fernández Rivero, 2018, p. 14). Lo cual genera un incremento en los niveles de confianza de sus clientes y aliados estratégicos, donde se establece un respaldo de continuidad y disponibilidad de Bitsoft en cada uno de sus procesos, lo que incrementa el valor comercial o productivo y mejora la imagen de la empresa.

Instrumentos de medición

Se emplean los siguientes instrumentos informáticos, cuyos procesos y comunicaciones con el recurso humano se hacen de manera remota o a través de plataformas virtuales. La recolección de la información se lleva a cabo mediante el uso de las computadoras, dispositivos móviles y la conectividad a internet. Además, se utilizan las herramientas colaborativas para la transferencia de la información como Google Drive o el One Drive. Las reuniones establecidas se realizan a través de llamadas telefónicas y con el uso de medios sincrónicos como Microsoft Teams o Google Meet. Se utiliza la herramienta Excel para las plantillas de análisis de riesgos y los cálculos de las probabilidades y representación gráfica de la información mediante diagramas circulares o de barras.

- Computadora: dispositivo para llevar a cabo las diferentes tareas para el tratamiento de la información.
- Dispositivos móviles: comunicación de manera rápida y permanente con el equipo de desarrollo del proyecto.
- Google Drive: herramienta para el almacenamiento y transferencia de la información de los procesos.
- Microsoft Teams: reuniones virtuales parciales con el equipo de trabajo para el debido proceso de la investigación; además, dicha herramienta ofrece mayor seguridad en la protección de datos.
- La población objeto de este proyecto es el personal de organización de desarrollo de software ubicada en Bogotá. Como es una empresa pequeña, se trabajará con el 100% del personal vinculado a la misma por su tamaño del recurso humano.

Identificación de activos y clasificación

Como resultado del proceso de revisión de los activos informáticos de la organización y de los elementos que los componen, se obtiene en primer lugar su clasificación (véase Tabla 8).

Tabla 8

Clasificación de los activos informáticos

CLASIFICACIÓN DE LOS ACTIVOS INFORMÁTICOS APLICACIONES EN LÍNEA						
Nombre de la empresa: Bitsoft						
Responsable: Carlos Mario						
Lugar y Fecha: 12/10/2021						
Definición conceptual	**Definición operacional**	**Clasificación**	**Tipo**	**Activo**	**Sensibles**	**No sensibles**
Establece los niveles de protección como sensibles y no sensibles para resguardar la información según los tiempos de la empresa Bitsoft (MINTIC, 2016)	El tiempo considerado semanal desde la última operación	Activo de Información	[backup]	Copia de seguridad código probado semanalmente	x	
	El tiempo cumplido mensual	Software	[SO]	Windows 10		x
			[VPN]	Red virtual personal (VPN)		x
			[email]	Google Drive	x	
			[email]	Correo electrónico		x

Valoración de los activos

Se puede apreciar claramente la importancia o relevancia de la valoración de los activos de la organización identificados en cada una de sus dimensiones presentadas en la Figura 12.

Amenazas y vulnerabilidades

Se realiza el proceso de calcular la probabilidad del riesgo en los activos en cuanto a la naturaleza de la empresa Bitsoft, representada en la Figura 13.

Figura 12

Valoración de activos según el proceso

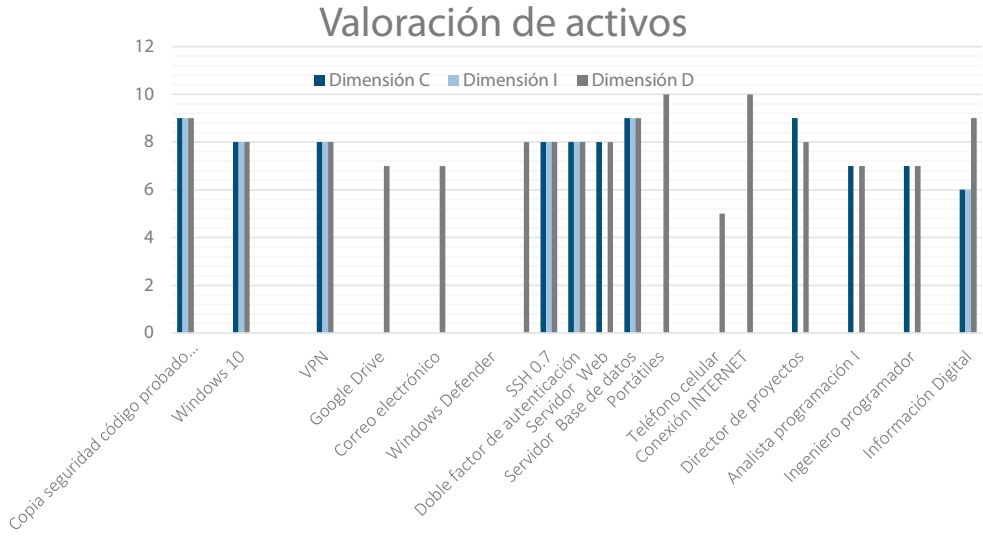
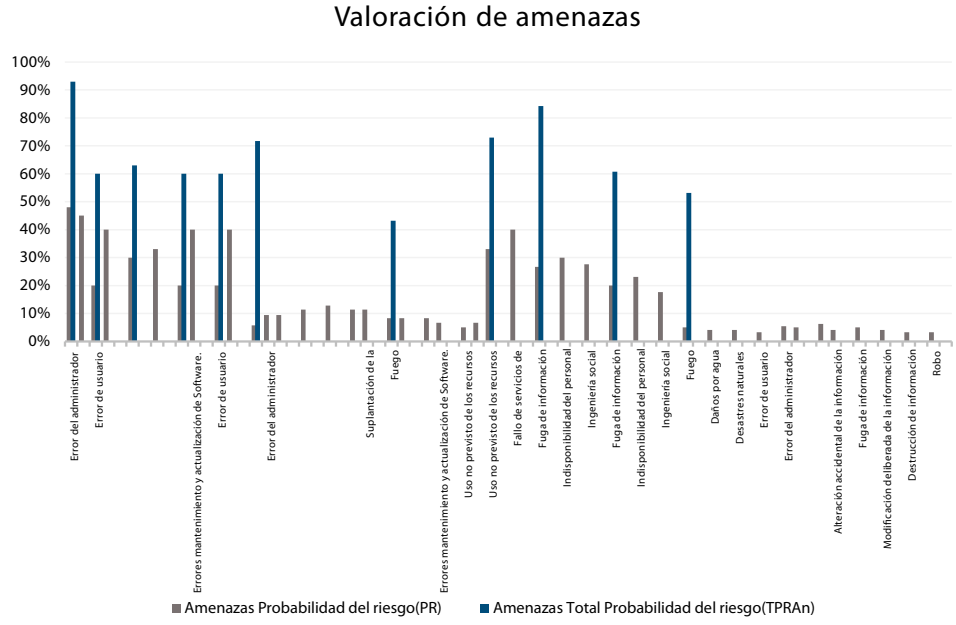


Figura 13

Valoración de las amenazas según el proceso



Probabilidad del riesgo

Se efectúa un seguimiento y control exhaustivo de los riesgos clasificados en color rojo, lo que indica una elevada probabilidad de que dicho evento se produzca al materializarse las amenazas. Ello podría comprometer el activo y poner en riesgo la información personal de terceros, como se aprecia en la Figura 14.

Controles

Por consiguiente, se identifican los activos que son posiblemente un riesgo latente para la empresa Bitsof. En la Tabla 9 se relacionan los controles indicados para cubrir dicha novedad según la valoración del riesgo, con el fin de minimizar el impacto que pueda generar sobre el tipo de información.

Diseño de la seguridad

En este segmento, se definen unos ítems con el objetivo de generar una estructura básica de políticas de seguridad, adaptándola a sus procesos en desarrollo de aplicaciones en línea para la empresa Bitsoft. Se presenta una lista que puede ser importante para la empresa, según las valoraciones de riesgos identificados previamente. Por consiguiente, se expresa la política de la seguridad empleada por la entidad y la cual se trató durante la investigación.

Figura 14

Valoración del riesgo

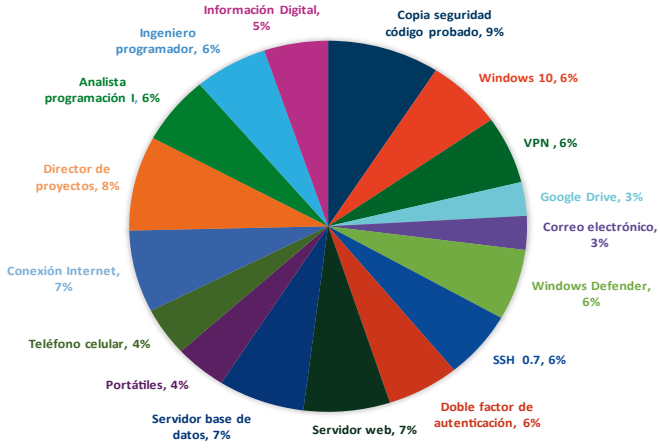


Tabla 9

Controles aplicados

Dominios, objetivos de control y controles				
Bitsoft				
Tipo	**Activo**	**Dominio**	**Objetivos de control**	**Control(es)**
[backup]	Copia de seguridad código probado semanalmente	7. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS 8. GESTIÓN DE ACTIVOS 12. SEGURIDAD EN LA OPERATIVA	7.2 Durante la contratación 8.1 Responsabilidad sobre los activos 12.3 Copias de seguridad	7.2.2 Concientización, educación y capacitación en seguridad de la información 8.1.1 Inventario de activos 8.1.3 Uso aceptable de los activos 12.3.1 Copias de seguridad de la información

Políticas de seguridad

Bogotá, 26 de enero de 2024

Bit Software SAS - BITSOFT

LA CIUDAD

Según lo acordado por la empresa Bit Software SAS se deben implementar o llevar a cabo las siguientes políticas en conformidad a la alta gerencia de la empresa.

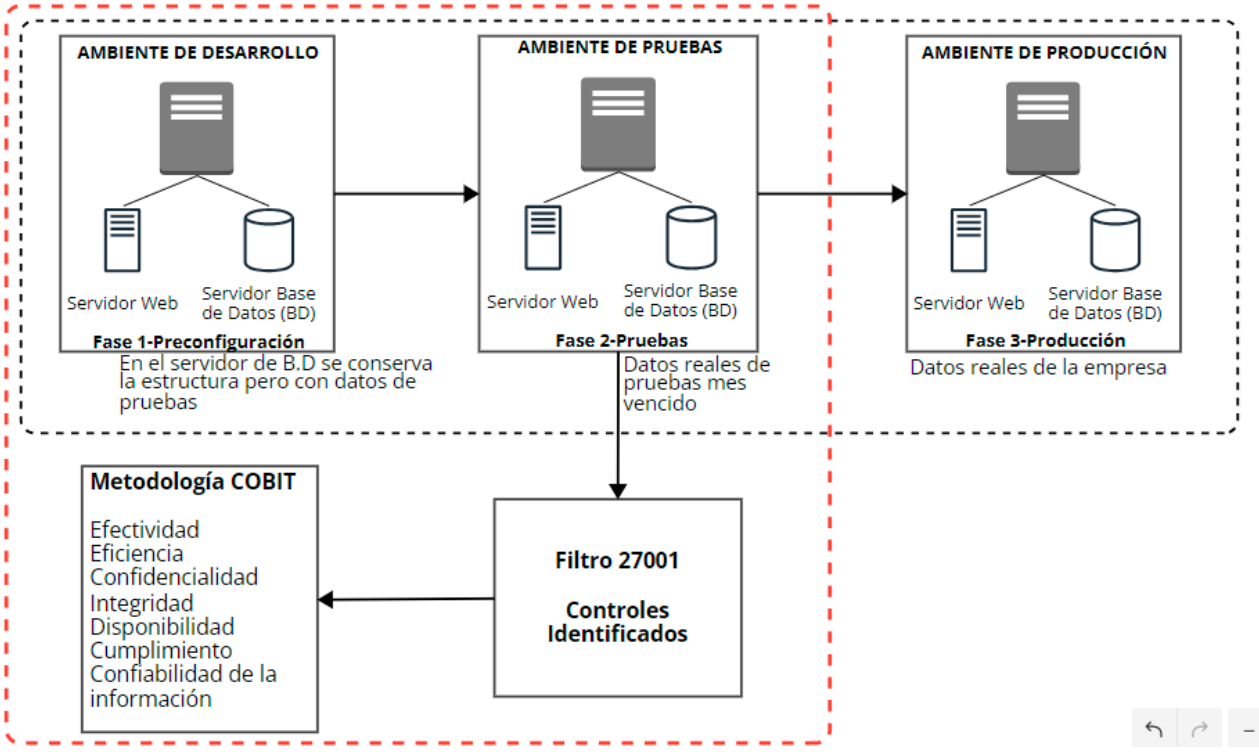
- Ningún usuario que opere el sistema debe tener recursos externos (memorias, disco de almacenamiento, dispositivos móviles).
- Ningún usuario puede ingresar memorias sin estar vacunadas, se ofrece un recurso para la revisión en caso de estar infectada.
- A nivel de correo se deshabilita el anexo de archivos para el equipo de desarrollo de software.
- Todas las máquinas deben tener deshabilitada a conexión por medio USB, SD, Micro SD y cámara web para evitar la fuga de información.
- Uso de cámara web detrás de cada programador.
- Avisos en las paredes que toda sesión están gradabas en las instancias de los equipos.
- Solo se puede hacer uso de dispositivos electrónicos que pertenezcan a la organización.
- Conexiones Virtual Private Network (VPN), o red privada virtual.

Aplicación de la propuesta

En el siguiente diagrama se indica la innovación o el aporte de la aplicación del roadmap en la investigación para la empresa Bitsoft. El estado o proceso actual de la empresa se ve reflejado en la línea negra, según la Figura 15, y se confirma que el problema funcionó, como se evidencia con los elementos utilizados en el desarrollo de la metodología en la línea roja.

Figura 15

Ambientes y procesos actuales en línea negra de Bitsoft - Aporte en línea roja según el proceso



Descripción de los resultados

Este roadmap con un grupo de datos, en un periodo de dos meses, arroja el reporte de acuerdo con lo que se indica en la Figura 14. Valoración de riesgo con un porcentaje de probabilidad de nivel del riesgo del 76%-100% y se aplican los siguientes controles referenciados en la Tabla 9. El resultado va en función de disminuir el problema e impacta en las variables y estas, a su vez, en el problema. El uso de las metodologías de otros autores ayuda a innovar y el beneficio es el mismo. En esta contribución se puede evidenciar que las estrategias de mitigación o reducción de la probabilidad que se materialice una amenaza son: puede ser libre o aplicado al roadmap con base en la ISO 27001 o COBIT, con el fin de minimizar el nivel de riesgo. Ante una situación, se optó por una metodología libre, aplicando controles específicamente a aquellas amenazas que se presentan como críticas (véase Tabla 9).

Discusión

Se ha visto que el roadmap es lo suficientemente flexible y específico para las aplicaciones de las empresas pymes de desarrollo en línea y cuadra perfectamente según las necesidades requeridas.

Para la identificación de los activos, no es necesario recurrir a las plantillas o referencias de la metodología de análisis de riesgo Magerit, sino a las plantillas del roadmap.

Se ha desarrollado y aplicado un roadmap de desarrollo en línea para ayudar a las empresas en el análisis de riesgos más ágil en el SGSI, pues era uno de los problemas observados en el estado del arte con las metodologías actuales.

Se ha encontrado que el activo código de seguridad probado semanalmente en la evaluación de las características COBIT cumple con algunas mediciones, aunque se tiene una infraestructura, no está correctamente aplicado, y existirá un riesgo latente en este tipo de información. Lo anterior, se ha corregido con la aplicación del roadmap.

Se presenta un roadmap personalizado, solo se tendrán en cuenta los activos que se pueden dar en las empresas de desarrollo de aplicaciones en línea.

Conclusiones

Con la adopción del roadmap para implantar el Sistema de Gestión de Seguridad de la Información y gestionar la seguridad de la información en una organización ISO 27001:2013, se permite identificar los activos informáticos a proteger o resguardar (información sensible) y que forman parte fundamental en la elaboración de los diferentes procesos organizacionales, determinando el impacto y riesgo obtenido de la posible materialización de las diferentes amenazas en un ámbito 100% en aplicaciones en línea.

Se confirma que el problema funcionó, se pudo disminuir la variable identificada en la problemática según el aporte de la Figura 15. Conociendo los resultados y el análisis de lo identificado en el estado del arte, existen características similares de la roadmap que tiene algunos controles que se están utilizando; ello indica que se están resolviendo problemas muy similares.

La implementación de los mecanismos y controles sugeridos en este documento permite a la alta gerencia organizar la seguridad de la información adecuándose a los objetivos estratégicos de la naturaleza de la organización, estableciendo diferentes lineamientos que apoyen su gestión y permitan reducir la aceptación del riesgo a un nivel mínimo.

Las políticas, procedimientos y controles, conforme al estudio realizado en el proyecto, se presentan como elementos para una administración y operación eficiente, como los apartados de la norma ISO 27001. Se mencionan algunos como el uso aceptable de los activos, inventarios de activos, gestión de claves, capacitación y política de control de acceso, del Sistema de Gestión de Seguridad de la Información, y deben ser adecuados, según la madurez que adquiera el SGSI, con el fin de la mejora continua.

Como aportación al proyecto, se definió un modelo de riesgo basado en el cálculo de probabilidad de ocurrencia de las amenazas que puedan afectar a lo(s) activo(s) informáticos de la organización objeto de estudio. A lo anterior, se permite identificar el nivel de riesgo asociado y clasificarlo según la escala establecida en la Tabla 6. Este nivel de amenaza detectada se emplea como base fundamental para implementar medidas de control o salvaguarda relacionadas con el objetivo de mitigar los riesgos identificados.

Trabajo futuro

Esta investigación se realizará con el enfoque de las características de COBIT 3, mientras se actualiza esta metodología, se toma como base y se va escalando el proyecto para robustecer los sistemas de gestión de la seguridad de la información y su mejora continua.

Podrán existir políticas, controles y escalamiento de la seguridad informática en el aseguramiento de la información; sin embargo, es fundamental realizar esfuerzos en términos de capacitación, sensibilización o entrenamiento para conocer la importancia del universo de los datos.

En el presente trabajo, se han aplicado (estudiado y resumido) las metodologías en el proceso de la gestión de seguridad, como son ISO 27001, el modelo PDCA y las características COBIT 3. Estas dos metodologías contribuyen a proteger la información personal sensible durante los distintos procesos en los que los datos son tratados u operados por otras entidades. Si bien es relevante que las metodologías se vayan perfeccionando con nuevas versiones, lo primordial es salvaguardar los datos sensibles y garantizar su adecuada protección.

Sin embargo, existen otras metodologías muy importantes y utilizadas que aportan aspectos o detalles diferentes a las metodologías analizadas o estudiadas, permitiendo complementarlas. En este caso, cabría destacar la metodología OCTAVE que, en futuras versiones de este trabajo de investigación, debería ser estudiada en profundidad para el aporte de nuevos puntos de vista, argumentos y características a los SGSI.

El roadmap diseñado es un factor muy importante al momento de garantizar que dicha metodología cubre los aspectos mínimos relevantes en la protección de los datos personales de terceros para los que fue diseñado; se obtienen resultados adecuados en su implementación y una aceptación por la alta gerencia o directiva. Para validarlo, es necesario contar con procesos de auditorías, diseño e implementación de un prototipo que permita conocer la madurez exacta de los controles o políticas propuestas en su desarrollo y aplicación en los procesos en recursos o sistemas en línea. Dicho prototipo deberá crearse en un entorno real y dependerá del presupuesto de la organización.

Nota de los autores

El presente artículo, producto de una investigación, es un desarrollo del trabajo de grado titulado Implementación de una metodología para asegurar información en desarrollos de aplicaciones en línea, presentado a la Universidad de La Rioja para optar al título de Magister en ciberseguridad en el 2021.

Referencias

Alemán-Novoa, C. I. (2015). *Metodología para la implementación de un SGSI en la fundación universitaria Juan de Castellanos, bajo la norma ISO 27001:2005*. [Tesis de maestría, Universidad Internacional de La Rioja]. Repositorio Digital reunir.

Andrés, A., & Gómez, L. (2012). *Guía de aplicación de la Norma UNE-ISO/IEC 27001 sobre seguridad en sistemas de información para pymes*. https://varios.cen7dias.es/documentos/documentos/90/iso.pdf

Bautista Torres, L. A. (2012). *Plan de seguridad de la información compañía XYZ soluciones*. [Tesis de maestría, Universitat Autònoma de Barcelona]. https://openaccess.uoc.edu/bitstream/10609/19443/2/TFM_ENT05_

Botero Vega, D. H. (2016). *Diseño del Sistema de Gestión de Seguridad Informática y de la Información (SGSI) para la empresa Belisario Ltda. de la ciudad de Bogotá, D. C*. [Proyecto de grado, Universidad Nacional Abierta y a Distancia]. Repositorio Institucional UNAD

Ingeniería de Calidad (4 de octubre, 2024) *Ciclo de Deming: Metodología de mejora continua | PDCA - PHVA*. https://www.ingenieriadecalidad.com/2020/02/ciclo-de-deming.html

COBIT. (1996). *COBIT Marco referencial* (3a ed.). Emitido por el Comité Directivo de COBIT y el IT Governance Institute (pp. 1-72). http://files.uladech.edu.pe/docente/02659781/CAT/S07/02_03MarcoReferencial.pdf

Fisher, R. (1988). *Seguridad en los sistemas informáticos*. Ediciones Díaz de Santos.

García, R. (2013, 13 de noviembre). *La información es el activo más importante para las empresas actualmente*. C de comunicación https://logistica.cdecomunicacion.es/noticias/sectoriales/7029/la-informacion-esel-activo-mas-importante-para-la-empresas

Giudice, O. F., Fauquex, J., Scotti, S., & Yelen, M. (2011). Protección de los datos personales de la historia clínica en Argentina y Uruguay e IHE XDS. *Journal of Health Informatics*, *3*. https://jhi.sbis.org.br/index.php/jhi-sbis/article/view/166

Gómez Fernández, L., & Fernández Rivero, P. P. (2018). *Cómo implantar un SGSI según UNE-EN ISO/IEC 27001 y su aplicación en el Esquema Nacional de Seguridad.* Editorial Aenor Conocimiento, S.L.U.

Hussain, S., Anwaar, H., Sultan, K., Mahmud, U., Farooqui, S., Karamat, T., & Toure, I. K. (2024). Mitigating software vulnerabilities through secure software development with a policy-driven waterfall model. *Journal of Engineering*, *2024*, 1-15. Article ID 9962691-https://doi.org/10.1155/2024/9962691

Hiscox (2023). *Informe de Ciberpreparación de Hiscox*. https://www.hiscox.es/sites/spain/files/2023-10/22594%20-%20Cyber%20Readiness%20Report%202023%20-%20Spanish.pdf

ESGinnova Group (2015, marzo 30). *ISO 27001: los activos de información*. https://www.pmg-ssi.com/2015/03/iso-27001-los-activos-deinformacion/

Kerr, C., & Phaal, R. (2022). Roadmapping and roadmaps: Definition and underpinning concepts, *IEEE Transactions on Engineering Management, 69*(1), 6-16. https://doi.org/10.1109/TEM.2021.3096012

Ley 1581 de 2012. "Por la cual se dictan disposiciones generales para la protección de datos personales". https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981

Ministerio de Hacienda y Administraciones Públicas (2012). *Magerit - versión 3.0: Metodología de análisis y gestión de riesgos de los sistemas de información. Libro I: Método.* Editorial del Ministerio de Hacienda y Administraciones Públicas

MINTIC. (2016). *Guía para la Gestión y Clasificación de Activos de Información*. https://gobiernodigital.mintic.gov.co/692/articles-150528_G5_Gestion_Clasificacion.pdf

Mujica, M., & Álvarez, Y. (2009). El análisis de riesgo en la seguridad de la información. *Publicaciones en Ciencias y Tecnología*, *4*(2), 33-37. https://revistas.uclave.org/index.php/pcyt/article/view/1086

Muñoz Periñán, I. L., & Ulloa Villegas, G. (2011). Gobierno de TI – Estado del arte. *Sistemas & Telemática*, *9*(17), 23-53. https://www.redalyc.org/articulo.oa?id=411534384003

Kaspersky (2023, 23 de agosto). *Nueva epidemia: el phishing se sextuplicó en América Latina con el reinicio de la actividad económica y el apoyode la IA*. Kaspersky daily https://latam.kaspersky.com/blog/panorama-amenazas-latam-2023/26586/

Pinzón Parada, I. (2014). *Gestión del riesgo en seguridad informática.* Universidad Piloto de Colombia. [Tesis de posgrado, Universidad Piloto de Colombia]. Repositorio Unipiloto

Trías, M., González, P., Fajardo, S., & Flores, L. (2019). *Las 5 W + H y el ciclo de mejora en la gestión de procesos*. LATU (Laboratorio Tecnológico del Uruguay). https://ojs.latu.org.uy/index.php/INNOTEC-Gestion/article/view/5/4