Polo del Conocimiento

Pol. Con. (Edición núm. 67) Vol. 7, No 2
Febrero 2022, pp. 894-910
ISSN: 2550 - 682X
DOI: 10.23857/pc.v7i1.3625

Evaluación de riesgos de seguridad de la información. Caso de estudio: Empresa Cognoware CIA. LTDA.

Information security risk assessment. Case Study: Cognoware Company

Avaliação de riscos de segurança da informação. Estudo de caso: Empresa Cognoware CIA. LTDA.

Byron Adrián Ortega-Guillén [I]
byron.ortega.60@est.ucacue.edu.ec
https://orcid.org/0000-0003-1796-3471

Juan Pablo Cuenca-Tapia [II]
jcuenca@ucacue.edu.ec
https://orcid.org/0000-0001-5982-634X

Correspondencia: byron.ortega.60@est.ucacue.edu.ec

Ciencias Técnicas y Aplicadas
Artículo de Investigación

***Recibido:** 02 de enero de 2022 ***Aceptado:** 20 de enero de 2022 * **Publicado:** 11 de febrero de 2022

I. Ingeniero de Sistemas, Estudiante de la Maestría en Ciberseguridad, Unidad Académica de Posgrado, Universidad Católica de Cuenca, Cuenca, Ecuador.
II. Ingeniero de Sistemas, Docente de la Maestría en Ciberseguridad, Unidad Académica de Posgrado, Universidad Católica de Cuenca, Cuenca, Ecuador.

Resumen

La empresa Cognoware Cia. Ltda., tiene como finalidad realizar el análisis de datos y el desarrollo de software de varias instituciones financieras dentro del territorio nacional ecuatoriano y de américa latina. El análisis que se busca realizar, tiene como finalidad, enfocarse en el sector tecnológico de la información, análisis, evaluación, amenaza y tratamiento de riesgos de la empresa, con el objetivo de valorar los activos informáticos existentes mediante un control más robusto en la seguridad y así poder proteger la información; donde, la metodología a utilizar será cuantitativa y cualitativa, considerando de manera referencial los anexos de la ISO/IEC 27001:2013, pues se pretende implementar en la empresa un Sistema de Gestión de Seguridad de la Información, lo que se logrará realizando un análisis y evaluación general de todos los riesgos existentes, además de realizar una valoración junto a un modelo de madurez respecto a los riesgos iniciales; los resultados muestran que la "Gestión de riesgos, la Protección del sistema y las comunicaciones" tienen un cumplimiento del 50% aproximadamente, mientras que el resto de dominios constituidos en el nivel 3 tienen un porcentaje entre el 10 y el 30%, considerando así los puntos que aún quedan por fortalecer. Por lo que se puede establecer que en los niveles objetivos con los que consta la empresa, aún se encuentran falencias, lo que permite ser un indicador que además de tener que incrementar los dos niveles restantes, es indispensable mejorar los niveles ya existentes.

Palabras clave: Valorar; amenaza; riesgo; dominio; gestión de seguridad.

Abstract

The company Cognoware Cia. Ltda., has the purpose of performing data analysis and software development of various financial institutions within the Ecuadorian national territory and Latin America. The analysis that is sought to be carried out has the purpose of focusing on the information technology sector, analysis, evaluation, threat and treatment of risks of the company, with the aim of valuing the existing computer assets through a more robust control in security. and thus be able to protect the information; where, the methodology to be used will be quantitative and qualitative, considering as a reference the annexes of ISO/IEC 27001:2013, since it is intended to implement an Information Security Management System in the company, which will be achieved by performing an analysis and general evaluation of all the existing risks, in addition to carrying out an assessment together with a maturity model with respect to the initial risks; the results show

that "Risk management, system protection and communications" have a compliance of approximately 50%, while the rest of the domains constituted at level 3 have a percentage between 10 and 30%, thus considering the points that still need to be strengthened. So, it can be established that in the objective levels with which the company consists, there are still shortcomings, which allows it to be an indicator that in addition to having to increase the two remaining levels, it is essential to improve the existing levels.

Keywords: Assess; threat; risk; domain; security management.

Resumo

A empresa Cognoware Cia. Ltda., tem como objetivo realizar análise de dados e desenvolvimento de software de diversas instituições financeiras dentro do território nacional equatoriano e da América Latina. A análise que se pretende realizar pretende centrar-se no setor das tecnologias de informação, análise, avaliação, tratamento de ameaças e riscos da empresa, com o objetivo de valorizar os ativos informáticos existentes através de um controlo de segurança mais robusto. capaz de proteger as informações; onde, a metodologia a ser utilizada será quantitativa e qualitativa, tendo como referência os anexos da ISO/IEC 27001:2013, uma vez que se pretende implementar um Sistema de Gestão da Segurança da Informação na empresa, o que será alcançado através da realização de uma análise e avaliação geral de todos os riscos existentes, além de realizar uma avaliação juntamente com um modelo de maturidade quanto aos riscos iniciais; os resultados mostram que "Gestão de riscos, proteção de sistemas e comunicações" apresentam uma conformidade de aproximadamente 50%, enquanto os demais domínios constituídos no nível 3 apresentam um percentual entre 10 e 30%, considerando assim os pontos que ainda precisam ser fortalecidos . Assim, pode-se apurar que nos níveis objetivos em que a empresa se compõe, ainda existem lacunas, o que permite ser um indicador que para além de ter de aumentar os dois níveis restantes, é fundamental melhorar os níveis existentes.

Palavras-chave: Avaliar; ameaça; risco; domínio; gerenciamento de segurança.

Introducción

El análisis del presente artículo tiene como finalidad, enfocarse en el sector tecnológico de la información, análisis, evaluación y tratamiento de riesgos de la empresa Cognoware Cia. Ltda.,

con la finalidad de valorar los activos informáticos existentes mediante un control más robusto en la seguridad y así poder proteger la información; este proceso se debe a que actualmente, los mercados, organizaciones, sociedades, entre otras entidades, han sufrido cuantiosos cambios, por lo que es primordial ser un ente competitivo, buscando ventajas en su desarrollo y la capacidad para ser competentes con la demanda tecnológica que va mejorando a gran escala.

La empresa Cognoware Cia. Ltda. Nace en el año 2013 con 3 socios, con un enfoque en el desarrollo de productos y servicios tecnológicos, la finalidad es brindar soluciones informáticas con tecnologías actuales e innovadoras que permitan resolver los desafíos empresariales y sociales de la nueva era digital.

Actualmente, entre los clientes que han brindado la oportunidad de implementar los productos que ofrece la empresa están: Banco de Loja, Banco del Litoral, Banco del Pacifico, Banco Pichincha, Cooperativa JEP, OSCUS, Cooperativa Riobamba Ltda., Novacredit, Banco Internacional, entre otros.

La empresa ha ido creciendo considerablemente, por lo que este hecho no ha sido previamente planificado, mucho menos controlado, entre sus activos cuenta con una infraestructura física de dos servidores de aplicaciones y base de datos, cinco estaciones de trabajo para desarrolladores, y seis servidores de aplicaciones, seguridad y base de datos en AWS, cuatro colaboradores técnicos que son: Dos desarrolladores backend, un desarrollador frontend, y un especialista de base de datos, además de contratos ocasionales a personal externo para proyectos específicos, en lo que va del año los colaboradores externos han sido cuatro, en respuesta a este fenómeno únicamente se ha compensado con una inversión en tecnología que ayuda en el desarrollo de procesos de software, lo que indica que la implementación en los controles de seguridad de la información ha quedado de lado.

En consecuencia, se pretende implementar en la empresa un Sistema de Gestión de Seguridad de la Información, lo que se logrará realizando un análisis y evaluación general de todos los riesgos existentes en relación con la seguridad de la información, además de realizar una valoración junto a un modelo de madurez respecto a los riesgos iniciales.

Según Guerrero et al. (2020) la implementación de un plan estratégico de seguridad, será fundamental para obtener un informe de la valoración de los activos informáticos que van a ser asegurados, dentro del cual, se realizará un informe adicional aproximado de los costos que requerirá implementar los controles en la seguridad de la información. Un lugar muy importante

es el que ocupa la gestión de riesgos, cuando se habla de un nivel organizacional, y su administración ayuda al: enfoque de procesos y al mejor uso de recursos.

Estado del arte

Tanto en Ecuador, como en Latino América, con respecto a la evaluación de riesgos en las empresas públicas y privadas, se ha reflejado una falta de desarrollo progresivo en el campo de la seguridad informática, y, por ende, el déficit de profesionales en la rama de la seguridad informática, que permitan implementar un sistema de gestión de Seguridad de la Información, acorde a la problemática actual. (BID & OEA, 2020)

En el artículo de Riesgos, avances y el camino a seguir en América Latina y el Caribe, publicado por el Banco Inter Americano de Desarrollo, indica que desde el año 2016 hasta el 2020, en los cinco apartados que se realizan las métricas y con niveles del 1 al 5 en cada una, se evidencia un avance de 1 punto con relación al periodo anterior, sin embargo, en la mayoría de estos apartados, no se llega a los valores aceptables de la seguridad de la Información. (BID & OEA, 2020)

Además, en el mismo artículo publicado por el (BID & OEA, 2020) indica que: Si bien Ecuador aún no cuenta con una estrategia de seguridad cibernética, sí ha logrado hacer avances significativos en la mejora de sus capacidades cibernéticas y en el enfrentamiento de amenazas, apoyado por el establecimiento de un grupo de trabajo para el desarrollo de la estrategia nacional de ciberseguridad. (p. 13)

Según una publicación realizada por el diario El Comercio indica que la compañía de seguridad informática ESET indicó que "en Ecuador hubo más de 51 mil registros relacionados con cryptominers (malware utilizado para la minería de criptomonedas), alrededor de 140 mil detecciones de exploits (código utilizado para aprovechar vulnerabilidades en software), cerca de seis mil detecciones de ransomware (malware para el secuestro de información) y casi ocho mil detecciones de spyware (software espía), como datos de algunos tipos de software malicioso". (El Comercio, 2021)

Con estos antecedentes, se puede determinar que Ecuador a pesar de ser un país con un porcentaje de compenetración del internet de la población de un 57% (BID & OEA, 2020), es el objetivo de un gran número de ciberataques, de ahí la importancia de que las empresas empleen una estrategia de ciberseguridad adecuada.

Una medición de madurez elaborada por (Ramírez, 2016), indicó en el estudio realizado en MiPymes colombianas, que únicamente el 11.4% de las empresas que se consideraron en su

análisis, tenían un Sistema de gestión de seguridad de la información o más conocido como "SGSI" establecido de manera formal, el 63.3% no consta con un sistema establecido y el restante 25.3% se consideraría como el grupo que tiene un sistema y control de manera inconstante.

Por esta razón se indica que la mayoría de las empresas están a favor de la importancia que conlleva la seguridad cibernética, sin embargo, al conocer los costos de inversión en este tema, aun conociendo el riesgo de ser blancos de los delincuentes informáticos, este porcentaje no es tan alto. (Ramírez, 2016)

Concluyendo de esta manera, (Ramírez, 2016) a pesar de que existan un sin número de diferentes modelos de madurez, muy pocos son los que se ajustan a las necesidades enfocadas a las MiPymes, por lo que únicamente el 11%, ha establecido de manera formal un SGSI, debido a lo que conlleva hacerlo, es decir la inversión económica, el esfuerzo, los recursos y el tiempo necesario para su implementación.

En otro análisis del modelo de madurez, pero esta vez enfocado en el área de la salud, (Pérez & Salcedo, 2021), indican que al realizar una comparativa entre los controles elaborados por ellos y las fuentes en NIST Cybersecurity, con un margen de error de ±1 punto, existió una mínima diferencia que estaría acorde al margen de error, por lo que se pudo observar que el análisis realizado en la ciberseguridad, privacidad y gestión de datos de salud, facilita el monitoreo, control y sobre todo en el cumplimiento de las normativas y de las prácticas.

Sin embargo, el nivel de desarrollo en la que se encuentran llega a un nivel 2, que es indicador de aspectos aun por mejorar en el cumplimiento de las normativas de la salud, y por esta razón se comprende que existe una aceptación válida en este modelo, con un promedio de 4.6/5.0 del cual se estableció un análisis. (Pérez & Salcedo, 2021)

Marco teórico referencial

Sistema de gestión de seguridad de la información (SGSI). Según la normativa ISO 27001 (2013) cuando se habla de un sistema de gestión para la Seguridad de la información, ésta se compone de una serie de procesos en la que se podría implementar, mantener y mejorar de forma continua la seguridad de la información, y esto se puede lograr utilizando los riesgos que afecten a la seguridad de la información en una determinada empresa u organización.

ISO/IEC 27001. Es una normativa aprobada y publicada por International Organization for Standardization e International Electrotechnical, 2005 contiene parámetros para la seguridad de la información. (ISO, 2013)

Seguridad de información. Preservación de la confidencialidad, integridad y disponibilidad de la información. (ISO, 2013)

Disponibilidad. En este caso se hace referencia con la propiedad para poder hacer posible y utilizable a partir de una solicitud de una entidad autorizada. (ISO, 2013)

Confidencialidad. Al hablar de confidencialidad se dice que es la propiedad en la que la información en general ya sea de una persona o de una empresa no se pondrá a disposición o se divulgará la misma a personas, entidades o procesos que no estén autorizados.

Integridad. Cuando se habla de integridad de la información, se hace referencia al compromiso en la confidencialidad de datos, este hecho tiene una relación con una normativa, en la misma que indica cómo debe hacerse el cumplimiento del RGPD, y este únicamente se puede dar por medio de un conjunto de procesos, reglas y algunas normas que deberán mantenerse vigentes durante todo su proceso. (ISO, 2013)

Control. Aplica a las medidas de seguridad, ya sean técnicas o administrativas las mismas que pueden ayudar a disminuir las amenazas que pueden actuar debido a una vulnerabilidad. (ISO, 2013)

Objetivo de control. Tras implementar algún sistema de control, lo que ayudará este objetivo es realizar una descripción sobre el contexto al que se debe llegar como resultado de esta modificación en el sistema. (ISO, 2013)

Riesgo. Al hablar de un efecto de riesgo, se hace referencia a la incertidumbre o duda que se puede generar a partir de los objetivos, adicionalmente existe una probabilidad sobre un impacto que desvíe el resultado previsto durante el análisis, el mismo que puede ser positivo o negativo según sea el caso, por último, se puede deducir que el riesgo general o parcial depende de la información relacionada o comprensión de un nuevo evento. (ISO, 2013)

Evaluación de riesgo. Es un proceso en el que se puede comparar los diferentes tipos de resultados obtenidos en el análisis de riesgo realizado previamente, con la finalidad que pueda ayudar a tomar una decisión sobre cómo enfocar el tratamiento de los riesgos. (ISO, 2013)

Identificación de riesgo. En este apartado, es necesario realizar un proceso en el que se debe incluir una búsqueda, la misma que ayudará a identificar el riesgo o sus fuentes, posteriormente un

reconocimiento en la que se detallará la causa de los eventos que puedan estar sucediendo, y, por último, la descripción de riesgos en la que puede estar incluido datos históricos, análisis y opiniones de expertos en el tema. (ISO, 2013)

Tratamiento de riesgo. Según la normativa ISO 27001 (2013) existe un proceso en el que se puede modificar el riesgo, sin embargo, es necesario entender cuál es el tratamiento del riesgo que se puede involucrar:

- Evitar el riesgo al decidir no comenzar o continuar con la actividad que genera el riesgo.
- Tomar o aumentar el riesgo para buscar una oportunidad.
- Eliminar la fuente de riesgo.
- Cambiando la probabilidad.
- Cambiando las consecuencias.
- Compartir el riesgo con otra parte o partes.
- Retener el riesgo por elección informada.

Vulnerabilidad. En el contexto de vulnerabilidad se puede incluir algunos detalles, sin embargo, el principal enfoque es el que engloba la debilidad en el contexto de la seguridad que puede ser explotado por varias amenazas. (ISO, 2013)

Probabilidad. Hace referencia al riesgo que pueda suceder u ocurrir en algún evento, produciendo una amenaza contra la seguridad de la información. (ISO, 2013)

Frecuencia. Es un parámetro que puede ayudar a un pronóstico con la que un evento puede volver o no a ocurrir. (ISO, 2013)

Metodología

La metodología utilizada fue cuantitativa y cualitativa, considerando de manera referencial los anexos de la ISO/IEC 27001:2013.

Se realizó la evaluación de riesgos de la información, donde se utilizaron cuestionarios y entrevistas realizadas a los funcionarios correspondientes al desarrollo de sus actividades. También se utilizaron diferentes fuentes de información, tales como tesis, textos, revistas, y documentos en medios electrónicos.

En la investigación se tomaron como fuente de información primaria, al gerente general y los funcionarios del área de Análisis de Datos y Desarrollo de Software de la empresa Cognoware Cia. Ltda., y se emplearon los elementos y las secciones más importantes a tener en cuenta para

seleccionar la información referente con la finalidad de ayudar a mejorar la seguridad informática de los clientes, por medio de la implementación de nuevas maneras de seguridad.

Para este proceso es importante entender la Fig. 1, en la que se puede visualizar la secuencia con la que se aplicó esta metodología, en donde se empieza con el reconocimiento de la empresa, posteriormente se verifica el cumplimiento de la implementación de la Certificación del modelo de madurez de ciberseguridad o "CMMC", posteriormente se valoraron los activos de la información de la empresa y se procedió con la evaluación de los riesgos sobre los activos.

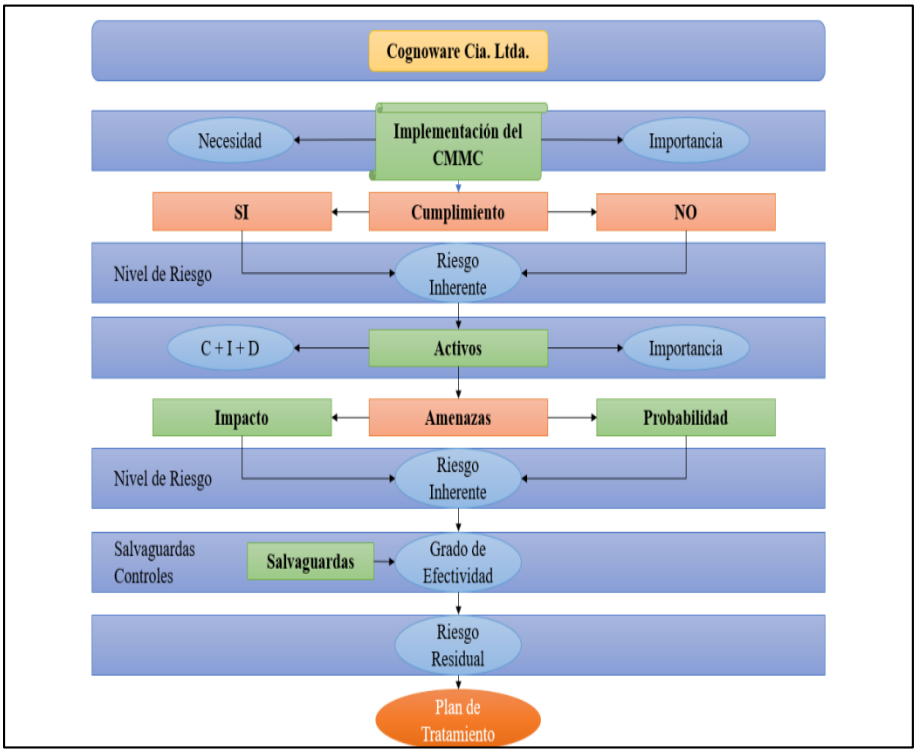

Fig. 1. Flujo de la metodología de aplicación

Fases de implementación

En este apartado se considera el desarrollo de una manera de emplear la metodología cuantitativa, con un proceso estructurado en una secuencia de varios pasos indicados en la Fig. 2.

Pol. Con. (Edición núm. 67) Vol. 7, No 2, febrero 2022, pp. 894-910, ISSN: 2550 - 682X

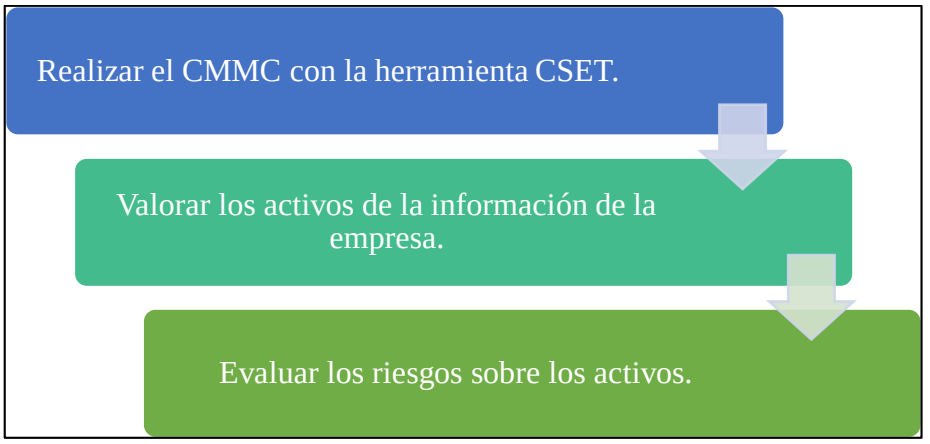

Fig. 2. Pasos de la metodología a implementar

Nivel objetivo de evaluación dentro de las prácticas y procesos de CMMC

El modelo CMMC mide la madurez de la ciberseguridad con cinco niveles. Cada uno de estos niveles, a su vez, consta de un conjunto de procesos y prácticas que se caracterizan en la Fig. 3. Los procesos van desde "Realizado" en el Nivel 1 hasta "Optimización" en el Nivel 5 y las prácticas van desde la "Ciber Higiene Básica" en el nivel 1 a "Avanzado / progresivo" en el nivel 5.

Los niveles de CMMC y los conjuntos de procesos y prácticas asociados en todos los dominios son acumulativos. Más específicamente, para que una organización logre un nivel CMMC específico, también debe demostrar el logro de los niveles inferiores anteriores.

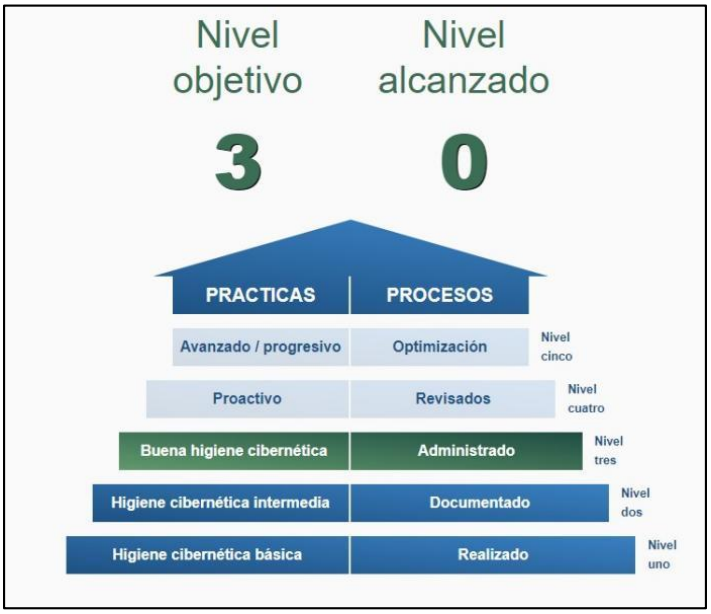

Fig. 3. Nivel objetivo de evaluación

Resultados y discusión

Valoración de Activos de Información de la Empresa

Para la valoración de los activos de información, se utilizará la matriz mostrada en la Tabla 1, que hace referencia a la valoración según el impacto, posteriormente en la matriz de la Tabla 2, se muestra la valoración según su confidencialidad, y finalmente, la matriz de la Tabla 3, muestra el resultado de su importancia.

Tabla 1. Valoración de activos según el impacto.

VALOR		DESCRIPCIÓN
BAJO	1	El daño o modificación no autorizada de información que maneja el activo no tendrá consecuencias negativas para la Organización.
MEDIO	2	El daño o modificación no autorizada a la información que maneja el activo tiene consecuencias moderadas para la Organización.
ALTO	3	El daño o modificación no autorizada a la información que maneja el activo tiene consecuencias severas y presenta pérdidas económicas.

Tabla 2. Valoración de activos según su confidencialidad

CLASIFICACIÓN	DESCRIPCIÓN
CONFIDENCIAL	Información de alta sensibilidad que debe tener acceso personal autorizado
USO INTERNO	Información sensible, acceso controlado y solo con autorización personal interno.
PÚBLICA	Información que puede conocerse por personal interno o externo.

Tabla 3. Resultados importantes de la valoración de activos

IMPORTANCIA		DESCRIPCIÓN
PRESCINDIBLE	1	En caso de pérdida o difusión no autorizada hay una baja probabilidad de pérdida en la situación organizacional actual.
IMPORTANTE	2	En caso de pérdida o difusión no autorizada hay una posible probabilidad de pérdida de reputación, imagen y credibilidad.
GRAVE	3	En caso de pérdida o difusión no autorizada hay una alta probabilidad de perdida de objetivos estratégicos y metas del proceso o procesos vinculados.

Pol. Con. (Edición núm. 67) Vol. 7, No 2, febrero 2022, pp. 894-910, ISSN: 2550 - 682X

Este informe ilustra la postura de madurez de la seguridad de la información en toda la organización. Donde se puede observar que en la Fig. 4, Fig. 5 y Fig. 6, se muestra el progreso de la organización a lo largo de CMMC según el nivel objetivo individual y la evaluación general de ciberseguridad.

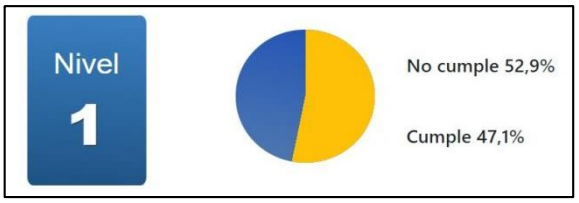

Fig. 4. Proteger la información del contrato federal (FCI)

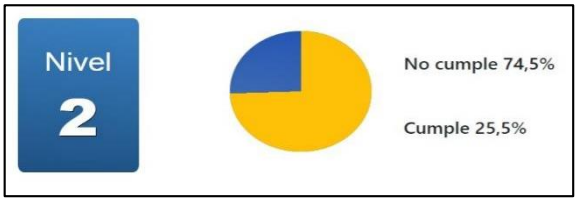

Fig. 5. Sirve como un paso de transición en la progresión de la madurez

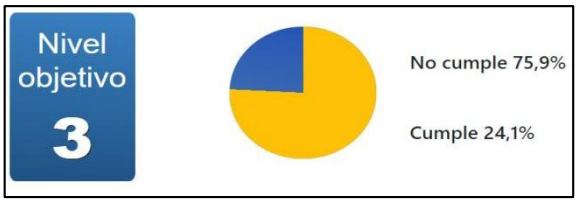

Fig. 6. Proteger la información no clasificada controlada (CUI)

Como dato adicional se elaboró un desglose de la puntuación de cumplimiento, en el que se muestra el número de prácticas satisfechas para cada nivel, como se puede observar en la Fig. 7.

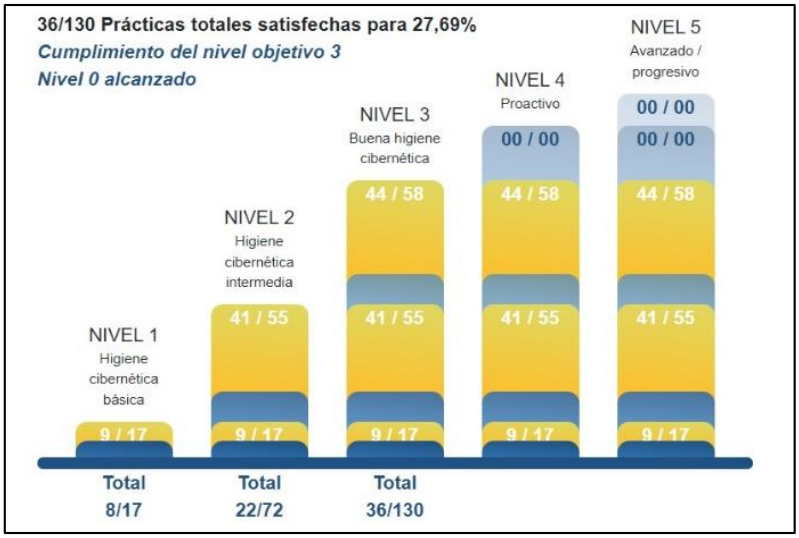

Fig. 7. Desglose de la puntuación de cumplimiento

Como se observa al analizar la Fig. 7, el análisis se realizó a los 3 niveles iniciales, donde es importante entender que en el nivel 1, con relación a la protección de la información del contrato federal (FCI) cumple en un 47,1% mientras que el porcentaje restante no cumple con este apartado; en el nivel 2, que indica si sirve como un paso de transición en la progresión de la madurez de la seguridad cibernética para proteger CUI cumple alrededor del 25,5% mientras que el 74,5% no la cumple; y finalmente se tiene en el nivel 3, que trata sobre la protección de la información no clasificada controlada (CUI) cumple un porcentaje mínimo del 24,1% ,mientras que el restante 75,9% no la cumple.

Para una comprensión que permita entender la razón por la que se analizó hasta el nivel 3, en la Fig. 8, se puede observar que los tres primeros niveles son los únicos que se están cumpliendo en la actualidad, por lo que para analizar los niveles siguientes primero se deberá reforzar los niveles iniciales para poder obtener información de los siguientes niveles restantes.

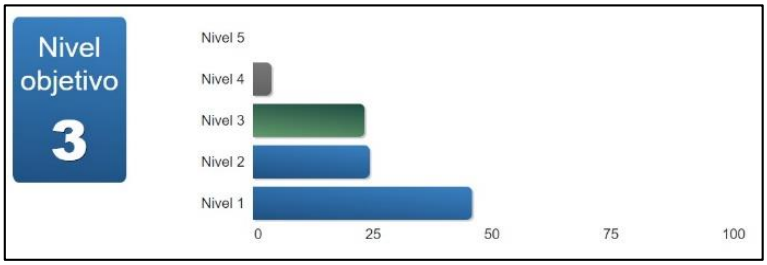

Fig. 8. Porcentaje alcanzado por los 5 niveles objetivos

Pol. Con. (Edición núm. 67) Vol. 7, No 2, febrero 2022, pp. 894-910, ISSN: 2550 - 682X

Según las representaciones gráficas extraídas de la evaluación, se puede verificar que se implementaron múltiples niveles de madurez que van desde "Higiene de ciberseguridad básica" hasta "Buena Cyber Higiene", también expresada como "Realizada" a "Gestionada", debido a que el nivel objetivo alcanzado es el nivel 3, como se muestra en la Fig. 8; sin embargo, en la Fig. 9 se muestra el cumplimiento de CMMC por dominio.

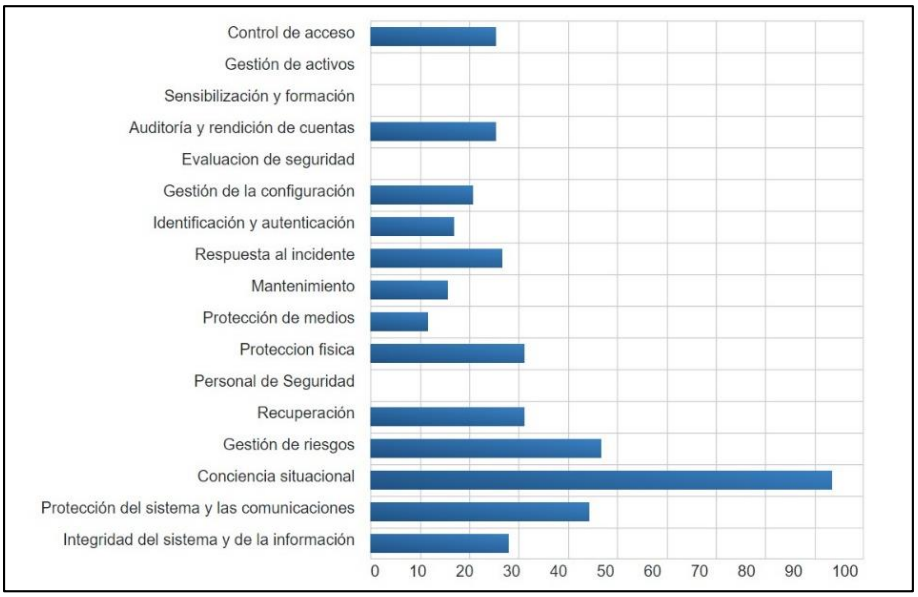

Fig. 9. Porcentaje de cumplimiento de CMMC para cada dominio del nivel 3.

Según la interpretación obtenida a partir de la Fig. 9, se puede distinguir que la “Conciencia Situacional” tiene un mayor porcentaje de cumplimiento, tanto la “Gestión de riesgos, la Protección del sistema y las comunicaciones” tienen un cumplimiento del 50% aproximadamente, mientras que el resto de dominios constituidos en el nivel 3 tienen un porcentaje entre el 10 y el 30% considerando así los puntos que aún quedan por fortalecer.

Una vez indicado los resultados obtenidos, en la Fig. 10, se puede identificar una evidencia que consiste en un total de 30 activos valorados, donde 1 de ellos es prescindible pues representa un 4%, posteriormente 16 activos que representan el 53% son importantes, y finalmente 13 activos que representan el 43% son graves.

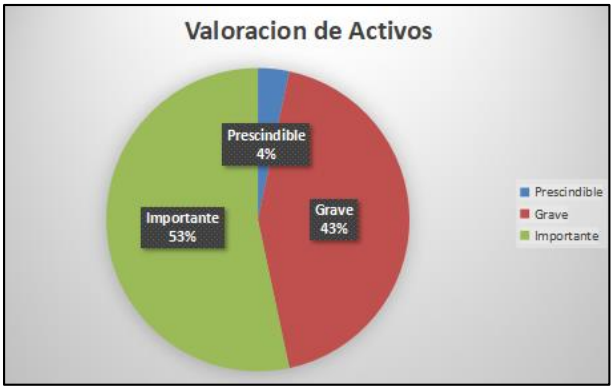

Fig. 10. Resultado valoración de activos

En la Fig. 11, se muestra un análisis de riesgos iniciales, en donde se observa una evidencia que de un total de 69 amenazas detectadas de los activos valorados como graves, 37 son considerados como riesgo moderado, lo mismo que representa el 54%, mientras que 32 son considerados como riesgo alto, y representan el 53%.

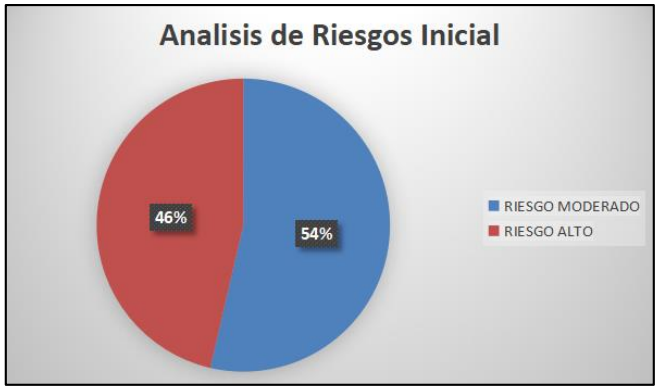

Fig. 11. Resultado del análisis de riesgo inicial, antes del tratamiento del riesgo.

Una vez realizado todo el análisis y luego de haber realizado el tratamiento adecuado del riesgo con la aplicación de los controles, lo que se pretende es que las amenazas de riesgo alto desaparezcan, mientras que las amenazas que tienen in riesgo moderado o bajo disminuyan en un 90 %.

Es por eso que en la Tabla 4, y según la normativa (ISO, 2013), se intenta mantener la seguridad de la información en las organizaciones, realizando una evaluación y evaluación de riesgos, para

que esto sea posible es necesario considerar la implementación de algunos controles de seguridad, transferir riesgos, evitar riesgos y por último aceptar el riesgo en cuestión.

Tabla 4. Controles de seguridad a aplicar para el tratamiento de riegos

CONTROLES DE SEGURIDAD - ISO-IEC 27001-2013
A.11.1.4 - PROTECCIÓN CONTRA AMENAZAS EXTERNAS Y DEL AMBIENTE
A.11.2.2 - SERVICIOS DE APOYO
A.11.2.4 - MANTENIMIENTO DEL EQUIPAMIENTO
A.12.1.1 - PROCEDIMIENTOS DOCUMENTADOS DE OPERACIÓN
A.12.3.1 - RESPALDOS DE LA INFORMACIÓN
A.12.5.1 - INSTALACIÓN DE SOFTWARE EN LOS SISTEMAS OPERATIVOS
A.12.6.1 - GESTIÓN DE VULNERABILIDADES TÉCNICAS
A.14.2.2 - PROCEDIMIENTOS DE CONTROL DE CAMBIOS DEL SISTEMA
A.7.2.2 - CONCIENTIZACIÓN, EDUCACIÓN Y FORMACIÓN EN SEGURIDAD DE LA INFORMACIÓN
A.8.2.1 - CLASIFICACIÓN DE LA INFORMACIÓN
A.9.2.3 - GESTION DE DERECHOS DE ACCESO PRIVILEGIADO
A.9.2.5 - REVISIÓN DE LOS DERECHOS DE ACCESO DE LOS USUARIOS
A.9.4.1 - GESTION DE DERECHOS PRIVILEGIADOS
A.9.4.3 - SISTEMA DE GESTIÓN DE CONTRASEÑAS
A9.1.1 -REVISIÓN DE LOS DERECHOS DE ACCESO DE LOS USUARIOS

Conclusiones

- Se pudo identificar los niveles de madurez de la ciberseguridad con el modelo CMMC, con lo que se observa que la empresa Cognoware Cia. Ltda., por más que incremente su tecnología, aún tiene falencias en su ciberseguridad, por lo que es propensa a tener errores o fallos debido a ataques cibernéticos.
- Se estableció que en los niveles objetivos con los que consta la empresa, aún se encuentran falencias, lo que permite ser un indicador que además de tener que incrementar los dos niveles restantes, es indispensable mejorar los niveles ya existentes.
- Se recomienda realizar un plan de implementación de controles de seguridad en toda el área de Tecnología de la empresa Cognoware Cia. Ltda., con la finalidad de garantizar el servicio ofrecido a sus clientes, debido a que están expuestos a múltiples ataques de ciberseguridad.
- La valoración de activos muestra que existe un riesgo grave de nivel elevado, por lo que es recomendable tomar acciones en este aspecto, al igual que el riesgo inicial se encuentra en condiciones elevadas; por este motivo es indispensable que se mejoren estos aspectos.

Referencias

1. BID, B. I., & OEA, O. d. (2020). Ciberseguridad, Riesgos, avances y el camino a seguir en Amerca Latina y el caribe. Obtenido de https://publications.iadb.org/publications/spanish/document/Reporte-Ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-America-Latina-y-el-Caribe.pdf
2. El Comercio. (29 de 07 de 2021). Ecuador está entre los países con más ciberataques en América Latina. Obtenido de https://www.elcomercio.com/tendencias/tecnologia/ecuador-ciberataques-america-latina-hacker.html
3. I. 2. (2013). REFERENCIAS NORMATIVAS ISO 27000. Obtenido de https://normaiso27001.es/referencias-normativas-iso-27000/#def364
4. Pérez, H., & Salcedo, H. (18 de Marxo de 2021). Modelo de madurez en ciberseguridad para empresas que manejan datos de salud. Obtenido de https://repositorioacademico.upc.edu.pe/bitstream/handle/10757/655801/PérezN_H.pdf?sequence=3&isAllowed=y
5. Ramírez, B. (2016). Medición de madurez de CiberSeguridad en MiPymes colombianas. Obtenido de https://repositorio.unal.edu.co/bitstream/handle/unal/57956/80245271.2016.pdf?sequence=1&isAllowed=y