RESUMEN – TRABAJO DE GRADO

AUTORES	**Diego Armando Cervantes Ramos** **Karen Dayana Ortiz Ortiz**
FACULTAD	**Ingeniería**
PLAN DE ESTUDIOS	**Ingeniería de Sistemas**
DIRECTOR	**Luis Fernando Morales Martínez**
TÍTULO DE LA TESIS	**Sistema de Gestión del Riesgo de Seguridad Informática para Beneficiar la Operación del Servicio en Empresas Ubicadas en Ocaña Norte de Santander.**
TITULO EN INGLES	Information Security Risk Management System to Benefit the Operation of the Service in Companies Located in Ocaña Norte de Santander.

RESUMEN
(70 palabras)

El Sistema de Gestión de Riesgos de Seguridad Informática, tiene como finalidad facilitar a las empresas ubicadas en el municipio de Ocaña, Norte de Santander en la mejora de los procesos de seguridad informática y el beneficio de las operaciones de servicios de cada entidad, para que estas no se detengan o se encuentren comprometidas debido a un ataque de seguridad informático presentado.
Este Sistema mantendrá la información de forma segura y mitiga el riesgo significativamente.

RESUMEN EN INGLES

The purpose of the Information Security Risk Management System is to facilitate the companies located in the municipality of Ocaña, Norte de Santander in the improvement of the information security processes and the benefit of the service operations of each entity, so that they are not stopped or compromised due to an information security attack.
This system will keep the information secure and mitigate the risk significantly.

PALABRAS CLAVES	Sistema, Seguridad, Información, Riesgos
PALABRAS CLAVES EN INGLES	System, Security, Information, Risks

CARACTERÍSTICAS

PÁGINAS:176	PLANOS:	ILUSTRACIONES:23	CD-ROM:

Sistema de Gestión del Riesgo de Seguridad Informática para Beneficiar la Operación del Servicio en Empresas Ubicadas en Ocaña Norte de Santander

Diego Armando Cervantes Ramos

Karen Dayana Ortiz Ortiz

Facultad de Ingenierías, Universidad Francisco de Paula Santander Ocaña

Ingeniería de Sistemas

Ing. Luis Fernando Morales Martínez

15 Marzo del 2022

Dedicatoria

La presente tesis está dedicada primeramente a Dios por todas las bendiciones que nos ha dado, ya que gracias a él logramos llegar hasta este momento tan importante de nuestra formación profesional.

A nuestros padres Aida Ramos, Juan Cervantes, Rosabel Ortiz y Luis Ortiz, por ser nuestro apoyo incondicional en todo este proceso, por todos sus sacrificios y esfuerzos, ser el pilar más importante en cada etapa de nuestras vidas, demostrando siempre su cariño y amor.

Gracias a todos.

Agradecimiento

Agradecemos primeramente a Dios, por darnos fuerza y fortaleza para seguir con nuestra formación y dedicación en todo este lindo proceso.

Agradecemos al ingeniero Luis Fernando Morales Martínez, por la confianza que nos brindó y ser nuestro director de tesis, por todo el apoyo y los conocimientos brindados a lo largo de este proceso, la paciencia brindada para que todo saliera delante de la mejor forma.

Agradecemos enormemente a todas las personas que han ayudado y apoyado a lo largo de toda nuestra formación académica en estos años.

Contenido

Pág.

Lista de Tablas

Pág.

Lista de Figuras

Pág.

Lista de Apéndice

Pág.

Capítulo I. Sistema de Gestión del Riesgo de Seguridad Informática para Beneficiar la Operación del Servicio en Empresas Ubicadas en Ocaña Norte de Santander

1.1 Planteamiento del Problema

En el presente, la información es un activo indispensable para los diferentes modelos de negocios, según Chinchilla & Allende (2017) "La información es el activo más importante de toda empresa y que se debe hacer lo necesario para salvaguardarlo" (p. 6); similarmente Meraz (2018) expresa que "actualmente, empresas pequeñas, medianas o grandes, utilizan la tecnología para todo tipo de procesos, así como una gran cantidad de información que requiere resguardo y protección" (p. 295); considerando lo anterior, es de vital importancia que se desarrollen protocolos de protección de datos para que estos no sean obtenidos de forma no autorizada por personas ajenas a la empresa.

En la época actual, hay necesidad de adquirir tecnología avanzada que mitigue los riesgos a los que está sometida la empresa frente a los *hackers*; haciendo un paréntesis sobre la definición de Hacker, autores como Sweigart (2013) quien lo detalla como "un individuo que estudia un sistema informático para comprenderlo tan profundamente, que pueda ser capaz de modificarlo de distintas formas, en su mayoría creativas" (p. 105). Por otra parte, Erickson (2008) señala que el *hacker* resuelve problemas en formas inimaginables comparado con aquellos que se circunscriben en resolverlos pensando en metodologías convencionales.

Por tal razón, personajes como los *hackers* son los causantes de múltiples incidentes negativos dentro de las organizaciones a nivel global, por ejemplo, estos característicos

individuos han realizado ataques a las elecciones presidenciales de 2016 en Estados Unidos, y a los procesos electorales desarrollados en la década del noventa; a su vez, ocurrieron múltiples actos de sabotaje, espionaje y manipulación informativa en internet en varios países (Ospina & Sanabria, 2020).

Otro ejemplo a mencionar, es el sufrido por la "petrolera PEMEX en México", que no solo se trató de un ataque de secuestro de información, sino que, mutó luego a una extorsión de filtrado de información sensible, en caso de no pagarse el rescate (ESET, 2020). Con relación a esto, Ospina & Sanabria (2020) señalan que "en la actualidad, ya no parece necesario lanzar misiles o atacar físicamente una infraestructura (instalaciones, bases militares, estructuras de servicios, etc.), sino que puede generarse daño mediante la divulgación de información y carreras políticas, neutralizar opositores, difundir secretos industriales o militares o sabotear páginas web y sistemas de información, entre otros; gracias a la manipulación, secuestro o destrucción de información personal o institucional" (p. 201); asimismo, este contexto es pertinente a toda organización siendo consciente de que el uso de las tecnologías en sus procesos reduce en gran medida los costos, pero, también, representa riesgos para la seguridad de las mismas (Chinchilla & Allende, 2017)

En lo que a Colombia respecta, el país ha registrado un número alarmante del crecimiento de los ataques informáticos en un 612% (Ceballos, 2020); puesto que, en lo corrido del año 2020 esta tendencia del cibercrimen en gran medida fue propiciada debido a la emergencia provocada por la pandemia del covid-19 ya que muchas empresas implementaron el trabajo remoto o teletrabajo. De acuerdo con esto, la capacidad de adaptación de cada empresa a las circunstancias cambiantes deben contemplar el bloqueo de situaciones que fomenten la vulnerabilidad en provecho de actores maliciosos que comprometan la ciberseguridad (Betancourth, 2020); de

modo que, esta apreciación considerada anteriormente está provocando que muchas personas sean víctimas de ataques de informáticos producto de la falta de sistemas de gestión adecuados para prevenir ataques o en su defecto sean poco eficientes a la hora de prevenirlos. Al respecto, Ospina & Sanabria, 2020 refieren que para el año 2019 los delitos informáticos llegaron a una cifra cercana a 30.410, los cuales fueron denunciados un 54% más que en 2018 distribuyéndose en: *phishing* (42%), suplantación de identidad (28%), envió de malware (14%) y fraudes en medios de pago online (16%) en donde ciudades como Bogotá, Cali, Medellín, Barranquilla fueron el epicentro de las actividades ciber delictivas.

De acuerdo con los datos recopilados en el estudio *Security Report Latinoamérica-ESET* (2020), en Colombia al menos un 58% de las empresas sufrió un incidente de seguridad, lo que ubica al territorio colombiano como el octavo más afectado en Latinoamérica por la actividad maliciosa; además, el 79% de las empresas encuestadas implementan algunos niveles de control básico de seguridad y solo el 71% de las empresas implementan políticas de seguridad.

Por otra parte, Patiño, (2017), expone que, los reportes de ciberataques para Colombia indican que, "más de un tercio de la población registra haber sido víctimas de ciberataques, y 6 de cada 10 personas piensan que los atacantes trabajan dentro de las mismas organizaciones" (p. 37), lo que puede dificultar que se haga un buen manejo para poder mitigar esos ataques. De manera similar, Aristizábal et al. (2018) afirman que "no tener control sobre la información manejada por la organización puede fomentar las acciones de filtrar datos confidenciales acerca de los procesos internos, ocasionando estragos económicos y grandes pérdidas considerables para los involucrados" (p. 13), lo cual está en concordancia con los casos mencionados y sus formas de prevención.

Estas situaciones han sido aprovechadas por los ciberdelincuentes para poder realizar sus acciones; un claro ejemplo ocurrió en Norte de Santander, en la ciudad de Cúcuta en donde dos empresas, una del sector educativo y otras del sector constructor, tuvieron unos ataques muy parecidos; según Caracol Cúcuta (2017)

> "Los casos son relacionados con una variante parecida con lo que está sucediendo a nivel mundial lo que hace este software malicioso o programa mal intencionado es que llega por un correo electrónico, al abrir ese correo que desconocemos su procedencia, automáticamente, se descarga el programa y se contagia el computador y le va a cifrar todos los archivos que contiene el computador pidiendo un rescate a cambio de volverle la clave para poder restablecerle esa información" (p. 59).

No obstante, en el ámbito regional, las actuales empresas en Ocaña que se han enfocado en la zona céntrica no cuentan con una estrategia para hacer frente a los riesgos informáticos de manera que les permita identificar todo tipo de vulnerabilidades que colocan en peligro la seguridad de la información (Claro & Espinel, 2019), esto se debe a que la información es digital y es enviada a través de la red de datos, siendo de suma importancia proteger el sistema que está compuesto por software, hardware, la información que maneja e incluso el mismo operador del sistema.

Con respecto a la ciberseguridad, un reporte de ESET (2018) informó que, "de los ataques informáticos dentro del sector financiero, gobierno o empresas privadas el 60% ocurre a través del *watering hole*, que son esas vulnerabilidades en conexiones con proveedores o intermediarios informáticos" (p. 91). Por lo cual, las tecnologías han tenido un crecimiento muy elevado y por esta razón no es posible tener un sistema completamente seguro mientras se tenga acceso a internet; no obstante, la implementación de los sistemas de gestión del riesgo de

seguridad informática en las empresas a través de herramientas, sistemas y estrategias que permitan un sitio seguro para las operaciones propias de las empresas respaldadas por el acompañamiento conjunto de la Universidad Francisco de Paula Santander Ocaña se plantea el desarrollo de un sistema de gestión del riesgo de seguridad informática que beneficie la operación del servicio en empresas ubicadas en Ocaña Norte de Santander.

1.2 Formulación del Problema

¿Cómo el desarrollo de un sistema de gestión de riesgos de seguridad informática, puede lograr salvaguardar la información relevante para las organizaciones ubicadas en el municipio de Ocaña Norte de Santander?

1.3 Objetivos

1.3.1 Objetivo General

Desarrollar un sistema de gestión del riesgo de seguridad informática que beneficie la operación del servicio en empresas ubicadas en Ocaña Norte de Santander.

1.3.2 Objetivos Específicos

Analizar el contexto de las empresas ubicadas en el municipio de Ocaña Norte de Santander, con el objetivo de conocer los protocolos que gestionan el riesgo de pérdida de información a través de técnicas de recolección de datos.

Caracterizar los estándares, métodos, técnicas y tecnología requeridos para la proposición de los componentes necesarios en un sistema de gestión del riesgo de seguridad informática, a partir de un análisis previo del contexto.

Estructurar los componentes del sistema de gestión del riesgo en seguridad informática considerando las mejores prácticas de gestión de TI, mitigando con ello los incidentes que generan impactos negativos a nivel empresarial.

Aplicar un caso de pruebas en relación al sistema de gestión del riesgo, comprobando con ello su utilidad a través de una simulación de ataques informáticos.

1.4 Justificación

La relevancia de esta investigación radica en que a través de su desarrollo se trata de indagar acerca de la poco gestión desarrollada frente a un tema delicado como es el aseguramiento de la información en el contexto de diversas empresas en un ámbito regional (municipio de Ocaña, Norte de Santander), en donde actualmente los delitos informáticos van en aumento, según Mendoza (2020),el 76.1% esperaba que en el 2020 aumentaran los ciberataques a infraestructuras, y, el 75% esperaban que aumentaran los ataques en busca de dinero o datos; la información hackeada trae consigo consecuencias muy graves como suplantación de identidad, robo en cuentas bancarias y diversa información de suma importancia para la misma. Por lo cual, para las empresas es de gran importancia que toda su información se mantenga segura según la definición que da la ISO 27001/2013,respecto a que, “la información es un activo que, como

otros activos comerciales importantes, tiene valor para la organización y, en consecuencia, necesita ser protegida adecuadamente", debido a esto es necesario que las empresas tomen medidas que les ayude mantener sus datos y la información de los clientes y empleados salvaguardados y protegidos ante cualquier amenaza.

Por su parte, Torres (2016) Menciona "Las amenazas siempre han existido, la diferencia es que ahora, el enemigo es más rápido, más difícil de detectar y mucho más atrevido" (p. 67), es por esto que toda organización debe estar en alerta y saber implementar sistemas de seguridad basados en un análisis de riesgos para evitar o minimizar las consecuencias no deseadas. De modo que, los ataques informáticos se están convirtiendo en una de las mayores amenazas para las empresas siendo esto un problema al que se debe prestar mayor importancia, a lo que se le suma que muchas organizaciones no tienen un plan bien definido para mitigar estos ataques lo que hace vulnerables sus sistemas, cada vez que nuevas tecnologías se implementan para facilitar los procesos, también tiene que crecer la necesidad existente de proteger los datos en Colombia (Peñuela, 2018). Con relación a esto, gran parte de los ataques informáticos que se producen en las empresas se basan en que hay poca información, o que la educación que reciben los usuarios referentes a tema es nula, lo cual agrava más la situación de las empresas en tema de seguridad y protección de sus datos. Respecto a esto, Aristizábal et al. (2018) "Cuando no se tiene un control sobre la información manejada por la organización, se pueden filtrar datos confidenciales acerca de los procesos internos, lo que puede ocasionar estragos económicos y pérdidas de gran consideración para todas las personas involucradas".

De manera que, la gestión de sistemas para la detección de incidentes de ciberataques es de suma importancia en la organización porque mitiga los ciberataques, ayudando a las empresas a anticiparse ante los ataques de los cibercriminales, ya que, esta modalidad está en aumento,

siendo vital contar con sistemas de gestión de riesgo de seguridad informática al interior de las empresas, lo que a su vez, ayuda a mantener la información segura representado múltiples beneficios a lo que Caro (2011) describe que

> "La ciberseguridad es el conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciber entorno" (pp. 54-55).

Por lo cual, seguir estos lineamientos brindará la oportunidad que más empresas estén mejor preparadas ante cualquier ataque informático que se les pueda presentar; no obstante, un adecuado proceso de gestión de riesgo es fundamental para mantener dentro de la organización la seguridad de todos sus activos, esto se convierte en uno de los pilares importantes (Guachi, 2012); puesto que, el alcance de las acciones para la protección de la información y todos los activos informáticos tiene sus bases en la construcción de herramientas de gestión de seguridad. Por consiguiente, la presente investigación se justifica en virtud del desarrollo de un sistema de gestión del riesgo de seguridad informática que, beneficie la operación del servicio en empresas ubicadas en Ocaña Norte de Santander, mediante el análisis del contexto de las empresas locales; así como de la caracterización de los estándares, métodos, técnicas y tecnología requeridos para la proposición de los componentes necesarios en un sistema de gestión del riesgo de seguridad informática que conlleven a la estructuración de los componentes del sistema de gestión del riesgo en seguridad informática.

1.5 Delimitaciones

1.5.1 Geográfica

El proyecto se desarrollará considerando el contexto de empresas ubicadas en el municipio de Ocaña Norte de Santander.

1.5.2 Temporal

El tiempo estimado para el desarrollo de la presente investigación será de 6 meses a partir de la aprobación de la propuesta de Trabajo de Grado.

1.5.3 Conceptual

Seguridad informática, ciberataques, Hacker, sistema de información, sistema de gestión, activo, incidentes, cibercrimen, phishing, mitigar, salvaguardar, gestión de riesgo, virus informático, vulnerabilidad.

1.5.4 Operativa

Para el desarrollo del proyecto, es necesario el suministro de información por parte de las empresas participantes en Ocaña-Norte de Santander, así como la disposición y actitud positiva por parte de las mismas para poder llevar a cabo distintas pruebas con respecto a los hitos del proyecto.

Capítulo II. Marco Referencial

2.1 Marco Histórico

2.1.1 Antecedentes a Nivel Internacional

Entre los estudios ejecutados por los autores en el ámbito internacional se destaca la investigación realizada por Pardo (2015) en su tesis de grado, en la Universidad Nacional de Loja en Loja-Ecuador titulada "Modelo de Gestión de Seguridad de la Información para la Universidad Nacional de Loja basado en la norma ISO/IEC 27001",el cual se basó en la adopción de los requerimientos de dicha norma para las actividades y funciones realizadas en la unidad, estableciendo fases de desarrollo a través del análisis de la situación actual de la UTI en cuanto a seguridad de la información; la valoración de los activos de información (bajo las dimensiones de confidencialidad, disponibilidad e integridad); la determinación de amenazas y vulnerabilidades asociadas a los activos de información; y el análisis de riesgos encontrados para los activos de información y determinación de los mecanismos de control necesarios para la mitigación de dichos riesgos. Por su parte, los objetivos de Control y Controles de Seguridad de la Información ISO/IEC 27001:2005 que contiene 133 mecanismos de control, distribuidos en 11 secciones permitieron esquematizar la propuesta de un Manual de Políticas de Seguridad de la Información, destinado a la mitigación de riesgos informáticos y creación de cultura de seguridad de la información a nivel institucional, todo ello gestionado por la Unidad de Telecomunicaciones e Información de la institución.

De modo que, lo anteriormente expuesto hace parte de los aportes que contribuyen a la realización de la presente investigación, puesto que los objetivos se relacionan con la pretensión del anterior trabajo citado el cual se refiere a las fases de implementación para gestionar la ciberseguridad, lo cual está en concordancia con lo que se pretende desarrollar.

Por otra parte, un importante informe presentado por Guamán (2014) como tesis de Maestría, de la Escuela Politécnica Nacional, en Quito-Ecuador titulado "Diseño de un Sistema de Gestión de Seguridad de la Información para Instituciones Militares" incorpora estándares internacionales en la investigación los cuales están ajustados al campo militar, así como a las nuevas tecnologías de la información y comunicación. El objetivo principal del proyecto se basó en diseñar un sistema de gestión de seguridad de la información para Instituciones Militares que incorpore estándares internacionales ajustados al campo militar y nuevas tecnologías de la información y las comunicaciones con el fin de contribuir a la modernización de las Instituciones Militares. Para acercarse a esto, la metodología del proyecto se sustentó en 3 fases, las cuales fueron: el estudio diagnóstico, la factibilidad y por último el diseño de un Sistema de gestión de Seguridad de la Información para Instituciones Militares, guiándose por la Norma ISO 27001:2005. Los resultados mostraron que, para dar soporte a la gestión de seguridad de la información en función de los requisitos de las Instituciones Militares, se requiere realizar un manual de política de seguridad de la información en representación del nivel político o estratégico de dichas instituciones a partir de la Dirección de Tecnologías de la información y Comunicaciones. Asimismo, los resultados mostraron una alta tendencia a que casi siempre la Dirección de Tecnologías de la Información y Comunicaciones llevan las políticas de seguridad de información de la empresa. Se concluyó que las actividades para la factibilidad operativa,

técnica y económica para el establecimiento del diseño de un Sistema de Gestión de Seguridad de la Información para Instituciones Militares puede acarrear beneficios para los usuarios dado por el levantamiento de la información por observación directa a partir de las cláusulas, objetivos de control basados en los requerimientos de la institución.

De modo que, el anterior proyecto aporta bases que enriquecen el conocimiento de las pautas para acercase a la implementación significativa de los sistemas de seguridad informáticos aplicados a empresas de índole pública, pudiendo ser extrapolada a otros dominios; lo cual es importante para el desarrollo de la presente investigación.

Seguidamente, el proyecto realizado por Bermúdez & Bailón (2015) como tesis de pregrado, en la Universidad Politécnica Salesiana, Sede Guayaquil-Ecuador titulado "Análisis en Seguridad informática y Seguridad de la información Basado en la Norma ISO/IEC 27001-Sistemas de Gestión de Seguridad de la información Dirigido a una Empresa de Servicio financieros", tuvo por objetivo analizar los procesos críticos de Credigestión respecto a las gestiones de seguridad adecuadas para garantizar la confidencialidad, integridad y disponibilidad de la información, mediante la formulación recomendaciones de seguridad y controles basados en la Norma ISO/IEC 27001. De tal forma que para conocer las vulnerabilidades a las que está expuesta la información por la falta de aplicación de controles de seguridad, este trabajo tuvo una metodología de análisis dirigida a una empresa financiera mediante el estudio de seguridad en los procesos críticos de cuatro fases a través de reuniones, revisión de documentación, consultas, observación, encuestas y ejecución de entrevistas con directivos que poseen un amplio conocimiento del negocio, de modo que se logró identificar los riesgos actuales a los que se exponen los datos tanto físicos, lógicos y sistemas de procesamiento de información. A su vez, la

ejecución del análisis de riesgos da a conocer el nivel de impacto que tendría la ocurrencia de las amenazas identificadas en cada activo de la información que pueden afectar datos relevantes utilizados o resultantes de la ejecución de las actividades propias del negocio.

Los resultados mostraron que, para minimizar los riesgos existentes en las empresas, es necesario implementar controles de seguridad, lo cual ayuda a fortalecer tres aspectos importantes dados por la confidencialidad, integridad y disponibilidad del compromiso y trabajo en equipo que debe tener la empresa. Se concluyó que los activos de información de las áreas críticas y las circunstancias actuales de la empresa con respecto a la seguridad de la información puede reflejar potenciales repertorios de riesgo ya que estos exponen la información ante tobos, alteraciones, y daños causando un impacto negativo en las actividades del negocio.

De acuerdo con esto, el anterior trabajo resalta la importancia de la ciberseguridad para la gestión al interior de las empresas constituyéndose esto como un eje de fortaleza para las operaciones de la misma. Adicionalmente, este trabajo aporta a los conocimientos acerca de la gestión de la ciberseguridad al interior de la estructura empresarial, siendo esto fundamental para enriquecer el marco referencial, y de antecedentes de la investigación en curso como un punto de referencia para el logro del objetivo principal.

Asimismo, Toapanta et al. (2020) en el artículo titulado “Un enfoque de modelo de seguridad para mitigar el riesgo de Ciberataques a instituciones públicas en Ecuador”, publicado en 4th International Conference on Information System and Data Mining, ICISDM-2020, en Hilo-Estados Unidos, se planteó como objetivo proponer un prototipo de un modelo de seguridad para mitigar los riesgos de ciberataques a instituciones públicas para definir la estructura organizativa y la seguridad para definir la estructura organizativa y sus niveles para adoptar

protocolos de seguridad. De modo que, la metodología implementada en la investigación consistió en el método deductivo para verificar las tendencias actuales de los modelos de seguridad y proteger la información disponible sobre la entidad ministerial.

Los resultados mostraron que, el prototipo propuesto estableció un modelo de seguridad para mitigar los riesgos de ataques cibernéticos, de manera que, fue posible plantear una estructura definida por capas que se pueden implementar estratégicamente en aseguramiento de cada una de estas capas sean efectivas; asimismo, en caso de que una amenaza logre sobrepasar el filtro de seguridad de una de estas capas, la siguiente capa tendrá diferentes sistemas de protección, por lo cual, cada nivel logra anteponerse y mitigar el riesgo, evitando que el ataque pase a un siguiente escenario.

Por consiguiente, se concluyó que es necesario que una estrategia de seguridad diseñada contenga datos a través de una ruta correcta, confiable y de alta disponibilidad para ofrecer un mayor nivel de fiabilidad. Debido a que, el contenido de este plan fue presentado y puesto a disposición de todos los miembros del público institución, especialmente aquellos que participan activamente en la seguridad procedimientos de información.

Con respecto a los hallazgos anteriores, la principal contribución de este trabajo se basó en demostrar la confiabilidad de la implementación y aplicación de los filtros de seguridad a través de distintos niveles para salvaguardar los datos, así como la información de las empresas. De este modo, este aporte está en concordancia con los objetivos de la presente investigación, siendo esto un aspecto relevante para el desarrollo de la misma.

2.1.2 Antecedentes a Nivel Nacional

En el ámbito nacional se resalta monografía de investigación realizada por Remolina, (2019) como trabajo de grado en la Universidad Cooperativa de Colombia, en Bogotá D.C., titulada "Diseño de un Modelo de Seguridad Informática a una Empresa en su Sistema de Monitoreo del Área de Tecnología" cuyo objetivo fue implementar un modelo de seguridad informática en un sistema de monitoreo del área de Tecnología de una empresa, para lo cual se realizó una propuesta de seguridad informática con el fin de establecer medidas para la protección de la información en una empresa respecto al área de Tecnología.

La metodología de desarrollo del proyecto se asentó en el análisis de activos informáticos y la seguridad de los mismos a través del análisis de riesgos, en donde se identificaron los activos y el valor de los mismos, así como la identificación de amenazas, la evaluación de impacto y la clasificación de riesgos que pudiesen causar dichas amenazas. A su vez, se realizó el tratamiento de los riesgos, en donde se identificaron los controles de seguridad existentes en la empresa tomando como referencia la norma ISO/IEC 27001:2013, ya que es objetivo primordial de la compañía certificarse en esta norma, se identificó la situación actual y las brechas de seguridad.

Los resultados del proceso de investigación arrojaron los datos necesarios para dar paso al diseño de la política de seguridad y establecer el modelo de implementación remitido al comité de seguridad de la empresa para su respectiva revisión y aprobación. Igualmente, esto dio paso a la realización del diseño de conexión entre redes, internas y externas, de la compañía. Finalmente, se realizó la implementación de una herramienta de seguridad aplicando las medidas de seguridad correspondientes. Se concluyó que, el compendio de los valores de los activos no fue precisos, pero esto permitió completar el análisis y extraer los resultados evidenciando los riesgos de seguridad que potencialmente afectan el desempeño del área. Adicionalmente, el

análisis de riesgos dio paso a contemplar el estado actual de la empresa en el ámbito de la seguridad conforme al área de tecnología.

El anterior trabajo da cuenta de la importancia de implementar los planes y políticas de seguridad en las estructuras internas de las empresas tendiendo en consideración que el monitoreo y el control de la seguridad evidencia que es posible reducir la vulnerabilidad de los sistemas informáticos; lo cual esta relacionad con el objetivo que persigue la presente investigación siendo también un referente que aporta conocimientos acerca de los aspectos descritos en temas de ciberseguridad y mitigación de riesgos en sistemas informáticos.

Con relación a las contribuciones en el ámbito nacional referentes al eje central de esta investigación, Nieves (2017) realizo un proyecto de grado de especialización en la Institución Universitaria Politécnico Grancolombiano, en Valledupar-Colombia titulado "Diseño de un sistema de gestión de la seguridad de la información (SGSI) basado en la norma ISO/IEC 27001:2013" el cual tuvo como objetivo el diseño de un sistema de gestión de seguridad de la información (SGSI) basados en la norma ISO/IEC 27001:2013, para lo cual se evaluaron tres pilares importantes dados por la integridad, la confiabilidad y la disponibilidad de los activos de información a las oficinas de ingreso de Centros de Educación y Tecnología del Cesar, a través de tres fases: "Planeación, activos de información, y, capacitación y sensibilización".

La metodología consistió en un estudio mixto (cualitativo y cuantitativo) de tipo tomando como referencia la línea de investigación de la ISO/IEC 27001:2013 cuyos datos e información fueron tomados mediante el cuestionario, la entrevista y la observación como instrumentos de recolección de datos. Los resultados apuntaron a que la identificación de los activos de

información es utilizada para el desarrollo de las actividades de cada área de la entidad, siendo útiles como insumos para el proceso de valoración de riesgos, determinado que cada uno de los activos brinda información cuya valoración fue distinta, puesto que cada uno cumple una función diferente en la generación, almacenaje o procesamiento de la información. Se concluyó que, la seguridad de los sistemas informáticos atañe a una responsabilidad de todos los miembros que conforman una entidad, la cual debe estar guiada por manuales y procedimientos de buen uso de los activos de información; además, el diseño de un Sistema de Gestión de Seguridad de la Información (SGSI), posibilita la identificación de las amenazas y vulnerabilidades de los activos de información que, posteriormente permite hacer la planeación de la disminución de los riesgos para los activos de información.

Este proyecto tuvo como principal contribución la demostración de que los planes de gestión de seguridad informática para la mitigación de los riesgos potencializan el uso de los activos informáticos de las entidades de manera confiable, siendo esto un aspecto que guarda nexos con el objetivo de la presente investigación contribuyendo al despliegue y desarrollo practico, teórico y metodológico de la misma.

Similarmente, Pinzón (2014) presenta un artículo de especialización realizado en la Universidad Piloto de Colombia titulado "Gestión de riesgo en Seguridad informática" con el fin de brindar orientación a las empresas y en especial al área de TI, para gestionar el riesgo de seguridad informática. En atención a esto, los resultados mostraron que, la gestión de riesgo en el campo informático busca sensibilizar a todas las empresas y, en especial a las colombianas, en el tema de la seguridad y la administración del riesgo está relacionada con el manejo de datos, activos e información, puesto que esta se realiza teniendo en cuenta una fase de análisis, con la

que se busca conocer: los activos, el sistema y los datos; encontrando sus vulnerabilidades y amenazas, teniendo como objetivo principal la determinación del riesgo.

Tras la obtención, se realiza la clasificación, se toma cada uno de los riesgos encontrados y se implementan controles, con el fin de obtener un riesgo aceptable, motivo por el cual se analizar y evaluar el funcionamiento, así medir la efectividad en el proceso de reducción de riesgo. Se concluyó que, es importante tener en cuenta las políticas de seguridad, normatividad del país y reglas institucionales en todas las implementaciones con el fin de apoyar la misión del negocio.

De tal suerte que, el anterior artículo aporta una clasificación de los riesgos informáticos a los que puede estar expuesto una compañía, ofreciendo una visión de la efectividad de las acciones de control para la mitigación de los riesgos, lo cual se relaciona con lo planteado en esta investigación en la consecución de los objetivos propuestos.

En este sentido, el proyecto realizado por Fonseca (2019) como tesis de maestría en la Universidad EAN, en Bogotá D.C., Colombia, titulado “Modelo de un Sistema de Gestión de Seguridad de la Información en la Organización Geo consult CS” presenta como objetivo diseñar un modelo de un sistema de gestión de la seguridad de la información, que aplique a todos los procesos y áreas de la organización Geo consult CS, alineado con la norma NTC2 -ISO3 -IEC4 27001:2013, el cual permita conocer su estado actual con respecto a la seguridad de la información, y de una manera sistemática y eficaz implementar los controles procedimientos y políticas necesarias para preservar la integridad, confidencialidad e integridad de los activos de la información. Dicho modelo se aplica a una organización llamada Geo consult CS, quien presta servicios de gestión y administración de información técnica en el sector de hidrocarburos.

El modelo presentado es totalmente ajustable a una nueva actualización de la norma ISO27001 y es compatible con estándares como COBIT e ITIL. Por tanto, le permite responder de una manera eficaz a los cambios tecnológicos y a las nuevas amenazas que se puedan generar. Adicionalmente, dados todos los elementos que lo componen puede ser la base para establecer un gobierno de tecnologías de la información en cualquier organización.

Además, el modelo de un Sistema de Gestión de Seguridad de la Información es un elemento clave dentro del plan estratégico de cualquier organización, especialmente en las empresas del sector petrolero, financiero y de tecnologías de la información. Debido a que más allá, de cumplir requisitos contractuales y proteger sus activos, le permite obtener un valor diferenciador dentro de la operación de sus servicios, incrementa la percepción positiva de la imagen de la empresa, mejora los procesos y disminuye costos.

De modo que, lo anteriormente expuesto hace parte de los referentes nacionales que apoyan la ejecución de la presente investigación tendiendo eje central los sistemas de riesgo informáticos cuya principal contribución reside en demostrar las estrategias subyacentes a los modelos de Sistema de Gestión de Seguridad, siendo esto relevante para el desarrollo de la presente investigación.

2.1.3 Antecedentes a Nivel Regional

En cuanto a las investigaciones, estudios y trabajos académicos que contribuyen a conformar los antecedentes en el ámbito regional, se desataca el trabajo desarrollado por Martínez et al. (2021) para el Instituto Departamental de Salud y la Gobernación de Norte de Santander, en Cúcuta, titulado “Sistema de Gestión de Seguridad Informática y Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información”; cuyo principal objetivo

fue determinar los lineamientos que permitan garantizar que la plataforma tecnológica de la IDS (recursos de software, recursos de hardware y sistemas de información) se usen únicamente para los propósitos para los que fueron creados y dentro del marco previsto, cumpliendo las normas y políticas de seguridad de la información. De modo que la metodología implementada consistió en cuatro pilares para el análisis de riesgos basados en los activos de información; las amenazas; los controles y la estimación de los riesgos, los cuales conformaron los componentes de estudio.

Los resultados de la evaluación mostraron que los valores en los que fueron basados los supuestos para el Instituto Departamental de Salud de Norte de Santander no se reflejan en costos, aunque si representa un gasto a la Entidad, así como una pérdida de credibilidad ante la población departamental, y principalmente ante los entes de Control del departamento y del ámbito nacional. Se concluyó que, las estrategias de seguridad de las políticas demuestran la relevancia que ostenta la organización ante el hecho de proteger uno de los activos más significativos e indispensables para el desarrollo de sus actividades y la consecución de las metas, el cual se basa en los recursos de la información.

De manera que, el anterior trabajo contribuye a la construcción de un marco que resalta la importancia del uso de políticas y estrategias para la gestión de la seguridad en un ámbito regional que puede ser abstraído a otros dominios, siendo esto importante para la investigación en curso debido a los nexos que presenta con el desarrollo de la misma.

De modo similar, Arévalo et al., (2015) en un artículo de investigación titulado "Implantación de un sistema de gestión de seguridad de información bajo la ISO 27001: Análisis del riesgo de la información", y publicado en la revista Tecnura, examina la estructura de la actividad empresarial del municipio de Ocaña-Norte de Santander con la finalidad de ampliar la

información para comprender las principales variables de la actividad productiva del municipio, su vocación empresarial, desarrollo tecnológico y estructura del tejido productivo. Tal acercamiento contempló la realización de una investigación descriptiva consistente en identificar la actividad económica, en sus diversas manifestaciones, y, promover la ejecución de prácticas administrativas acordes con referentes nacionales e internacionales. Los resultados permitieron establecer las debilidades empresariales, incluyendo las de la información, que una vez identificadas sirven para diseñar espacios de formación, adquisición de habilidades y prácticas gerenciales en los empresarios acordes con los retos de la competitividad y permanencia en el mercado. Como conclusión se afirmó que la recopilación de la información referente al componente tecnológico de las empresas del tejido productivo del municipio ha sido útil para la protección del activo más importante de las mismas: la información. De modo que para estas empresas se ha propuesto la aplicación de herramientas para el análisis de sistemas de información usando la norma ISO 27001:2005, mediante el uso de tecnologías de información más apropiadas para las organizaciones del estudio.

El trabajo y los hallazgos que se presentan consignados en este artículo contribuyen a fortalecer los aspectos operativos de la seguridad en las empresas regionales ya que esto puede tomarse como un acercamiento al entendimiento, y aplicación de las medidas de protección de la información considerando esto como parte de los activos de la empresa, de manera que, la relevancia del aporte enriquece el desarrollo de la presente investigación configurando una relación entre los hallazgos disponibles y los alcances que se plantea esta investigación en el ámbito de los sistemas de gestión del riesgo de la seguridad informática.

2.2 Marco Contextual

Ocaña es un municipio colombiano ubicado en la zona noroccidental del departamento de Norte de Santander, cuya economía se encuentra fuertemente está marcada por las actividades comerciales de la frontera colombo-venezolana; de modo que, las políticas y los criterios económicos de esta zona se muestran como una convergencia de las dinámicas de ambos países (Cámara de Comercio de Ocaña, 2017).En este sentido, Ocaña basa economía, principalmente, en el sector primario determinado por las actividades de la agricultura, y la ganadería; y actividades del sector secundario como la minería con explotación de plata, cobre, hierro; asimismo, el sector el comercio terciario, está dado en este municipio a partir de la pequeña industria, y el turismo (Sánchez & Chinchilla, 2020).

Sin embargo, el municipio se caracteriza por presentar una amplia utilización de los recursos que constituyen pequeñas áreas de cultivos permanentes de café, frutales y pastos, y semipermanentes de caña, piña, plátano y yuca; así como la explotación ganadera de tipo extensivo no tecnificada, actividades de avicultura, y piscicultura (Vergel, 2019).

El sector empresarial en el municipio de Ocaña, se ha posicionado como una de las zonas económicas más importantes del Departamento de Norte de Santander, por su economía basada en la gastronomía, la agricultura y el turismo; no obstante, el objeto de estudio de esta investigación se centra en las empresas Ocañeras dedicadas a los procesos de comercialización regional, siendo esto fundamental para las dinámicas de comercialización municipal e intermunicipal que regulan la economía en un contexto regional (Cámara de Comercio de Ocaña, 2017).

2.3Marco Conceptual

Ciberataques: El término se refiere a la utilización de las brechas de seguridad con las que cuentan las tecnologías de la información para replicarse, borrarse o modificarse en provecho de las vulnerabilidades que presentan la mayor parte de las estructuras cibernéticas (Izaguirre& León, 2018).

Cibercrimen: Puede ser considerado como una subcategoría de los delitos informáticos alusivo a los delitos y crímenes organizados y realizados a través del Internet y redes de computadores como medios para dirigir las operaciones, entre estos se desataca el ciberacoso, el fraude mediante criptografía, la extorsión, entre otros (Vereau, 2021).

Gestión de riesgo: Se refiere al manejo y adecuada administración de la confidencialidad, disponibilidad, e integridad de la información con el objetivo de destinar su uso para el cual fue diseñado, además de anticiparse a los peligros mediante la planeación y el estudio de la probabilidad de que ocurran incidentes a través de un plan para frenarlos, y mitigar sus efectos ante una inminente perdida de información (Bailón-Lourido, 2019).

Hacker: Se constituye como una persona o individuo que es capaz de explorar detalladamente los sistemas programables en búsqueda de expandir sus posibilidades tomando información de manera arbitraria pudiendo modificarla, o usarla para su conveniencia en violación de la privacidad, de modo que, contrario a los demás usuarios, un hacker suele sabotear

los recursos informáticos siendo esto, casi siempre, considerado como ciberdelincuencia (Sánchez, 2019).

Incidentes de seguridad de la información: La seguridad de la información contempla eventos cuya probabilidad de comprometer las operaciones de la entidad y amenazar la seguridad de la información son considerados como incidentes de seguridad que con respecto a la información incluyen los accesos no autorizados, la arbitraria modificación de recursos informáticos, el uso inapropiado de los recursos, entre otros (Ayala & López, 2019).

Operación del Servicio: De acuerdo con Puello (2012) "La operación del servicio es más que solo la ejecución repetitiva de un conjunto estándar de procedimientos o actividades. Todas las funciones, procesos, y actividades son diseñados para poder entregar un nivel de servicio establecido, pero deben ser entregados en un ambiente cambiante, lo que genera entonces un conflicto entre el mantener un estado quo y el adaptarse a los cambios en el negocio y los ambientes tecnológicos" (p. 9).

Phishing: Es una modalidad de la ciberdelincuencia basada en el fraude y la manipulación para conseguir información confidencial haciendo uso del envío de correos electrónicos a determinadas empresas o personas naturales, cuyo dominio puede parecer autentico para intentar conseguir datos, lo cual es una estafa o fraude ejecutado a través de internet logrando su cometido al emplear la manipulación social (Giraldo & Pacheco, 2018).

Seguridad informática: Se refiere a las acciones y decisiones que conllevan a frenar la ejecución de operaciones no facultadas sobre un sistema informático o sobre una red informática, haciendo que los efectos dañinos de los ataques puedan ser mitigados en favor de minimizar y mitigarlos daños sobre la información, haciendo que se proteja la confidencialidad, autenticidad o integridad de dicha información al impedir la disminución del rendimiento de los equipos a través del bloqueo del acceso de usuarios no autorizados al sistema (Pangalima, 2018).

Sistema de información: Pueden ser considerados como un conjunto de procedimientos interrelacionados que forman una unidad para el almacenamiento, procesamiento y distribución de la información como datos manipulados útiles para la toma de decisiones y para ejercer el control en una organización o empresa, que incluye a personas, artefactos y métodos organizados con las instalaciones, el personal y todos los componentes necesarios para el tratamiento, transmisión, visualización, diseminación y organización de la información (Fernández-Alarcón, 2021).

Sistema de gestión: Es una herramienta que le permite a las organizaciones obtener un mejor desempeño de manera organizada para controlar, planear y automatizar las tareas y actividades operativas y administrativas de las empresas; asimismo, el sistema de gestión consiste en una herramienta para examinar las utilidades y los riesgos para conseguir favorabilidades en cuanto al desempeño de la organización (Pineda & Burbano, 2019).

Virus informático: Se refiere a un tipo de malware o elemento perjudicial configurado por piratas informáticos, de modo que, la principal función de un virus informático es modificar

y poner en riesgo a la información sin previa aprobación por el usuario, debido a que su propagación es rápida y se hace usando los softwares con los que cuente el medio tecnológico, ya sea un computador, un celular o cualquier dispositivo relacionado, pudiendo alterar el funcionamiento del equipo con la consecuente pérdida de información (Cuellar, 2020).

Vulnerabilidad: Según Quiroz & Macías (2017) la Vulnerabilidad es "una característica o circunstancia de debilidad de un recurso informático la cual es susceptible de ser explotada por una amenaza" (p. 680).

2.4 Marco Teórico

2.4.1 Seguridad informática

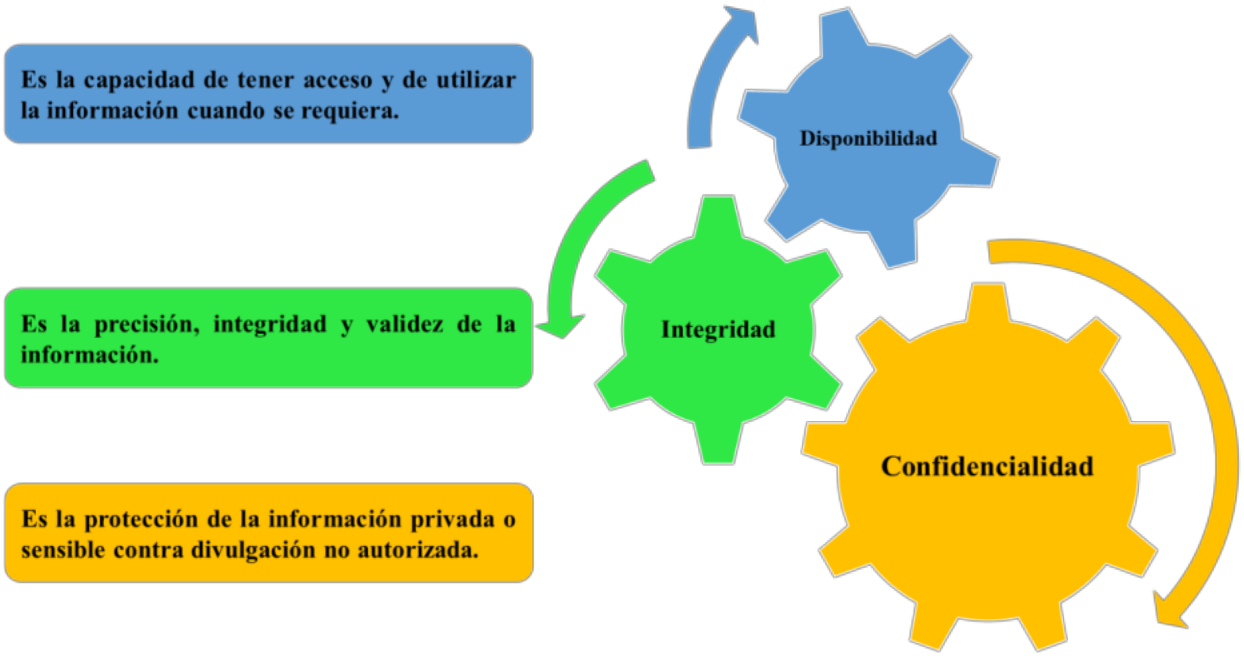
En la actualidad, el internet se proyecta en un creciente amento en cuanto a su uso, puesto que, grandes empresas y compañías les dan el acceso a sus socios o proveedores para que puedan ingresar a sus sistemas de información (Morales et al., 2020). Debido a lo anterior, es importante saber qué recursos de dicha empresa tienen la necesidad de ser protegidos y así tener mayor control de acceso a los sistemas de la empresa y a los llamados derechos de los usuarios del sistema de información.

La seguridad informática previene y detecta todo aquel uso inapropiado que personas sin autorización le dan a un sistema informático, puesto que, este proceso debe estar rigurosamente activo en cada empresa, protegiendo cada uno de los sistemas a los cuales intrusos inescrupulosos con intenciones maliciosas o intenciones de obtener ganancia le generan a la empresa riesgos muy elevados (Díaz, 2018). De acuerdo con Desarrollo y Gestión de Seguridad

de Redes (2022), los riesgos, en términos de seguridad, se caracterizan por lo general mediante la siguiente ecuación:

Riesgo = (amenaza * vulnerabilidad) / contramedida)

Figura 1 Principios Básicos de la Seguridad de la Información.
Principios Básicos de la Seguridad de la Información.



Fuente: EAN página institución educativa.

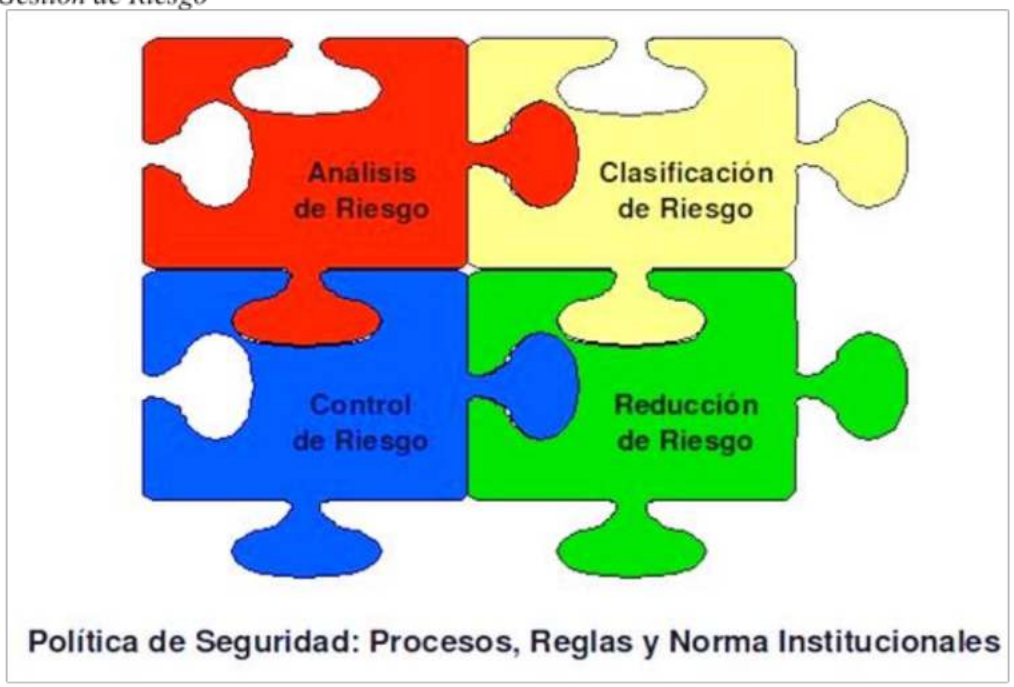
2.4.2 Principios de la Seguridad de la Información

La seguridad de la información, de acuerdo a Mayanquer, (2020), es vista como "una manera de garantizar la protección de los activos de información ante una variedad de amenazas que pueden comprometer la continuidad del negocio" (p. 53), cuyo objetivo de tales principios se basan en minimizar el riesgo y maximizar el retorno de inversiones y oportunidades para una empresa.

2.4.3 Gestión de Riesgo en la Seguridad Informática

Por su parte, los métodos, herramientas, y requerimientos útiles para determinar, analizar, valorar y clasificar el riesgo, hacen parte de las acciones para la gestión del riesgo que, tras la planificación y el cálculo de probabilidades de ocurrencia de evento desfavorables busca implementar mecanismos que permitan controlar los peligros y riesgos inminentes.

Figura 2 Fases de Gestión de Riesgo
Fases de Gestión de Riesgo



Fuente: //protejete.wordpress.com/gdr_principal/gestion_riesgo_si/ [Consultado el 13 de enero de 2022]

Asimismo, la gestión de riesgos en el ámbito de la seguridad informática tiende a resguardar la integridad, confiabilidad y accesibilidad a los datos, propios para el funcionamiento de una organización, empresa o entidad cuyos activos intangibles conforman el escenario para el desempeño de las tareas esenciales.

Dentro de las funciones del adecuado diseño e implementación de acciones para ejecutar los sistemas de gestión del riesgo de seguridad informática se destaca la importancia de diseñar barreras de seguridad destinadas a la solución rápida y oportuna de los inconvenientes que la plataforma de una determinada empresa presente. Además, se requiere considera la necesidad de establecer pruebas de seguridad como mecanismo de prevención cuya realización obedezca a una periodicidad establecida por el personal de trabajo de seguridad informática de la empresa.

En este sentido, la gestión de los incidentes ayuda a gestionar los riesgos identificados haciendo uso de los datos y la información asociada para generar una respuesta que evite problemas futuros, lo cual puede estar complementado con la detección de las vulnerabilidades del sistema de las empresas. No obstante, Miranda et al., (2016), dan a conocer en forma general, la gestión del riesgo en la seguridad informática mediante cuatro fases:

Análisis del riesgo: Esta fase determina cuales son los componentes que un sistema requiere para su protección de acuerdo con sus vulnerabilidades, es decir, aquellos factores que lo debilitan o lo hacen susceptible de ser atacado; y las amenazas que lo ponen en peligro, con la finalidad de que el resultado de tal análisis revele su grado de riesgo.

Clasificación del riesgo: Establece si los riesgos encontrados y los riesgos restantes son aceptables, de manera que, el riesgo como variable puede adoptar distintos grados siendo su clasificación la que indique si es factible o no hacer frete a las amenazas o los ataques de acuerdo con las soluciones diagnosticadas.

Reducción del riesgo: Es la resultante de implementar medidas de seguridad informática a través del análisis y posterior clasificación, de modo que, las acciones involucradas en esta fase implican la instrucción o educación de los usuarios acerca de prevenir y boquear los peligros que atañen a los datos y la información de la empresa.

Control del riesgo: Esta fase analiza el funcionamiento, la efectividad y el cumplimiento de las medidas, para determinar y ajustar las medidas deficientes y sanciona el incumplimiento. Adicionalmente, la finalidad de controlar los riesgos informáticos consiste en medir la efectividad de las medidas implementadas para la reducción y la prevención de los ataques, peligros y demás riesgos para poder concertar las faltas de la seguridad informática de la empresa.

De modo que, todo el proceso de la gestión de riesgo en la seguridad informática está basado en las llamadas políticas de seguridad, normas y reglas institucionales, que forman el marco operativo del proceso, con el propósito de potenciar las capacidades institucionales para reducir la vulnerabilidad y limitar las amenazas, lo cual, conlleva a la reducción el riesgo. Asimismo, dicha gestión puede orientar el funcionamiento organizativo y operacional para garantizar el comportamiento homogéneo y la corrección de conductas o prácticas que hacen que la información y los activos intangibles de la empresa sean susceptibles.

A partir de estas teorías se ha fundamentado la creación de un sistema de gestión del riesgo de seguridad informática para beneficiar la operación del servicio en empresas ubicadas en Ocaña norte de Santander, por lo cual se complementa con lo consignado a continuación:

Teoría de Código: Los inicios de la teoría moderna de la comunicación, incluye la teoría de códigos, la cual se sitúa al final de los años veinte con los trabajos de *Ralph Hartley* (Maldonado, 2019). Asimismo, en 1941, Claude E. Shannon, considerado el padre de la teoría de la información, comienza sus investigaciones en temas de comunicación, sus resultados se publicaron en el trabajo *"A Mathematical Theory of Communication"* (1948), que es la base de la moderna teoría matemática de la comunicación. Hacia 1950, los trabajos de Richard Hamming y Marcel Golay dieron un mayor impulso a la teoría de códigos (Maldonado, 2020). En ellos se construyen, de forma económica y elegante, códigos capaces de corregir un número especificado de errores producidos durante la transmisión.

En determinados casos, sus métodos son óptimos, en el sentido de que, para transmitir un determinado número de símbolos con una capacidad de corrección marcada, el número de símbolos añadidos es mínimo (Veglia, 2018). Una comunicación de datos consiste en la transmisión de una secuencia de caracteres de algún alfabeto finito A (normalmente A = {0, 1}) desde una localización física (fuente) a otra (receptor) a través de un canal de comunicación. En la mayoría de los casos, imperfecciones del canal, denominadas ruido, provocan que algunos caracteres transmitidos sean incorrectamente recibidos por el receptor (Cajusol & Céspedes, 2019). Por ello se introducen, de modo sistemático, redundancias en la información, las cuales permiten detectar, e incluso corregir, los errores cuando el mensaje recibido es descodificado (Rubiano et al., 2020).

Apropiación de métodos Criptográficos: Se puede decir que la criptografía se originó con la misma escritura y es tan antigua como ella, pero con los desarrollos tecnológicos de las últimas décadas, el crecimiento exponencial de los datas y la velocidad de procesamiento en las maquinas, la información se ha hecho vulnerable y puede ser manipulada por sectores

organizados que invierten todo su tiempo y esfuerzo en desarrollar herramientas sofisticadas para apropiarse de sistemas clasificados, riesgo demasiado grande, pues la información es el activo más importante en la sociedad moderna, tener el control de la información implica directamente tomar buenas decisiones y resolver problemas que pueden alterar el curso de la historia, con esta se crean estrategias que soportan los gobiernos, la economía y general cualquier acción cotidiana que asegure la existencia humana, es decir, que garantizar la seguridad de la información es fundamental para preservar y expandir las especies en este universo (Urrego, 2019).

En este sentido, la criptografía se ha convertido en el pilar de la seguridad de la información durante toda la historia, en la modernidad esta se ha encargado de la transmisión y almacenamiento de datos de tal manera que no puedan ser comprendidos ni modificados por terceros, proceso en el cual se realiza un intercambio de una o varias claves que permite codificar mensajes con seguridad absoluta siempre y cuando se realice un intercambio de claves de manera presencial (Pereyra, 2021). La criptografía es parte fundamental en el desarrollo de los procesos de seguridad de la información, y a medida que esta evoluciona se han implementado nuevas modelos que permiten mejorar los sistemas, a nivel de gestión, capacidad de respuestas y seguridad de los mensajes transmitidos (Sánchez, 2021).

2.5Marco Legal

Constitución Política de Colombia 1991

Con respecto a la normativa y legislación que atañe a los sistemas de gestión del riesgo de seguridad informática para el beneficio de la operatividad de las empresas, y las personas en general, la Constitución, mediante el articulo 15 proclama que,

> "Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en los bancos de datos y en archivos de entidades públicas y privadas." (p. 3).

De modo que la promulgación de dicho artículo es proclive a la protección de los datos siendo este un aspecto constitucional cuya garantía es jurídica haciendo referencia al almacenamiento y uso de la información y los datos personales, los cuales también incluyen los datos propios de las empresas y su funcionamiento.

Ley 1273 de 2009

A través de esta ley el Congreso de la República promulga acerca de la modificación del Código Penal para la protección de la información y de los datos, a la vez que se protegen de manera íntegra los sistemas que implementan las tecnologías de la información y las comunicaciones, considerando los diferentes daños, o alteraciones a los que se puede ver expuesto el sistema informático de cualquier usuario, siendo estos daños, robos, fraudes, entre otros delitos relacionados con la manipulación de los datos informáticos, de acuerdo con lo cual, el artículo 269ª se refiere al acceso no autorizado a los sistemas de información a través de medios tecnológicos afirmando que:

> "El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, incurrirá en pena de prisión de 48 a 96 meses, y, en multa de 100 a 1000 salarios mínimos legales mensuales vigentes" (p. 1).

Por su parte, la seguridad informática dada por la gestión de la prevención del riesgo debe estar regulada por las acciones que toda persona natural, o empresa realice para fines de impedimento de taques, ciberdelitos, entro otros. De acuerdo con lo cual, el articulo 269b de la Ley 1273 de 2009 establece que:

> "El que, sin estar facultado para ello, impida u obstaculice el funcionamiento o el acceso normal a un sistema informático, a los datos informáticos allí contenidos, o a una red de telecomunicaciones, incurrirá en pena de prisión de 48 a 96 meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con una pena mayor" (p. 1).

De modo que lo establecido por dicha normativa contempla la penalidad asociada a la obstaculización ilegitima del sistema informático, lo cual puede estar dado por bloqueos de datos, o por la inactividad subyacente de los ciberataques, siendo esto condenado por la Ley.

De manera que, todo impedimento al normal funcionamiento y operatividad a partir de los datos informáticos está contemplado en la penalización de dichas acciones a través de la ley, por lo cual, el artículo 269c acerca de la interceptación de los datos provenientes de sistemas informáticos contempla que quien:

> "…sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los transporte incurrirá en pena de prisión de 36 a 72 meses." (p. 1).

En razón de esto, la ley tiene en consideración las diferentes modalidades de alteración, robo, modificación, y sabotaje de los datos albergados en fuentes informáticas, por lo cual, la gestión de prevención de riesgos informáticos hace parte de los deberes de los usuarios, así como la capacitación para el uso y la prevención de riesgos informáticos, lo cual también incluye la respuesta generada para afrontar los ataques; de este modo, el articulo 269d que trata sobre el daño informático establece que, los usuarios no autorizados,

> "…sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos, o un sistema de tratamiento de información o sus partes o componentes lógicos, incurrirá en pena de prisión de 48 a 96 meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes" (p. 1).

Similarmente, el uso de software malicioso, es decir virus informáticos, así como la violación de datos personales, y la suplantación de plataformas digitales como forma de cat fish está contemplado y penalizado por la Ley 1273 de 2009 a través de los artículos 269 en sus apartados e, f, y g, respectivamente.

Por otro lado, la Ley Estatutaria 1581 de 2012 en favor de la protección de los datos personales, lo cual alude tanto a datos de usuarios en calidad de personas naturales, como a los datos almacenados para la operacionalización de las actividades de las empresas, establece mediante el articulo 1 la pertenencia de la misma, cuyo objeto es

> "…desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política; así

como el derecho a la información consagrado en el artículo 20 de la misma." (p. 1).

De manera que, si la información es un bien al que todos tienen derecho, también es cierto que el manejo y la confidencialidad de la misma corresponden a ciertas restricciones y consideraciones importantes que no apoya o favorecen el daño o el perjuicio; por lo cual, el ámbito de aplicación de dicha Ley dicta, a través del artículo 2, que "los principios y disposiciones contenidas en la presente ley serán aplicables a los datos personales registrados en cualquier base de datos que los haga susceptibles de tratamiento por entidades de naturaleza pública o privada" (p. 1).

Sin embargo, la información de carácter trasparente puede ser consultada y solicitada sin intervenir en delitos informáticos asociados al acceso no autorizado, el robo, sabotaje o alteración de los datos.

Código Penal colombiano

Por otra parte, el Decreto 599 de 2000 establecido en el Código Penal colombiano reúne los aspectos legales y punitivos de las faltas asociadas al inadecuado manejo de la información y los datos como activos de los soportes tecnológicos, por lo cual, el artículo 195 hace referencia a las consecuencias del acceso no autorizado a un sistema informático para en donde promulga que " El que abusivamente se introduzca en un sistema informático protegido con medida de seguridad o se mantenga contra la voluntad de quien tiene derecho a excluirlo, incurrirá en multa" (p. 31) lo cual está apoyado por las leyes anteriormente mencionadas.

Capítulo III. Diseño Metodológico

3.1 Tipo de Investigación

Se desarrolló una investigación Explorativa, ya que esta permitió comprender el tema abordado, y, a su vez, familiarizarse con lo investigado. Este tipo de investigación se aplicó de forma general dentro de las organizaciones encontradas en el municipio de Ocaña, puesto que, muchas organizaciones no manejan sistemas de gestión para la seguridad informática, de modo que la orientación y búsqueda sobre lo importante de un sistema de gestión garantiza la disponibilidad, confidencialidad y la integridad de la información.

De igual manera teniendo como referencia para el desarrollo de esta investigación, se implementó una metodología con enfoque cuantitativo, ya que se pretenden evaluar los riegos y amenazas latente dentro de las organizaciones abordando los temas de tecnología de la información, gestión de la seguridad y seguridad de la información a través de la recolección de datos.

3.2Población y Muestra

3.2.1Población

Esta investigación fue desarrollada tomando como referencia al sector empresarial de Ocaña-Norte de Santander, cuyas actividades económicas son principalmente de tipo comercial de compra y venta (Cámara de Comercio de Ocaña, 2017); así como los expertos en el área

"ingenieros informáticos", siendo de alto interés para la implementación y despliegue de la presente investigación.

$$n = \frac{NZ^2\ PQ}{d^2\ (Z-1) + Z^2 PQ}$$

3.2.2 Muestra

Ecuación estadística utilizada:

N= tamaño de la población

Z= nivel de confianza

P= probabilidad de éxito

Q= probabilidad de fracaso

d2 = Precisión

$$n = \frac{(2500)(1{,}96)^2\ (0{,}5)\ (0{,}5)}{(0{,}1)^2(2500-1) + (1{,}96)^2(0{,}5)\ (0{,}5)}$$

$$n = \frac{30625}{\beta 31} = 92{,}52$$

$$n = 92$$

Se obtuvo una muestra de 92 empresas en total para realizar la respectiva investigación, y de modo "no probabilístico", 4 ingenieros expertos en el área de riesgos informáticos, quienes participaron voluntariamente en la investigación.

3.3 Operacionalización de Variables

Tabla 1 Operacionalización de variables

Operacionalización de variables

Objetivos específicos	Variable	Dimensión	Indicador	Instrumento
Analizar el contexto de las empresas ubicadas en el municipio de Ocaña Norte de Santander, con el objetivo de conocer los protocolos que gestionan el riesgo de pérdida de información a través de técnicas de recolección de datos	Pérdida de Información	Protocolos de gestión de riesgo informático	• Ataques informáticos • Inactividad de la empresa por ataques • Medios tecnológicos • Sistema operativo • Portal de productos y servicios • Acceso a la información no autorizado • Ataques por robo de información • Almacén online • Personal de gestión de riesgos informáticos • Apoyo ante ataques informáticos • Seguimiento a los incidentes de seguridad informática	Encuesta
Caracterizar los estándares, métodos, técnicas y tecnología requeridos para la proposición de los componentes necesarios en un sistema de gestión del riesgo de seguridad informática, a partir de	Componentes de un sistema de gestión del riesgo de seguridad informática	Estándares, Métodos; Técnicas; y, Tecnologías	• Estándares metodológicos como criterios de análisis • Autores de tesis relacionadas • Tecnologías Emergentes	Análisis documental

un análisis previo del contexto				
Estructurar los componentes del sistema de gestión del riesgo en seguridad informática considerando las mejores prácticas de gestión de TI, mitigando con ello los incidentes que generan impactos negativos a nivel empresarial	Componentes del SGSI	Fases de la gestión del riesgo en seguridad informática	• Definición de la política • Alcance del SGSI • Análisis de Riesgos • Gestión del Riesgo • Selección de controles a implementar • Declaración de aplicabilidad • Revisión del sistema	Análisis documental
Aplicar un caso de pruebas en relación al sistema de gestión del riesgo, comprobando con ello su utilidad a través de una simulación de ataques informáticos	Utilidad del sistema de gestión de riesgo en seguridad informática ante ataques	Pruebas de verificación de eficiencia ante ataques informáticos	• Políticas • Seguimiento a los controles • Respuesta a incidentes • Mitigación de riesgos informáticos • Estructuración de Fases	Encuentro Google Meet y Entrevista semiestructurada

Capítulo IV. Resultados

Los resultados presentados a continuación dan cuenta del estado actual de los Sistemas de Gestión del Riesgo de la Seguridad Informática en beneficio de las empresas y su operatividad en el municipio de Ocaña, Norte de Santander; lo cual, conllevó al análisis del contexto de las empresas ubicadas en el municipio norte santandereano, con el objetivo de conocer los protocolos que gestionan el riesgo de pérdida de información a través de la recopilación de datos otorgados por los colaboradores de las empresas estudiadas; asimismo, se llevó a cabo la caracterización de los estándares, métodos, técnicas y tecnologías necesarias para la proposición de los componentes que un sistema de gestión del riesgo de seguridad informática exige partiendo del diagnóstico o análisis de los aspectos en seguridad informática y gestión de las empresas.

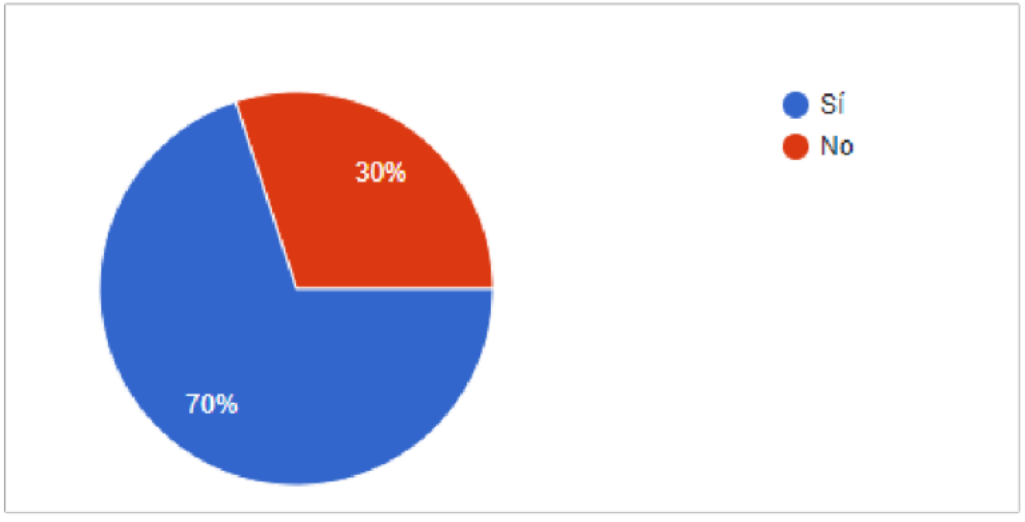
Por otra parte, el despliegue de la investigación confirió los medios para estructurar los componentes del sistema de gestión del riesgo en seguridad informática considerando las prácticas más favorecedoras aplicadas en la gestión de servicios de las tecnologías y la información (TI) ya que esto puede ayudar a mitigar los incidentes y demás situaciones que ponen en riesgo la funcionalidad operativa de las empresas. Adicionalmente, los resultados muestran la aplicación de un caso de pruebas y su relación con el sistema de gestión del riesgo a través de la comprobación de su utilidad mediante una simulación de ataques informáticos.

4.1 Análisis del Contexto de las Empresas Ubicadas en el municipio de Ocaña Norte de Santander, con el Objetivo de Conocer los Protocolos que Gestionan el Riesgo de Pérdida de Información a Través de Técnicas de Recolección de Datos

El contexto de la seguridad de la información y su gestión en las empresas del municipio de Ocaña-Norte de Santander fue analizado a partir de la información recolectada en torno a como se encuentran las empresas en su infraestructura tecnológica, así como de los mecanismos, acciones y actividades que son de ayuda para automatizar todos los procesos operativos, e incluso, acerca de las ventajas competitivas que estas gestiones les ofrecen a las empresas. De este modo, la información suministrada por las empresas del municipio de Ocaña, con respecto a la encuesta realizada, mostró los resultados detallados a continuación como parte del diagnóstico.

Figura 3

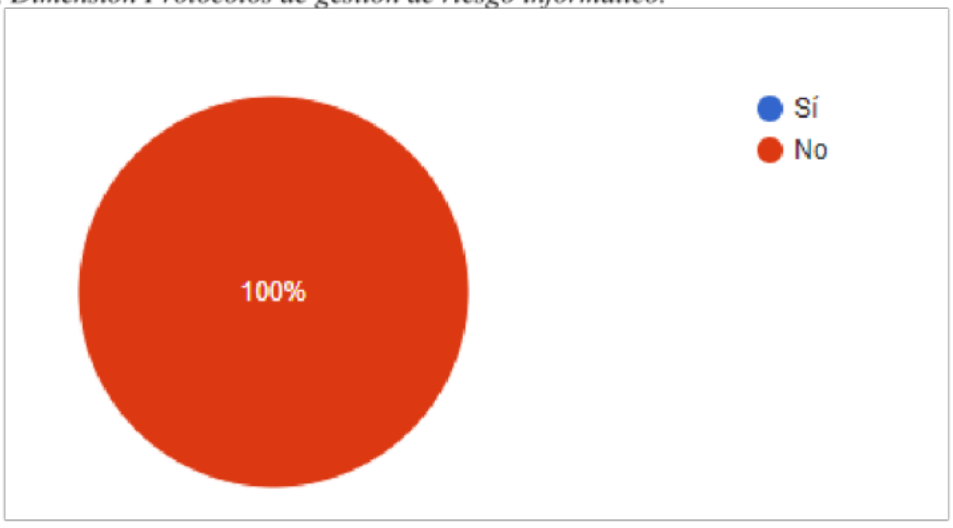
Pregunta A. ¿Han tenido ataques informáticos en los dos (2) últimos años? Acerca del indicador Ataques informáticos, de la variable Pérdida de información, Dimensión Protocolos de gestión de riesgo informático.



En cuanto a la variable perdida de información cuyo indicador hace referencia a la pregunta A de la figura 3, la mayoría de las empresas representadas por el 70% de los casos afirmaron que durante los últimos dos años han tenido ataques informáticos; mientras que, respecto a lo preguntado, el 30% de las empresas ofreció una respuesta negativa acerca de los ataques informáticos sufridos durante los últimos dos años. Por ende, se plantea que los ataques informáticos que impactan la seguridad de la información de las organizaciones y las compañías, pueden dificultar la implementación de tecnologías que ayuden a optimizar los procesos operacionales; por lo cual, estos percances ponen en verdadero riesgo a la operatividad de los servicios y productos generados siendo de suma importancia implementar sistemas de prevención ante las pérdidas de información.

Figura 4

Pregunta B. Si han sufrido ataques informáticos ¿éstos han detenido la operación del servicio de la empresa? Acerca del indicador Inactividad de la empresa por ataques, de la variable Pérdida de información, Dimensión Protocolos de gestión de riesgo informático.

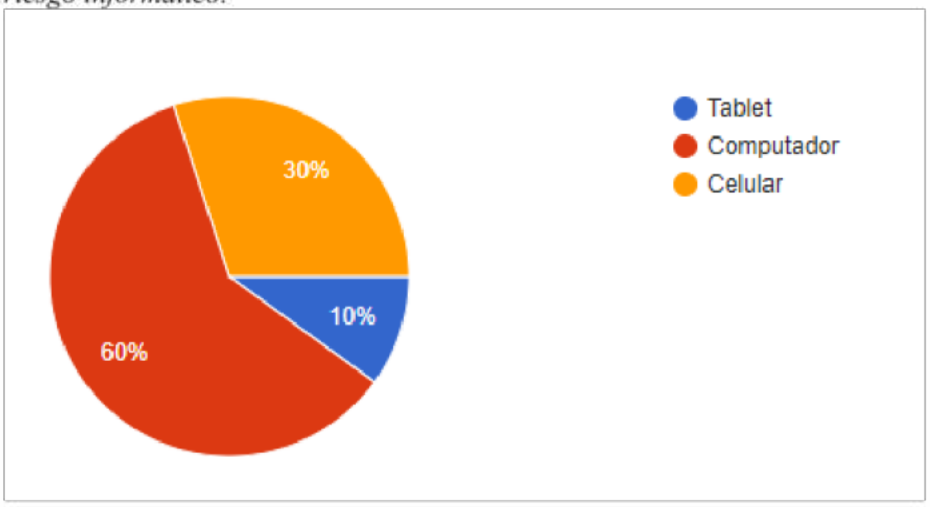


La grafica anterior plantea el tema de la seguridad de la información es un tema de vital importancia para mantener el funcionamiento de las empresas, así como garantizar la protección

de los usuarios, debido que, dicha información manejada requiere de un orden y una estructura en prevención de robos de documentación, entre otros; En este sentido, la figura 4 correspondiente a las respuestas ofrecidas por los representantes de las empresas de Ocaña-Norte de Santander, acerca de la detención e las operaciones de las empresas a causa de los ataques informáticos sufridos, se observó que la totalidad de los participantes afirman que en las empresas dichas actividades no han sido detenidas por tal causa.

Figura 5

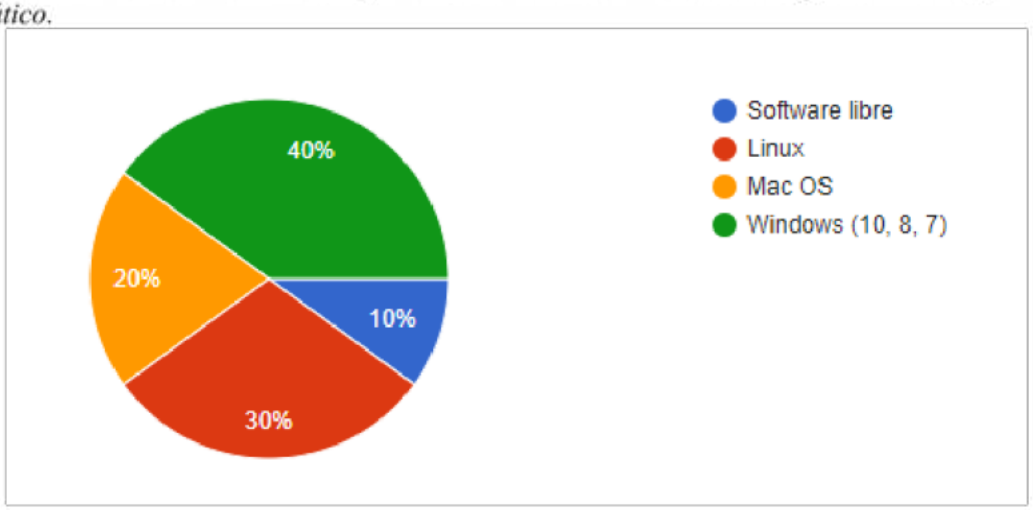
Pregunta C. ¿Qué tipo de medio de tecnología utilizan en su empresa (Tablet, computadores, celulares)? Acerca del indicador Medios tecnológicos, de la variable Pérdida de información, Dimensión Protocolos de gestión de riesgo informático.



El diagnóstico acerca de los medios tecnológicos utilizados en las empresas para ejecutar sus actividades se observó que, el 60% de las empresas de Ocaña-Norte de Santander utiliza el computador como herramienta de manejo tecnológico y de información; asimismo, el 30% de las empresas cuanta con el celular como parte de su estructura tecnológica; siendo el 10% de las empresas las que utilizan la Tablet para dichos fines (figura 5). Lo cual puede ser un indicio de que los parámetros de seguridad informática son adecuados en dichas empresas; no obstante, no

todos los ataques o peligros informáticos comprometen la operatividad de las empresas, puesto que las vulnerabilidades pueden no estar localizadas en la destrucción y alteración de la información.

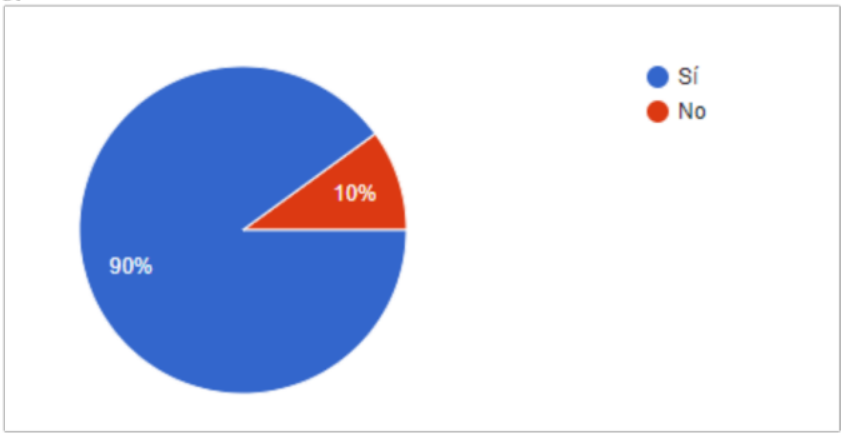
Figura 6 *Pregunta D. ¿Qué tipo de sistema operativo utilizan en la empresa? Acerca del indicador Sistema operativo, de la variable Pérdida de información, Dimensión Protocolos de gestión de riesgo informático.*



De manera consecuentemente, la figura 6 representa las opciones de las empresas en cuanto a los sistemas operativos usados a través de sus soportes tecnológicos, por lo cual, se observó que el 40% de las empresas en Ocaña-Norte de Santander hacen uso del sistema de Windows en alguna de sus versiones; asimismo, el 30% de las empresas del municipio en mención hacen uso del sistema *Linux*; en tanto que, el 20% de las empresas usan *Mac OS* como soporte tecnológico; y, el 10% de las empresas usan algún software libre. De acuerdo con esto, es necesario hacerle ver al empresario cuánto puede ganar con el buen uso de la tecnología, lo cual implica empezar por lo básico, es decir, desde el uso de internet o el correo electrónico, hasta el uso de aplicaciones administrativas para mejorar la gestión de la empresa.

Figura 7

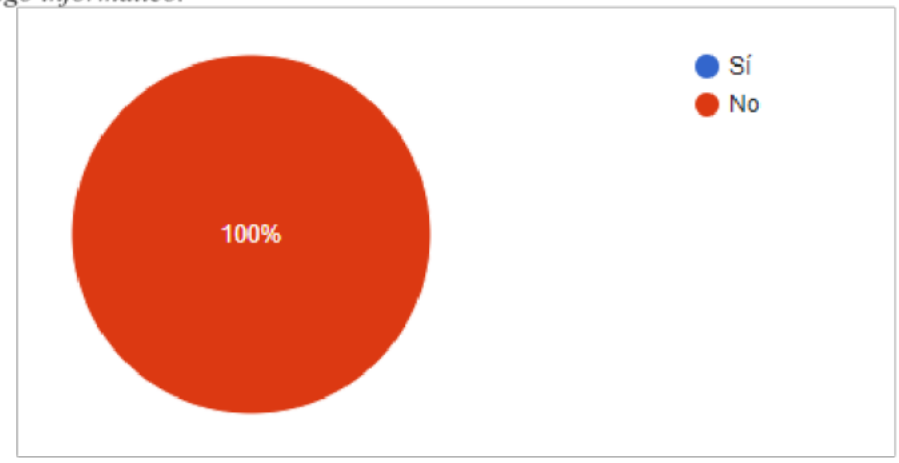
Pregunta E. ¿Utilizan algún portal donde brindan sus productos o servicios? Acerca del indicador Portal de productos y servicios, de la variable Pérdida de información, Dimensión Protocolos de gestión de riesgo informático.



La figura 7 sobre el indicador portal de servicios y productos de las empresas Ocañeras, mostró que el 90% de tales empresas cuenta con un portal online como almacén de los servicios y productos ofertados, de modo que, el 10% de las empresas del municipio señalaron que no cuentan con dicho portal online. Dichos recursos usados como soporte tecnológico pueden ayudar a la promoción del análisis y desarrollo de estrategias que ayuden a prevenir la pérdida de información subyacente de los riesgos que representa la susceptibilidad de los sistemas informáticos y sus planes de prevención.

Figura 8

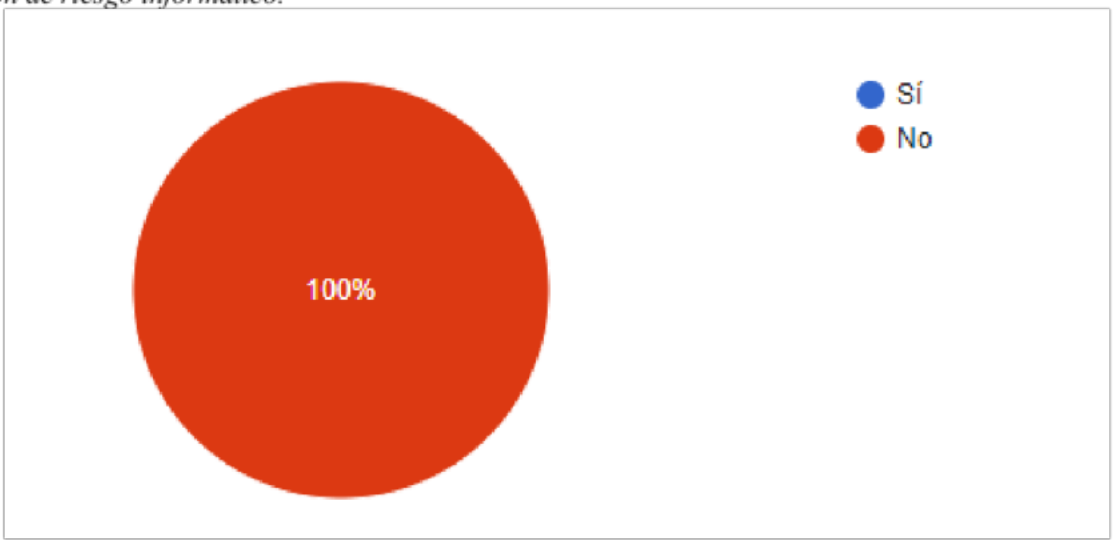
Pregunta F. ¿Ha sufrido robo o secuestro de su información dentro de la empresa? Acerca del indicador Acceso a la información no autorizado, de la variable Pérdida de información, Dimensión Protocolos de gestión de riesgo informático.



Por su parte, la Figura 8 representa porcentualmente las opciones mediante las cuales, empresas de Ocaña-Norte de Santander aseguran haber sido víctimas de robos o secuestros de la información al interior de la empresa. De este modo, se observó que la totalidad de las empresas no estuvo de acuerdo con lo afirmado, siendo esto un factor clave a considerar para la gestión de la prevención de riesgos de pérdidas de información en sistemas informáticos. De tal modo que, se analiza la extensión de las ofertas asevera las posibilidades brindadas a sus clientes y usuarios para la adquisición de servicios y productos, agilizando de esta forma los procesos comerciales, lo cual trae consigo el tratamiento de datos, siendo este un aspecto a considerar para la seguridad informática y la gestión de la protección de la información

Figura 9

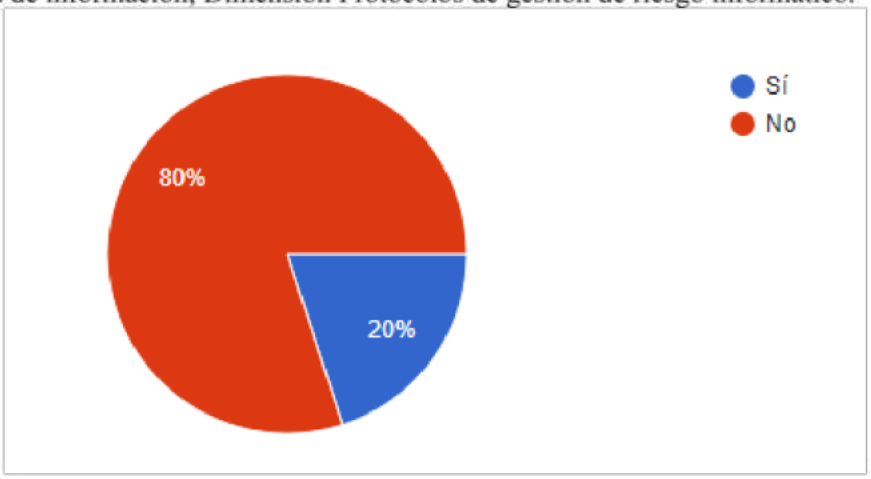
Pregunta G. ¿Han sufrido algún tipo de extorsión a causa de robo de información? Acerca del indicador Ataques por robo de información, de la variable Pérdida de información, Dimensión Protocolos de gestión de riesgo informático.



Se sabe de hecho que los robos, secuestros o usos no autorizado de la información por parte de los colaboradores de las empresas se constituye como un ciberataque común cuyas consecuencias legales, peor también incluye aquellas que comprometen la imagen de la empresa, siendo esto negativo para su competitividad y sus actividades operativas, incluyendo en el organigrama empresarial. Aun así, el indicador ataques por robo de información, representado mediante la Figura 9 acerca de si las empresas en Ocaña-Norte de Santander han sufrido alguna extorsión como consecuencia del robo de información mostró que tal situación es negativa, puesto que la totalidad (100%) de las empresas Ocañeras no han sufrido algún tipo de extorsión.

Figura 10

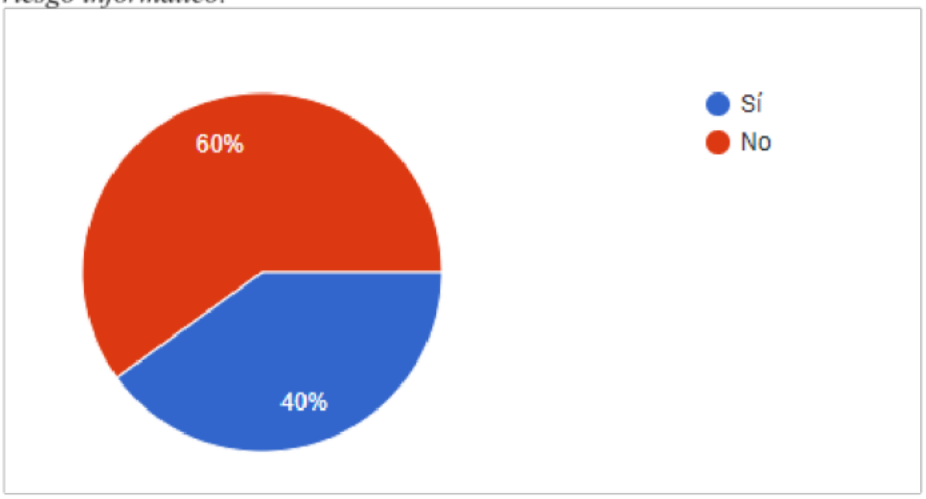
Pregunta H. ¿Actualmente cuentan con algún servidor propio? Acerca del indicador Almacén online, de la variable Pérdida de información, Dimensión Protocolos de gestión de riesgo informático.



En este sentido, la extorsión es considerada como un ciberataque cuyo impacto al interior de las empresas puede desencadenar en la inestabilidad de las operaciones dado por la alteración de las redes de seguridad informática generando pérdidas económicas y la disminución de la competitividad y la confiabilidad. Por ende, lo que a contar con un servidor propio respecta, la Figura 10 correspondiente a la representación porcentual de la pregunta H acerca del indicador almacén online, mostró que el 80% de las empresas Ocañeras no cuentan con algún servidor propio; en tanto que, el 20% de las empresas restantes afirmaron que si cuentan con un servidor propio.

Figura 11

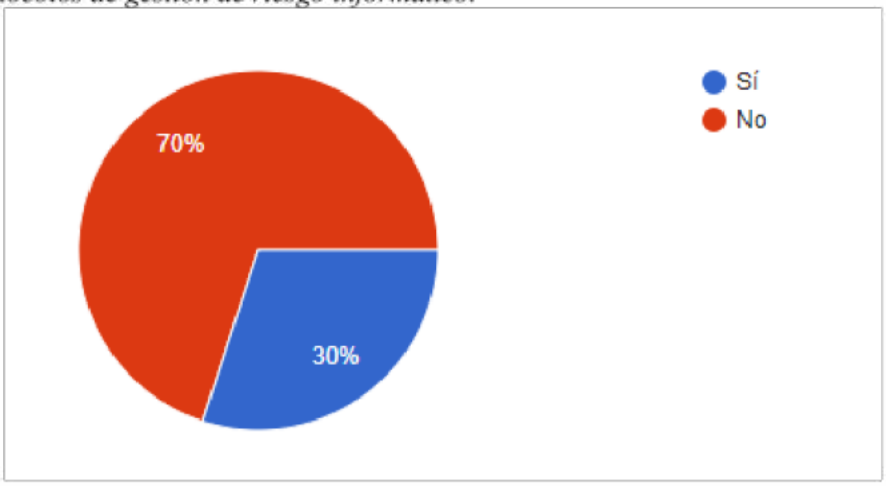
Pregunta I. ¿Cuentan con algún servicio de tercerización dónde monten su almacén de forma online? Acerca del indicador Ataques informáticos, de la variable Pérdida de información, Dimensión Protocolos de gestión de riesgo informático.



Asimismo, la pregunta I concerniente a la dimensión Protocolos de gestión de riesgo informático en las empresas de Ocaña-Norte de Santander, representado en la Figura 11 mostró que el 60% de las empresas estudiadas no cuentan con servicio alguno de tercerización donde monten su almacén de forma online; y, por el contrario, el 40% de las empresas afirman contar con algún servicio de tercerización de almacén online. Se puede observar la utilización de un servidor propio para las actividades comerciales de las empresas es considerado, como parte de las estrategias que la empresa desarrolla para controlar su propia seguridad, de modo que contar con un servido propio garantiza que las gestiones en materia de seguridad pueden cumplirse a cabalidad; lo cual no ocurre con la mayoría de las empresas Ocañeras.

Figura 12

Pregunta J. ¿Cuentan con personal idóneo dentro de la empresa para atender ataques informáticos? Acerca del indicador Personal de gestión de riesgos informáticos, de la variable Pérdida de información, Dimensión Protocolos de gestión de riesgo informático.

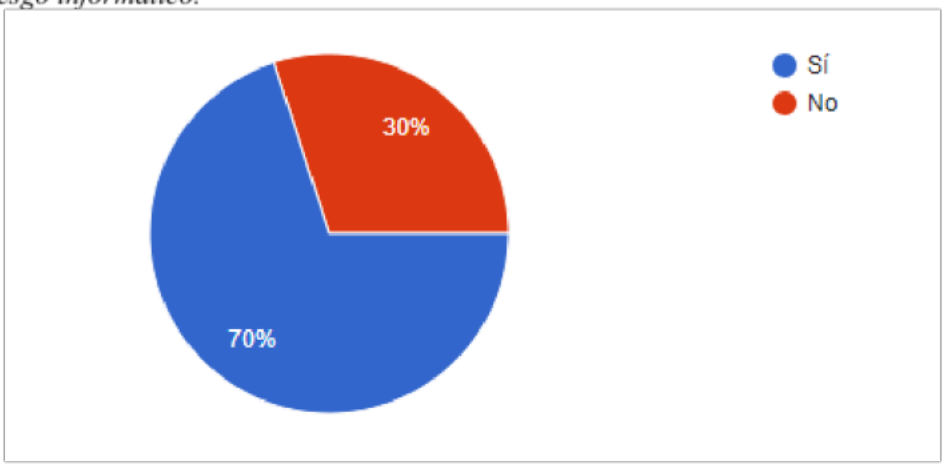


A pesar de esto, la prevención y gestión de riesgos por ciberataques pueden ser manejados por personal especializado dentro de las empresas quienes serán responsables de planear y diseñar los sistemas de seguridad de la información. Por lo cual, la Figura 12 en representación de los resultados de la pregunta J mostró que el 70% de las empresas en Ocaña-Norte de Santander no cuentan con personal idóneo dentro de la empresa para atender ataques informáticos ante los riesgos por pérdida de información; mientras que, el 30% de las empresas Ocañeras si cuentan con tal equipo de trabajo en atención a los riesgos de seguridad informática. Es decir generalmente los servicios de comercio electrónico son convenientes para ampliar las ofertas de las empresas, sin embargo, los métodos y mecanismos para las ventas y prestaciones

de servicios ejecutadas por internet representa ciertas susceptibilidades para la empresa debido al manejo de datos y el acceso a la información como activos y medios para las operaciones comerciales de compra y venta, siendo esto un aspecto a considerar para restringir y bloquear el acceso no autorizado para la promoción y recambio de stocks

Figura 13

Pregunta K. ¿Si no cuentan con personal idóneo dentro de la empresa para atender ataques informáticos buscan una persona fuera de la empresa para atender esa clase de inconvenientes? Acerca del indicador Apoyo ante ataques informáticos, de la variable Pérdida de información, Dimensión Protocolos de gestión de riesgo informático.

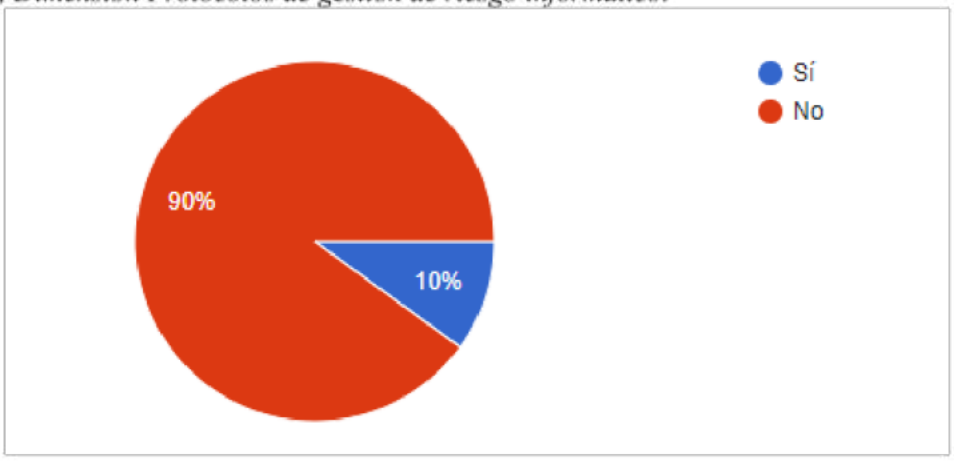


De acuerdo con lo descrito anteriormente, la Figura 13 muestra las alternativas de solución por las que optan las empresas en Ocaña-Norte de Santander para mitigar y contrarrestar los efectos de los riesgos informáticos a través de personal idóneo y calificado para tal gestión. De manera que, el 70% de las empresas afirmo que en caso de no contar con personal idóneo para atender los problemas por ataques a la seguridad informática tratan de buscar a una persona externa a la empresa para atender esa clase de inconvenientes; y por otra parte, se observó que el 30% de las empresas no solicitan tal apoyo, lo cual correspondió al indicador de apoyo ante ataques informáticos. De manera que, lo anteriormente mencionado puede indicar que la confiabilidad de las empresas (30%) cuentan con personal especializado para el manejo de

los riesgos informáticos incluyen a este factor, confiabilidad, como forma de asegurarse de que existen autorizaciones para el acceso a los recursos informáticos que están a nombre de los encargados del área, lo cual puede ocurrir a través del cifrado de información o la gestión de privilegios.

Figura 14

Pregunta L. Cuándo sufren algún ataque informático dentro de la empresa ¿han conseguido en Ocaña apoyo para atender dicho problema (algún grupo de especialistas en el tema o la Universidad Francisco de Paula Santander)? Acerca del indicador Apoyo ante ataques informáticos, de la variable Pérdida de información, Dimensión Protocolos de gestión de riesgo informático.

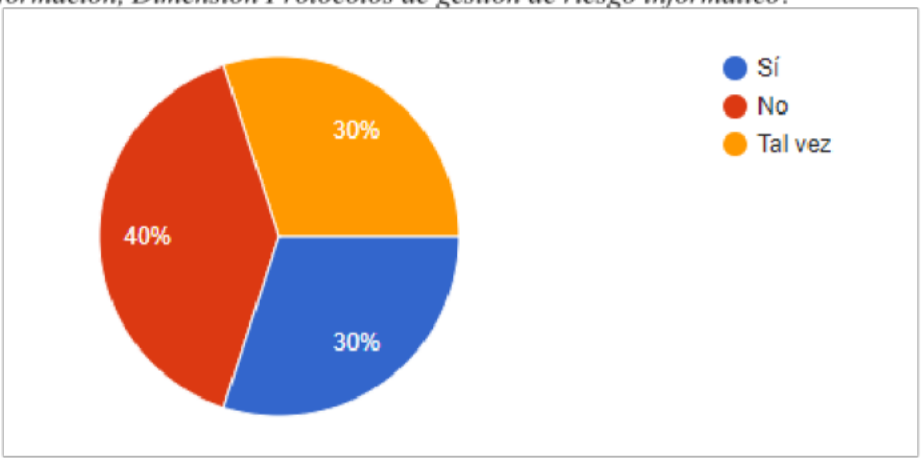


En seguimiento con el diagnóstico, se formuló la pregunta L acerca de, si en caso de sufrir ataques informáticos las empresas han conseguido apoyo para atender dicho problema; lo cual está representado en la figura 14, en donde como protocolos de gestión de riesgo informático, se observó que el 90% de las empresas no han conseguido en Ocaña apoyo para atender dicho problema que pueda incluir a personal externo como por ejemplo especialistas en el tema circunscritos a la Universidad Francisco de Paula Santander; mientras que el 20% de las empresas restante afirmó que si han buscado tales recursos humanos mencionados anteriormente. A partir de estos resultados, es posible afirmar que la irregularidad que implica contar o no con

personal idóneo para la resolución de problemáticas de seguridad informática puede ser una ventana para dar paso a que los ciberdelincuentes hagan provecho de la ausencia que regularmente representa la escasez de personal de seguridad informática para la administración de los datos y recursos.

Figura 15

Pregunta M. ¿A usted, como empresa le gustaría que la Universidad Francisco de Paula Santander-Ocaña, desde el observatorio de innovación tecnológica y en conjunto con el programa de ingeniería de sistema se les brindara apoyo y seguimiento a los incidentes de seguridad informática, de la variable Pérdida de información, Dimensión Protocolos de gestión de riesgo informático?



En atención a estas afirmaciones, la figura 15 que representa las respuestas de las empresas en cuanto a que la Universidad Francisco de Paula Santander-Ocaña, desde el observatorio de innovación tecnológica y en conjunto con el programa de ingeniería de sistema brinde apoyo y seguimiento a los incidentes de seguridad informática, se observó que el 40% de las empresas participantes no estuvieron de acuerdo con esta propuesta; mientras que, una parte del 30% considero que definitivamente si les gustaría recibir tal seguimiento y apoyo, en tanto otra parte correspondiente al 30% afirmo que tal vez les gustaría ser parte del tal seguimiento.

De esta forma, se observó que la mayoría de las empresas no cuentan con una organización en cuanto a su personal de confianza para gestionar y tratar estas problemáticas alusivas a la seguridad de la información y los datos; lo cual puede conllevar a que, las empresas no consolidadas en su seguridad informática como parte de la cultura corporativa puedan ser propensa a los peligros de los ataques informáticos derivados de los bajos estándares de ciberseguridad

Estos resultados corroboran la importancia que representa la gestión de la seguridad de los sistemas informáticos teniendo en cuenta que los activos informáticos son los recursos que los planes de prevención de riesgos deben tener como fuente de mitigación ante los peligros a los cuales se encuentra expuesto el monitoreo y la gestión informática en las empresas. De modo que, el análisis, identificación, y erradicación de los incidentes en torno a los datos y la información debe ofrecer pautas sobre cómo proceder a evitar el riesgo de pérdidas de información como parte del contexto empresarial.

A partir de los hallazgos y la descripción de los atributos de las empresas de Ocaña-Norte de Santander se puede contextualizar la situación actual a partir del diagnóstico de las características del sistema de gestión del riesgo de seguridad informática.

Los factores internos y externos de la Matriz DOFA están basados en los aspectos negativos y positivos de los sistemas de seguridad informática de las empresas de Ocaña-Norte de Santander como parte del análisis del diagnóstico de contexto, en el cual se reflejan las debilidades, oportunidades, fortalezas, y amenazas de las empresas con respecto a los protocolos que conforman las medidas para minimizar y mitigar el riesgo de pérdida de información.

De tal manera que, la Tabla 2 corresponde a los factores internos y externos que reflejan el diagnóstico del contexto de las empresas ubicadas en el municipio de Ocaña Norte de

Santander, con el objetivo de conocer los protocolos que gestionan el riesgo de pérdida de información, como resultado derivado de la aplicación del instrumento.

Tabla 2 Matriz DOFA acerca de los sistemas de gestión de seguridad de la información en las empresas de Ocaña-Norte de Santander.

Matriz DOFA acerca de los sistemas de gestión de seguridad de la información en las empresas de Ocaña-Norte de Santander.

	POSITIVOS	NEGATIVOS
	FORTALEZAS	**DEBILIDADES**
INTERNOS	• Seguridad ante riesgos informáticos de ciberataques en los dos últimos años • Continuidad de las operaciones del servicio de las empresas • Disponibilidad de varios sistemas operativos para las actividades comerciales de la empresa y su seguridad informática • Disponibilidad de algún portal para el ofrecimiento de productos o servicios • Cero reportes de robo, secuestro y extorsión de información al interior de las empresas	• Medios tecnológicos poco diversos para el soporte de los ciberataques • Ausencia de servidor propio para la gestión de riesgos informáticos • Escasez de personal idóneo dentro de las empresas para atender ataques informáticos
	OPORTUNIDADES	**AMENAZAS**
EXTERNOS	• Capacitar al equipo técnico en seguridad de la información • Realizar planes de mejora para los sistemas de información • Garantizar el uso de las buenas prácticas para el uso de las herramientas tecnológicas • Implementar un servicio de tercerización dónde pueda hacerse el montaje de almacén de forma online • Búsqueda de apoyo externo ante ataques informáticos • Posibilidad de incorporar especialistas de apoyo para atender los problemas del ciberataque en las empresas	• Falta de mantenimiento periódico en los servidores donde se localiza la base de datos • Mal uso de las herramientas tecnológicas • Falta de políticas de seguridad • Poco interés en aceptar ayuda y seguimiento a los incidentes de seguridad informática de las empresas • desprotección técnica contra el fraude informático

La matriz DOFA de la tabla 2 contiene el análisis de las características favorecedoras en cuanto a los sistemas de gestión de riesgos informáticos para las empresas en Ocaña-Norte de Santander, de las cuales se destacan las fortalezas que las empresas tienen en cuanto al manejo de la gestión de la seguridad informática dada por los casos favorables en los que no se reportaron robos, ni ataques de tipo cibernético, siendo esto un aspecto positivo que refleja el adecuado manejo de las restricciones hacia la información, así como del personal a cargo de la misma.

Conjuntamente, otro aspecto que representa una solidez para las empresas radica en la que, de acuerdo con los resultados de la encuesta, el 100% de las empresas no detuvo sus operaciones frente a ataques informáticos, errores, fallos, o ataques hacia la información, siendo esto un buen indicio acerca de la confiabilidad, lo cual en concordancia con lo estipulado anteriormente con los resultados de la encuesta, el 60% de las empresas, no cuenta con servicio de almacenamiento en la nube; hecho que desmiente su afirmación en donde los clientes o usuarios pueden visualizar sus procesos de adquisición de bienes y servicios a través del seguimiento del stock.

En este sentido, el análisis de las fortalezas representa el lado positivo de todos los factores internos de las empresas, lo cual subyace de los procesos propios como parte de sus interacciones; características que muestran la seguridad informática empresarial que reside en el adecuado manejo de los recursos internos para evitar los incidentes productivos y financieros derivados del inadecuado uso y acceso de la información. De igual manera los factores internos propios de la operatividad de las empresas representan ciertas debilidades que como resultantes del análisis DOFA pone en consideración la mejora de dichas características negativas e internas a cada organización, lo cual destaca la poca diversidad de medios tecnológicos usados como

soporte para prevenir los ciberataques; así como la ausencia de servidores propios para la gestión de riesgos informáticos en las empresas Ocañeras; y, la escasez de personal idóneo dentro de las empresas para atender los imprevistos relacionados con la seguridad informática.

De manera las amenazas de dicha matriz se obtuvieron a partir de los hallazgos y la descripción de los atributos de las empresas de Ocaña-Norte de Santander de acuerdo al análisis de los factores internos negativos como diagnóstico del contexto de la gestión para los sistemas de seguridad informática de las empresas Ocañeras, ofrece como resultados a las debilidades cuyas características contrarias a las fortalezas señala los aspectos a intervenir para la mejora.

No obstante, dicha mejora puede estar dada, también, por la identificación de las oportunidades, lo cual es un factor externo, debido que, depende de lo que el mercado imponga, siendo esto un aspecto para analizar a partir de la competitividad y la productividad, lo cual mostró que, los puntos de mejora externos para las empresas en estudio corresponden a capacitar al equipo técnico en seguridad de la información; lo que, puede incluir la realización de planes de mejora para los sistemas de información; garantizar el uso de las buenas prácticas para el uso de las herramientas tecnológicas; implementar un servicio de tercerización dónde pueda hacerse el montaje de almacén de forma online; buscar apoyo externo ante ataques informáticos; y la contemplación de la posibilidad de incorporar especialistas de apoyo para atender los problemas del ciberataque en las empresas. Por otra parte, el análisis del contexto ofrece como diagnóstico los aspectos negativos de los factores externos conformados por las amenazas, que en el caso de las empresas Ocañeras se trata de la falta de mantenimiento periódico en los servidores donde se localiza la base de datos; el mal uso de las herramientas tecnológicas; la falta de políticas de seguridad; el poco interés en aceptar ayuda y seguimiento a los incidentes de seguridad

informática de las empresas; y la poca disponibilidad de personal de gestión de riesgos informáticos vinculados a las empresas.

4.2 Caracterización de los Estándares, Métodos, Técnicas y Tecnología Requeridos para la Proposición de los Componentes Necesarios en un Sistema de Gestión del Riesgo de Seguridad Informática, a Partir de un Análisis Previo del Contexto

La importancia de entender los distintos estándares, métodos, técnicas y tecnologías para asegurar procesos que se gobiernan o que están apoyados en procesos de la información y las comunicaciones exige considerar a detalle las distintas perspectivas de autores, así como los sistemas, y conocimientos en favor de mejorar el contexto organizacional (Tamayo, 2020); por lo cual, los estándares, métodos, técnicas y tecnologías son detallados a continuación:

Los componentes necesarios en un sistema de gestión del riesgo de seguridad informática se basan principalmente en tres ejes denominados confiabilidad de datos, integridad, y disponibilidad, puesto que estos determinan la seguridad y fortaleza de las empresas en cuanto al manejo eficiente y eficaz de la información cuidando de la verificación y uso de la misma por parte de personal idóneo y autorizado (Fernández, 2021).

En este sentido, la confiabilidad de un sistema informático en lo que respecta al manejo de datos está estrechamente relacionado con resguardar la privacidad de la información (datos) a través de las acciones que las empresas planean ejecutar para el uso de estos datos y su seguridad ante sabotaje, espionaje, y ciberataques en general (Cruz & Cerrillo, 2020). Debido a esta obligatoria disposición de las empresas a garantizar la seguridad de sus usuarios, los responsables del área de seguridad informática deben esclarecer y conocer las metodologías,

técnicas y herramientas requeridas para la gestión de la seguridad de los datos más significativos que pueden acarreare serias consecuencias (Bailón-Lourido, 2019).

Por otra parte, las acciones a implementar para el incremento de la seguridad informática hacen necesaria la organización y estructura de las jerarquías colaborativas, lo cual significa que, los datos deben responder a un orden con el ánimo de que el personal encargado de la seguridad pueda conocerlos para realizar el manejo pertinente, y, asimismo, identificar aquellos cuyas vulnerabilidades son elevadas siendo esto una acción de gestión y prevención aunado al uso de tecnologías en donde los sistemas de seguridad construyan barreras de acceso (Bermúdez & Bailón, 2015); y a su vez, resguarde la información, como por ejemplo, con el encriptado de datos, y los mecanismos de verificación de identidad.

Por su parte, la disponibilidad como parte central de la seguridad de los sistemas informáticos relaciona el tiempo con la accesibilidad de los datos, en donde para las empresas se posibilita la consulta y verificación de la información; siendo la disponibilidad un aspecto problemático para las empresas en caso de presentar fallas, puesto que, la falta de acceso a los sistemas y a la información necesaria puede conllevar a la pérdida económica como consecuencia de no culminar procesos de compra o prestaciones de servicios de manera oportuna (Martín, 2021). No obstante, la solución de estos imprevistos está dada por la prevención, debido que, las actividades de mantenimiento y actualización necesariamente elimina los problemas de software y de estructuras de hardware permitiendo la actualización en el funcionamiento.

Dentro de los aspectos de la disponibilidad de la información se resalta, entonces, la actualización de los sistemas basados en una temporalidad establecida, así como la examinación de la compatibilidad de las actividades con relación a la conectividad para la oportuna ejecución de las diferentes diligencias tecnológicas relacionadas con los intercambios de las empresas

(Bautista, 2018);en donde los recursos de la disponibilidad consideran la agilidad, eficiencia y afirmación de los procesos de verificación de documentos, compra, venta, generación de facturas, cierre de tratos, entre otros, de modo que, la información de interés empresarial pero de confidencialidad personal sea dispuesta para el correcto tramite de los procesos de negocios (Pineda & Burbano, 2019).

Otro componente que atañe a los estándares, métodos, técnicas y tecnología de un sistema de gestión del riesgo de seguridad informática es la integridad, lo cual se refiere a la precisión y la estabilidad de los datos, y, en general, de los sistemas operativos y de seguridad por los que se rigen los servicios comerciales de las empresas (Ayala, 2017), siendo importante que la integridad englobe la intervención a la información para su manejo por parte del personal autorizado sin que esto signifique la alteración, o el daño de la misma.

Con relación a esto, la integridad de la seguridad de los sistemas informáticos está orientada a prevenir la alteración de los datos, lo que, a su vez, puede ser prevenido y contrarrestado a través de acciones como otorgar permisos, implementar sistemas de verificación de identidad, entre otros (Criollo, 2017). Asimismo, los estándares, métodos, técnicas y tecnologías que implementa un sistema de gestión del riesgo de seguridad informática está determinado por los criterios de las metodologías de normalización (Suárez, 2015), de tal manera que, los estándares y las metodologías para la ejecución de la gestión de seguridad informática puede surgir de los efectos sinérgicos de la combinación de distintas herramientas, técnicas y métodos enfocados en las etapas operativas de un sistema de gestión de seguridad informática.

En virtud de lo anterior, la tabla 3 reúne las normas, métodos y metodologías, las cuales se centran en la seguridad informática y todo lo concerniente a la gestión de riesgos a través de los incidentes consecuentes de actividades indebidas, cuyo análisis contribuye a responder ante

las posibles vulnerabilidades permitiendo identificar todas esas medidas preventivas que se deben tener ante las situaciones desfavorables.

Tabla 3*Estándares metodológicos como criterios de análisis*

Estándares metodológicos como criterios de análisis

Nombre de la Metodología	**Variable tratada**	**Lo que propone**	**Observación**
ISO 27001	Trata la Confidencialidad, Integridad y la Disponibilidad de la información de las empresas y las aplicaciones de los sistemas de seguridad informática.	Propone unos lineamientos para que las empresas puedan gestionar la información, incluso si es perteneciente al propio conocimiento y experiencia de las personas, o, sea tratada en reuniones etc.	Esta norma brinda mucha ayuda a las empresas y organizaciones en provecho del mejoramiento de la gestión de los riesgos concernientes a la seguridad informática. De igual manera, dicha metodología se centra en la seguridad de los datos.
Apropiación de métodos criptográficos	La Integridad de la información a través de la autenticación, y validación de la identidad.	Propone mecanismos para la protección de los datos de los usuarios corporativos, configurando su forma, de manera que, sea incomprensible ante el acceso no autorizado.	Los métodos criptográficos están en un continuo auge en diversas aplicaciones, puesto que, este método Es un método puede servir para escribir un mensaje con clave de manera secreta, buscando siempre las garantías para la protección de los datos y la información.
	Seguridad en la conectividad, los datos,	Ofrece una serie de pautas para garantizar y	Brinda el acompañamiento a todas

Controles de Ciberseguridad (CCS) ISO 27032	las redes; y la protección de infraestructuras tecnológicas críticas para la información.	proteger la seguridad de los datos para prevenir la pérdida de información, la cual se ve comprometida durante los intercambios que la hacen susceptible de hackeos, sabotajes o alteraciones	las organizaciones para que puedan estar respaldadas en todo el intercambio de información que hagan en la red frente a otras organizaciones o empresas consiguiendo una manera efectiva de hacer frente ante el Cibercrimen con una cooperación entre todos los empleados y personal empresarial.
Metodología de Análisis y Gestión de Riesgos de TI MAGERIT	Confidencialidad, Integridad y Disponibilidad de los recursos como objetos de riesgos.	Esta metodología propone sensibilizar al personal encargado de estructurar y organizar la información asociada a la existencia de riesgos y la consecuente necesidad de gestionarlos. Asimismo, ofrece un método sistemático para el análisis de los peligros procedentes del uso de tecnologías de la información y comunicaciones. A su vez, esta metodología contribuye con el descubrimiento y planificación de los riesgos a partir del oportuno tratamiento de los riesgos. Adicionalmente, la finalidad de este método, se basa en preparar a las empresas	Ofrece patrones para el análisis de los efectos de la inseguridad y la violación de la información en las empresas implicadas ayudando a la búsqueda de potenciales amenazas que comprometen el desempeño empresarial a partir de la identificación de las para establecer medidas preventivas eficientes.

		para continuar con los procesos administrativos propios de la evaluación, auditoría, certificación, entre otros.	
NTC ISO-31000	Valoración, tratamiento, monitoreo y seguimiento del riesgo.	Propone unos lineamientos para la gestión del riesgo de las organizaciones, entidades o empresas bajo un marco de trabajo que integre los mecanismos de prevención, tratamiento e identificación de los riesgos en todas las actividades operativas de las empresas ofreciendo, a su vez, una estructura de funcionamiento compleja para un adecuado sistema en la consecución de los objetivos de gestión de seguridad particulares.	La revisión y análisis de esta normativa permite a las empresas integrar la toma de decisiones, a partir del abordaje de las incertidumbres de la gestión del riesgo de manera estructurada, sistemática y oportuna basándose en los procesos de adaptación de las organizaciones al uso de la información disponible que forman parte de las entradas del proceso de la gestión de riesgos tales como las fuentes de información.
Manual ITIL	Disponibilidad e integridad de los ciclos de servicios de estrategias, diseño, transición, operación y mejoramiento continuo de los servicios.	Propone una serie de buenas prácticas dirigidas a que las empresas logren guiar su área tecnológica para la optimización de la comercialización de los servicios y productos Demandados en el mercado para estar en constante disposición de los usuarios a través de la gestión eficiente de los procesos del ciclo	Esta normativa ofrece a las empresas un sistema de buenas prácticas, la cual les permite gestionar eficientemente los servicios tecnológicos para el adecuado uso de la información. Asimismo, este sistema brinda las pautas para que las organizaciones puedan desarrollar una infraestructura de

		del servicio.	operaciones de las tecnologías de información destinadas a la mejora de los servicios y productos ofrecidos a los usuarios a partir de la alineación de la calidad, la satisfacción del cliente, y la independencia de las buenas prácticas ante las exigencias del entorno.
Estándar Australiano AS/NZS 4360	Integridad y confiabilidad, en la identificación, clasificación y valoración de los riesgos.	Este sistema propone una normativa global orientada a la gestión de riesgos aplicada a diversas actividades ejecutadas por las empresas o por entidades cuya estructura organizacional requiera la administración de riesgos en adaptación a las necesidades y características propias.	Este esquema metodológico se constituye como un sistema cuyas directrices contribuyen con las pautas para la implementación de los procesos del manejo del riesgo, a partir del cual las empresas pueden incluir en sus actividades la identificación, la evaluación, el análisis, y el tratamiento de los recursos en el manejo del riesgo como parte del contexto de la organización. Por lo cual, estas pautas siguen los procesos que regulan la administración de riesgos que pueden tener lugar en el ámbito financiero, de la competitividad, operativo, político, y

social de las empresas que lo implementan.

La síntesis de las metodologías consultadas y consignadas anteriormente, generan una perspectiva acerca de la aplicación, implementación, logros y alcances de cada una con relación a ejecución de un proyecto, siendo estos aportes capaces de estandarizar, estructurar y organizar la manera de trabajar. De modo que, los estándares, métodos, y técnicas necesarias en un sistema de gestión del riesgo de seguridad informática, permiten tener un enfoque en los resultados que se desean obtener en los proyectos, contemplando sus éxitos y perfeccionando las pautas, por lo que se hace un proceso de mejoras continuas, generando así, una notoria eficiencia en la medida en que se van utilizando y aplicando en el desarrollo de las investigaciones.

De acuerdo con la tabla 3 acerca de los estándares metodológicos como criterios de análisis, se destaca que, las normas que proporcionan mayores beneficios, y que permiten un mayor proceso de identificación y realización del proyecto en la búsqueda de protección de los activos informáticos de una empresa corresponden a la Norma ISO 27001 y la Norma ISO 27032.

Con respecto a la primera, la Norma ISO 27001:2013 se constituye como un conjunto de directrices internacionales, la cuales orientan que la empresa pueda seguir unas pautas para el manejo de la seguridad de la información a través de la confidencialidad de los datos, la integridad, y la disponibilidad de los mismos cumpliendo con la legislación en términos de tratado de datos. De modo que, esta normativa representa un estándar para la protección de los activos informáticos de las empresas, cuya implementación se enfatiza en los procesos de

instituir, manejar y mantener los sistemas de gestión de seguridad informática al interior de las organizaciones.

En cuanto a los aspectos legales, dicha normativa contempla los riegos y amenazas a partir de las implicaciones de los ciberdelitos que incluye la manipulación no autorizada de datos personales, así como el uso de virus y otras acciones que debilitan el funcionamiento de los sistemas informáticos de las empresas (Nieves, 2017). Es por ello que, para tal normativa la integridad, confidencialidad, y la disponibilidad de la información hacen parte de los componentes requeridos para los sistemas de gestión de seguridad informática.

En cambio, los Controles de Ciberseguridad corresponden a un conjunto de operaciones, de análisis y eficiencia acerca de la mejora de los criterios de ciberseguridad en una organización, compañía o empresa pudiendo abarcar una amplitud de estándares, y esfuerzos para la adecuación de un ciberespacio que sea eficiente, organizado e íntegro para el manejo de las operaciones de las empresas (Alfaro, 2020). De modo tal que, la Norma ISO 27032 como estándar de ciberseguridad guarda ciertas similitudes con la normativa anterior, puesto que, la ISO 27032 se presenta como una serie de guías para la implementar el resguardo de la información de usuarios y en general, de los datos que pueden acarrear consecuencias importantes para las empresas con el fin de prever un margen para generar respuestas ante posibles ataques a los sistemas de seguridad informáticos.

Por otra parte, el cifrado de los datos corresponde a la apropiación de métodos criptográficos, cuyas funciones son fundamentales en los procesos de recolección e intercambio de datos que tienen lugar en las aplicaciones y plataformas de uso para gestionar las actividades de una organización (Pazmiño, 2021), de manera que, el sistema de cifrado hace parte del uso de la encriptación de la información en Internet, lo cual es útil en la prevención del robo de activos

informáticos efectuados por piratas informáticos materializados en ciberdelitos, así como para la prevención del espionaje, entre otras.

Asimismo, la criptografía vista como una herramienta técnica de gestión de la seguridad para los sistemas informáticos crea códigos de seguridad cuyo contenido no es comprensible, sino que solo es descifrado por el emisor y el receptor de dicho mensaje, ya que este cifrado se compone por complejos algoritmos matemáticos (Samaniego, 2018); de manera que este grupo de herramientas de cifrado se basan en la integridad, confidencialidad y disponibilidad de la información.

Con relación a la metodología de análisis y gestión de riesgos de las tecnologías de información MAGERIT, esta puede ser considerada como un conjunto de herramientas que apoyan a las empresas para la toma de decisiones basadas en el análisis y la gestión de riesgos para detectar las potenciales amenazas en a través de la identificación y posterior sistematización de los peligros (Gómez et al., 2019), además, esta metodología posibilita, también, crear o diseñar acciones o actividades destinadas a salvaguardar la información como una manera de prevenir los ataques.

Es posible considerar a MAGERIT como una técnica que, mediante el análisis de la esquematización de gráficos, diagramas de procesos, planificación de proyectos, análisis Delphi, entre otras técnicas generales articuladas con técnicas específicas de análisis de algoritmos matemáticos puede ayudar a evaluar los riesgos, las amenazas, estimar vulnerabilidades, entre otras (Alama, 2019). Por lo cual, esta metodología representa una técnica cuya aplicación a la gestión de la ciberseguridad de las empresas puede ser un paso inicial hacia la configuración de las estrategias de seguridad que debe implementase a partir del diagnóstico detallado y examinado que esta herramienta ofrece.

En cuanto a la Norma Técnica Colombiana ISO-31000:2011, para los sistemas de seguridad, esta normativa ayuda a las empresas a dirigir las acciones orientadas a gestionar el riesgo de manera efectiva en un contexto de trabajo para la mejora de las actividades que atañen a la planeación de las medidas de prevención ante riesgos. Dicha normativa permite tal acercamiento a partir de la valoración, tratamiento, monitoreo y seguimiento del riesgo; de modo que, los lineamientos que las empresas pueden seguir para trabajar bajo un marco colaborativo en la organización de los tratamientos de los riesgos tras su identificación están consignados y esquematizados de acuerdo con los mecanismos de operatividad para frenar los peligros del ciberespacio en términos de seguridad informática.

Asimismo, la ISO-31000 es clave para abordar las inseguridades de los componentes de los sistemas informáticos de forma estructurada; puesto que, la eficacia es un elemento indispensable para la trazabilidad de la gestión de riesgos en las empresas y organizaciones; en este sentido, la efectividad de tal gestión debe representar la conformación del contexto, así como la apreciación de los riesgos subyacentes de los elementos identificados en el entorno.

Por su parte, el Manual ITIL es funcional sobre la base de la disponibilidad e integridad de los ciclos de servicios de las estrategias para el diseño, la transición, la operación y el mejoramiento continuo de los servicios ofertados por las empresas (Martínez & Rodríguez, 2019); de modo que su relación con la gestión de riesgos se basa en el ofrecimiento de un sistema de seguridad para optimizar los procesos y mecanismo de comercialización en las empresa, lo cual, trae como consecuencias la prevención ante el manejo de datos de forma no autorizada entre otros delitos de ciberseguridad asociados a las actividades económicas de las organizaciones.

Es por ello que, ITIL ayuda en la gestión de los servicios tecnológicos, contribuyendo con la disminución de los peligros a los que se ven enfrentados los sistemas informáticos, siendo útil para el correcto manejo de la información (Zúñiga, 2021). No obstante, las buenas prácticas derivadas de la implementación de ITIL consolida las pautas para el logro de la seguridad informática, pero también para los logros a los que la empresa se acerca en cuanto a su estructura de funcionamiento teniendo en cuenta a los usuarios de acuerdo con la calidad y los procesos.

En adición a lo anterior, el Estándar Australiano AS/NZS 4360se basa en la Integridad y confiabilidad, de la información y los datos mediante la identificación, clasificación y valoración de los riesgos informáticos a los que una empresa puede verse expuesta. De este modo, el sistema conforma unas directrices ligadas a distintas aplicaciones dependiendo del contexto de la empresa u organización teniendo en consideración la importancia de contar con una estructura organizada en cuanto a la administración de riesgos.

Adicionalmente, el estándar presenta un ámbito de aplicación que hace parte de distintos contextos en los que se puede resaltar las funciones administrativas relacionadas con la reiteración de los procesos de toma de decisiones para la administración de la prevención del riesgo. De tal modo que, la determinación de los elementos que caracterizan y componen las normativas, estándares, técnicas y herramientas de gestión de la seguridad de los sistemas informáticos consideran los distintos requerimientos que las empresas tienen en cuanto a su accionar en el manejo de la confiabilidad, integridad, y disponibilidad de la información, así como su ajuste según sus contextos y necesidades (AS/NZS 4360, 1999).

Tabla 4 Autores de tesis relacionadas

Autores de tesis relacionadas

Autores	Título de la tesis	Lo que propone	Observación
Luis Carlos Remolina Becerra	DISEÑO DE UN MODELO DE SEGURIDAD INFORMÁTICA A UNA EMPRESA EN SU SISTEMA DE MONITOREO DEL ÁREA DE TECNOLOGÍA	Este proyecto de investigación identifica los riesgos a los que se encuentran sometidos los activos, y, los elementos de trabajo en el área de la seguridad informática, para efectuar la entrega de un modelo que cumpla con los principios básicos y requisitos mínimos para la protección adecuada de la información enfocados en el modelo normativo ISO/IEC27001:2013. De modo que, este proyecto plantea la creación de una política de seguridad sumado a un modelo de implementación, empleando la guía para la etapa de creación, comunicación, cumplimiento y excepciones. Además, se utilizó la metodología MAGERIT para establecer parámetros, ya que esta permite saber cuánto valor está en juego ayudando a protegerlo.	Este proyecto de investigación está bien estructurado, presenta unos objetivos claros lo que hace más fácil al analista entender este diseño que propone el autor, además la metodología es más adecuada para poder cumplir con todo lo propuesto.
Arlenys Carolina Nieves	DISEÑO DE UN SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN (SGSI)	Esta investigación sirve de guía para evaluar la integridad, confidencialidad y disponibilidad	Este proyecto de investigación como el autor lo indica busca servir de guía para que las

	BASADOS EN LA NORMA ISO/IEC 27001:2013	de los activos de información, a la vez que, analiza e implementar un sistema de gestión de seguridad de la información, el cual permite identificar las amenazas y las vulnerabilidades que darán lugar a la elaboración de un plan de tratamientos de mitigación de los riesgos. Para esto, se utilizan la norma ISO 27001:2013 y la metodología MAGERIT, la cual se divide en tres fases: planeación (análisis de situación y descripción de los procesos), preparación (análisis y evaluación de riesgos), capacitación y sensibilización (concientización de seguridad de sistemas y activos de información).	empresas lo tengan en cuenta a la de buscar proteger sus datos, ya que los orinienta a la hora de identificar las amenazas que pueden estar por sufrir en sus organizaciones, elaborando un plan adecuado que les beneficiara a mitigar los riegos existentes.
Ruby Esperanza Buitrago Giraldo	SISTEMAS DE GESTIÓN EN SEGURIDAD INFORMÁTICA SGSI EN UNIVERSIDADES PÚBLICAS DEL EJE CAFETERO – COLOMBIA	La pretensión de esta investigación se basa en conocer el estado actual de las universidades públicas del eje cafetero (Colombia) en cuanto a SGSI, en favor de indagar detalladamente sobre la aplicación de las normas internacionales que presiden la necesidad de contar con un adecuado SGIS en el	La investigación se centra en el estado actual de las universidades públicas del eje cafetero con especial énfasis en la seguridad de la información, de manera que, el trabajo consta del diseño de un sistema de gestión de seguridad informática con la finalidad de beneficiar al sector empresarial e términos de ciberseguridad. La

		ámbito nacional a partir de la norma ISO 27001 y metodologías probadas como MAGERIT. El eje central de la investigación consiste en el análisis de la experiencia organizacional de las universidades colombianas en lo que a seguridad informática respecta, así como la elaboración de conclusiones, que permitan efectuar comparaciones para finalmente contribuir con la generación de nuevo conocimiento.	metodología se basa en la utilización de la norma ISO 27001 y la metodología MAGERIT, siendo estas de gran utilidad a la hora de efectuar los análisis y comparaciones para la oportuna toma de decisiones.
Lina Patricia Mendoza Penagos	DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD INFORMÁTICA PARA LA EMPRESA GED (GESTION ESTRATEGIA Y DESARROLLO) DE LA CIUDAD DE BOGOTA	La investigación trata de diseñar un sistema de gestión de la información, tomando como referente la situación actual de la empresa GED para enumerar los riesgos y el impacto de la afectación de los mismos. El diseño del sistema fue realizado en el área de sistemas, ya que, los funcionarios denominados asesores y desarrolladores son conocedores del proceso de información a tratar en el sistema de presentación integral de la	Este proyecto de investigación va enfocado única y exclusivamente a una área en específico que es la de sistemas, con la ayuda de los funcionario de dicha área realizar un análisis e indagar el estado en el que se encuentran los sistemas de información manejados para el área de funcionamiento de los sistemas, con el fin de fortalecerla a partir del estudio previo utilizando como metodología la norma ISO 27001 y MAGERIT con la finalidad de alcanzar una alta efectividad en la toma de

		gestión institucional. La aplicación de la norma ISO 27001, junto con la aplicación de la metodología MAGERIT, permitió verificar los riesgos a los que la empresa estaría expuesta en cada proceso. De acuerdo con esto, la determinación y definición de las políticas y controles de seguridad se destinaron a tratar de disminuir los riesgos, y, a su vez, mejorar la seguridad en la empresa.	decisiones que contribuyan con mitigar el riesgo existente.
Martha Lucia Briñez Bautista	DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD INFORMÁTICA PARA LA ALCALDÍA MUNICIPAL DE LA JAGUA DE IBIRICO – CESAR BASADO EN LA NORMA ISO 27001:2013	La presente investigación consiste en la descripción de un diseño metodológico útil para implementar un SGSI que dé garantías del nivel de seguridad y permita obtener la certificación ISO/IEC 27001:2013. Para tal finalidad, se efectuó un análisis de para determinar la pertinencia de la información en cuanto a la veracidad. Tras la identificación de los activos encontrados en riesgo, cuyo impacto estimado fue alto, se procedió a definir las políticas de	La investigación se propuso diseñar un sistema de gestión de seguridad, para beneficiar la operatividad de los recursos dentro de una organización, que en este caso se trata de la alcaldía de la Jagua de Ibirico (Colombia) como organización de función pública. El autor busca que realizando este diseño se logre la certificación ISO, para eso utilizara esta norma como guía y analizando en profundidad el cómo se está manejando la información dentro de la alcaldía y así tomar las

	seguridad, así como la declaración y aplicabilidad de los controles para el uso de cada uno de estos activos considerando las directrices de la ISO/IEC 27001 en provecho de obtener una amplia perspectiva de los sistemas de información, con el consecuente diseño del análisis del riesgo mediado por MAGERIT.	mejores decisiones para con las metas trazabas. Utilizando como metodología MAGERIT para poder analizar los riesgos existentes.

En síntesis, los sistemas de gestión de la seguridad de la información son cada vez más necesarios para salvaguardar los activos de las organizaciones, en el siguiente análisis se detalla la investigación presentada en la tabla 4.

En la tabla 4 el autor Luis Carlos Remolina propone un diseño de un modelo de seguridad informática, en el cual, a través del análisis de su investigación, se pudo notar que éste optó por utilizar la norma ISO 27001, debido a que, dicha normativa ofrece los principios básicos de la integridad, confiabilidad, y disponibilidad de la información protegida en todo momento y garantizando su uso correcto por personal autorizado; asimismo, los requisitos mínimos ofrecidos por la normativa para la protección efectiva de la información, sigue las directrices de la protección de datos y la evaluación de las condiciones en las que se encuentran las organizaciones.

De modo que, la investigación consultada contempla la idea de requisitos mínimos y principios de la ISO 27001 para efectuar un mejor análisis de la situación actual de la empresa. Adicionalmente, la investigación hizo uso de la metodología MAGERIT, debido a que, las empresas a las que dicha investigación estuvo orientada de caracterizan por desempeñarse mediante información de forma digital y sistemas informáticos, siendo, entonces, esta metodología muy efectiva a la hora de saber qué información puede estar en riesgo dentro de la empresa, lo cual ayuda a que pueda se pueda gestionar adecuadamente la protección de la misma.

De acuerdo con esto, la combinación de estos métodos (ISO 27001 y MAGERIT) permite que las empresas que inicien con la gestión de seguridad de la informática tengan más claridad de la importancia de proteger sus datos, ya que su aplicación es sencilla, además ayuda a concientizar a los responsables de las organizaciones acerca de si la información que está manejado se encuentra en riesgo.

Por su parte, la investigación de Arlenys Carolina Nieves ofrece el diseño de un Sistema de Gestión de Seguridad de la Información (SGSI) a partir de la implementación de la norma ISO/IEC 27001:2013 para lo cual realizó un análisis de la normativa, lo cual permitió identificar y clasificar los activos de información como método a implementar derivado de tal análisis; asimismo, la normativa en esta investigación permitió realizar una valoración y tratamiento de los riesgos de seguridad de los activos de información.

A su vez, la investigación arrojó un cronograma para ejecutar capacitaciones respecto a la temática de la seguridad de la información, razón por la cual esta metodología fue usada teniendo como resultados la verificación de la situación real y actual de la oficina de Ingreso del Centro de Educación Técnica y Tecnológica del departamento del Cesar mediante la diagnosis inicial y comparativa final e inicial, pudiendo identificar las expectativas, las brechas y las posibles mejoras a efectuar de acuerdo con la norma.

De modo que, el seguimiento de la normativa ISO/IEC 27001:2013 brindó las pautas para la realización de las actividades de gestión y clasificación de los activos de información; la identificación y valoración de las amenazas; y el análisis del riesgo siendo estos importantes motivos para su implementación.

Similarmente, Ruby Esperanza Buitrago Giraldo en su investigación relacionada en la tabla 4 proyectó tal trabajo para ofrecer conocimientos acerca del estado de la gestión de la información que las universidades públicas de la zona de eje cafetero, en Colombia, presentan en cuanto a normas del ámbito nacional como del internacional; puesto que, se considera necesario que las organizaciones de cualquier índole gubernamental sean fortalecidas en cuanto a la identificación de las vulnerabilidades a través del análisis de metodologías como la Norma ISO 31000 de 2009, la Norma ISO 27001 de 2005 y la metodología MAGERIT en distintos contextos para hacer comparativas.

De modo que dichas normativas y metodologías fueron útiles para entender la experiencia organizacional de la gestión de la información que tiene lugar en las universidades, en donde los beneficios aportados por tales revisiones se basaron en la identificación y estudio de los potenciales riesgos y sus amenazas; así como las formas de garantizar la seguridad de las organizaciones educativas de la región a través de la disponibilidad de la información en favor de cumplir con los requerimientos legales de la protección de los datos y la seguridad informática, en general.

Sin embargo, la exploración de esta investigación permitió observar que las metodologías consolidadas para un SGSI hacen necesaria la revisión, ejecución y alcances de la seguridad de las entidades basados en metodologías y normativas como MAGERIT e ISO 27001:2005 y 31000 de 2009.

Por otra parte, la autora Lina Patricia Mendoza Penagos desarrolló un proyecto en el cual, el uso de la metodología MAGERIT permitió avanzar en el diseño de un sistema de gestión estratégico para la seguridad de la información destinado a la empresa GED (Gestión Estrategia y Desarrollo) detectando los riesgos a partir del diagnóstico del contexto actual de dicha empresa.

De manera que, la metodología permitió destacar las amenazas y el impacto de las mismas en cuanto a los controles de seguridad, siendo también útil la revisión y verificación de la norma ISO 27002 que de manera complementaria ofrece a la investigación las recomendaciones y las mejoras que la gestión de seguridad debe proveer en interés de la manutención de los sistemas de gestión a través de la confiabilidad de los datos y la disponibilidad para el acceso autorizado, así como la integridad en todos los procesos de uso.

A través de tales implementaciones, el trabajo logró la verificación de los controles de los sistemas de seguridad, y con ello, la disminución de los riesgos y la mejora de la

seguridad de la empresa en el uso de información en acuerdo con la correcta definición de las políticas de seguridad y control de la empresa. En otro sentido, la autora Martha Lucia Briñez Bautista (tabla 4) propone el diseño de un Sistema de Gestión de Seguridad Informática en la alcaldía de La Jagua de Ibirico a través de la aplicación de la Norma ISO 27001:2013, lo cual, accedió describir y descomponer las partes de la implementación de un Sistema de Gestión de Seguridad Informática en provecho de adquirir la certificación del estándar.

Los autores realizaron un análisis acerca de la veracidad de la información aportada por lo activos disponibles, no obstante, se identificó que existen algunos activos en riesgo con un alto impacto en la seguridad de la empresa. En este sentido, fue necesario realizar una revisión de las políticas de seguridad a fin de aplicar los controles necesarios. De acuerdo con esto, la metodología implementada basada en las directrices de la ISO/IEC 27001 y la metodología MAGERIT permitieron efectuar el diseño de un SGSI que buscó optimizar los procesos operacionales de conllevan a la obtención de la certificación ISO/IEC 27001:2013. Asimismo, las situaciones derivadas de la ejecución de esta investigación consistieron en considerar que las instrucciones subyacentes de las normativas tienen funciones de protección y prevención ante los peligros de la perdida de información proporcionando los controles de la seguridad de la empresa.

***Tabla** 5 Tecnologías Emergentes*

Tecnologías Emergentes	Lo que proponen	Observación
Blockchain o Cadena de bloques	Trabaja de manera eficiente y tiene la capacidad de manejar varias transacciones, funciona como un libro mayor que es administrada por una red de pares, es la implementación de tres tecnologías, Internet, criptografía y un protocolo basado en incentivos, los	Esta tecnología es una de la más importante en la actualidad, ya que establece condiciones para ejecutar una transacción de forma segura, además, las organizaciones pueden lograr importantes ventajas competitivas, ya que, cada

	registros se enlazan y se cifran protegiendo la seguridad de las transacciones, el ahorro en costos que tiene este tipo de sistemas permite que su uso se lo pueda realizar en: sistemas financieros, de salud, manufactura, logística, Gobierno, donaciones, identidad digital, contratos, productos culturales, seguros.	uno de sus participantes es dueño de la información, lo que ayuda a mantenerla de forma segura.
Analytics	Como herramienta digital para el análisis que a través del seguimiento a sitios *web, blogs*, redes sociales, entre otros permite tomar decisiones. De modo que la propuesta de esta herramienta consiste en ofrecer soluciones para la emisión de informes detallados a usuarios determinados de acuerdo con criterios que tienen en cuenta los procesos que están en función de la recolección y procesamiento de datos para la elaboración de informes.	La importancia de esta tecnología es que permite tomar decisiones de forma acertada, ya que con el análisis previo de la información contribuye a una mejor elección. Además, ayuda a las organizaciones tomar mejores decisiones para optimizar sus procesos, los que le da una ventaja competitiva contra las demás empresas.
Big Data	Es la capacidad de poder explotar y extraer grandes cantidades de datos e información, tiene la finalidad de diseñar nuevos productos y servicios, en función a las percepciones que los clientes tienen actualmente, competidores y el mercado. La propuesta del manejo de conjuntos de datos de gran tamaño se basa en la ventaja competitiva ofrecida por esta herramienta, debido que, en medio de la complejidad se favorece la toma de decisiones de acuerdo con la interpretación de la información organizada y estructurada mediante los datos, representando un adelanto ante la	Es una de las utilizas por las organizaciones, ya que les ayuda a aprovechar los datos de una manera más óptima y así tomar mejores decisiones en base a los datos que las mismas organizaciones manejan. Actualmente la *bigdata* ayuda a las organizaciones a identificar nuevas oportunidades y sacar un provecho competitivo contra las demás organizaciones.

	competencia, y, por ende, mejorando el rendimiento financiero de la compañía.	
Sistemas de inteligencia artificial	Es la combinación de algoritmos que permiten crear maquinas con capacidades similares a la de un humano, tecnología que poco a poco se está desarrollando, estos sistemas inteligentes son capaces de manejar grandes cantidades de información.	Esta tecnología a futuro puede ser una de más utilizadas, ya que puede pensar o simular a un humano lo que le da más capacidad de maniobra a las organizaciones que los están utilizando, ya que les ayuda a tomar mejores decisiones con el análisis previo.
Agentes de seguridad de acceso a la nube (CASB)	Es un punto de control que protege el acceso a los recursos informáticos que están en la nube. Por lo tanto, esto propone que, tales puntos son diseñados por los proveedores *cloud* como forma de garantizar el acceso exclusivo de los servicios ofrecidos a los usuarios.	La tecnología ofrecida por CASB concede a los profesionales de la seguridad informática los puntos de control crítico que pueden tener uso en la compatibilidad de los servicios en la nube mediante múltiples proveedores.

Como síntesis de las tecnologías emergentes están generando un impacto positivo dentro de las organizaciones, debido a que, dichas tecnologías proporcionan los medios propulsores para que las empresas tengan un rápido crecimiento en el mercado debido a la masificación de las propuestas comerciales dadas por la conectividad y las herramientas digitales que se ven implicas en el tratamiento de datos.

Además de las estrategias que se realizan en todos los niveles y que ayudan para que exista un balance en todos los sectores de la misma organización, actualmente las empresas pueden realizar alianzas con otras organizaciones, así como, compartir habilidades, tecnologías, y costos, que conllevan a generar ventajas competitivas que, a su vez, se manifiestan accediendo a herramientas de procesamiento de datos (Melchor et al., 2012), y,

produciendo información de valor para la empresa, lo cual, es un aspecto que mejora la toma de decisiones, así como también el rendimiento financiero de forma ascendente.

De manera general, las tecnologías emergentes han tomado un papel fundamental e imprescindible en el desarrollo estratégico de las organizaciones, puesto que, es necesario que tanto los directivos como el talento humano se preparen y fortalezcan sus conocimientos y habilidades en beneficio de estar a la vanguardia de las nuevas tendencias en innovaciones tecnológicas, debido a que, esto ayudara con el cumplimiento de los objetivos planteados dentro de las organizaciones de manera eficiente (González & García, 2010).

En la tabla 5 se nombra una serie de tecnologías emergentes como el *Big Data*, que es una de las utilizas por las organizaciones, puesto que, ésta les ayuda a aprovechar los datos de una manera óptima para la toma de decisiones con base a los datos que las mismas organizaciones manejan. Esto da cuenta de la efectividad que tiene *Big Data* para la prospección de las empresas, de modo que, la variedad, velocidad y volumen de la información de manejo siendo la complejidad un aspecto que las empresas pueden manejar a través de la implementación y adopción de esta herramienta (Cabas, 2021).

De manera similar, la Cadena de bloques (*Blockchain*)se presenta como un conjunto de registros electrónicos que, de manera progresiva aumenta de tamaño, además de la complejidad de la información debido al gran volumen que maneja se adiciona el hecho que tal tecnología hace uso del cifrado mediante la criptografía asegurando la integridad y confiabilidad de los datos (Figueroa et al., 2019).

De este modo, la disponibilidad de los mismos también es un aspecto clave que favorece el crecimiento de las empresas ya que esta plataforma se considera inalterable a pesar de la posibilidad e interactuar con los datos en tiempo real (Guachi, 2012). Por tal

razón, las empresas pueden hacer uso de una herramienta versátil en su uso que, a su vez, conserva la integridad, disponibilidad y confidencialidad de la información.

Asimismo, la tecnología de *Analytics* da seguimiento a los dominios web ampliamente utilizados en el ámbito global, siendo esto útil para las empresas puesto que esto les permite descubrir quienes siguen sus productos y servicios y de alguna forma estor representa el acercamiento a los datos de ocurrencia que reflejan el interés por adquirir las ofertas de dichas empresas (Aguado, 2018). De modo que, las empresas pueden explotar estos recursos en provecho de hacer crecer su competitividad aprovechando las oportunidades en el mercado y anticipándose a las necesidades que los usuarios presenten, teniendo a su vez, seguridad en que los datos no serán objeto de vulnerabilidades.

De forma singular, los sistemas de inteligencia artificial(IA) son un gran potencial de provecho para las empresas, en términos financieros y de seguridad informática, debido a que, los sistemas de IA reproducen la inteligencia humana para la reiteración de procesos y tareas dinamizadas por la información para el análisis crítico y exhaustivo de grandes conjuntos de datos, teniendo alguna relación con el *Big Data* (Rouhiainen, 2018); sin embargo, la IA puede ser trasgresora en cuanto a la imitación de las capacidades humanadas, pero a su vez, esto se constituye como un recurso o activo empresarial de alto valor. Por otro lado, y en concordancia con lo anterior, los agentes de seguridad de acceso a la nube (CASB) ofrecen una potente garantía de seguridad a la hora de acceder a la información posibilitando hacer frente a las amenazas a partir de la prevención de los peligros de perdida de información, y la protección de la identidad que subyace de los análisis de flujos de datos (Hernández, 2020).

4.3 Estructuración de los Componentes del Sistema de Gestión del Riesgo en Seguridad Informática Considerando las Mejores Prácticas de Gestión de TI, Mitigando con ello los Incidentes que Generan Impactos Negativos a Nivel Empresarial

Las buenas prácticas para la gestión de las Tecnologías de la Información TI hacen parte de la organización de las empresas en referencia a la consecución de los objetivos trazados que tienen relación con la seguridad informática y los mecanismos implementados para mitigar los impactos negativos en caso de que existan riesgos inminentes que representen la inseguridad, o inestabilidad de los sistemas informáticos (Pérez, 2021).

Es por esto que, la mitigación de los incidentes que generan impactos negativos en las empresas es un aspecto fundamental en todo proceso de gestión de la seguridad de sistemas informáticos, para lo cual, existen metodologías, herramientas, técnicas y tecnologías que han sido mencionadas y cuyos aportes ofrecen perspectivas diferentes y complementarais para diseñar un adecuado plan para al manejo de los posibles incidentes, y, asimismo, estimar su prevención (Ayala & López, 2019).

En un análisis de los resultados obtenidos anteriormente en la encuesta realizada, se seleccionó la Norma ISO 27001:2013, ya que esta establece los criterios de políticas de seguridad de la información y su organización, seguridad de los recursos humanos, controles de acceso y gestión de incidentes de seguridad de la información ya que estos están siendo afectados, de esta forma esta norma es la idónea para la realización del esquema de los componentes del sistema de gestión de riesgo en seguridad informática orientado al beneficio de operativo del servicio en empresas ubicadas en Ocaña Norte de Santander.

Puesto que, contribuye en la mitigación de los incidentes como parte de la gestión de la seguridad de los sistemas informáticos presentados a continuación corresponde a distintas fases que progresivamente conllevan al desarrollo de la estructuración de los componentes del sistema de gestión del riesgo considerando que los peligros relacionados con los datos pueden tener diversos orígenes, y, por ende, diferentes impactos. Es por ello que, a continuación, se presentan detalladamente los componentes del sistema de gestión de riesgo en la seguridad informática lo cual incluye las fases de desarrollo de acuerdo con el estándar ISO 27001:2013 para los Sistemas Gestión de la Seguridad de la Información ya que esta posibilita a las empresas evaluar los riesgos y aplicar los controles requeridos para la mitigación del impacto pudiendo ser, simultáneamente, eliminados.

4.3.1 Componentes del sistema de gestión del riesgo en seguridad informática

Resulta indispensable conocer acerca de los componentes del sistema de gestión del riesgo informático en apoyo de la norma ISO 27001:2013, puesto que, esta normativa es ampliamente utilizadas por las organizaciones con relación a la protección de los datos e información.

La norma NTC- ISO 27001:2013 hace hincapié en que un SGSI debe estar formado por los siguientes pliegos:

- Alcance del SGSI: Corresponde al ámbito de la organización que queda sometido al SGSI, incluyendo una identificación clara de las dependencias, relaciones y límites que existen entre el alcance y aquellas partes que no hayan sido considerados.

- Política y objetivos de seguridad: Documento de contenido genérico que establece el Compromiso de la Alta Dirección y el enfoque de la organización en la gestión de la seguridad de la información.

- Estándares, Procedimientos, y Guías que soportan el SGSI: Consiste en los documentos y mecanismos que regulan el propio funcionamiento del SGSI para la medida de la eficacia de los controles implantados.

- Metodología de Evaluación de riesgos: Es una descripción de la metodología a emplear acerca de cómo se ejecutará la evaluación de las amenazas, vulnerabilidades, y las probabilidades de ocurrencia de los incidentes con relación a los activos de información contenidos dentro del alcance selecto; el tratamiento y desarrollo de criterios de aceptación de riesgo; y la fijación de niveles de riesgo aceptables.

- Informe de evaluación de riesgos: Estudio resultante de aplicar la metodología de evaluación anteriormente mencionada a los activos de información de la organización.

- Plan de tratamiento de riesgos: Documento que identifica las acciones de la Alta Dirección, los recursos, las responsabilidades y las prioridades para gestionar los riesgos de seguridad de la información, en función de las conclusiones obtenidas de la evaluación de riesgos, de los objetivos de control identificados, de los recursos disponibles, entre otros.

- Registros: Documentos que proporcionan evidencias de la conformidad con los requisitos y del funcionamiento eficaz del SGSI.

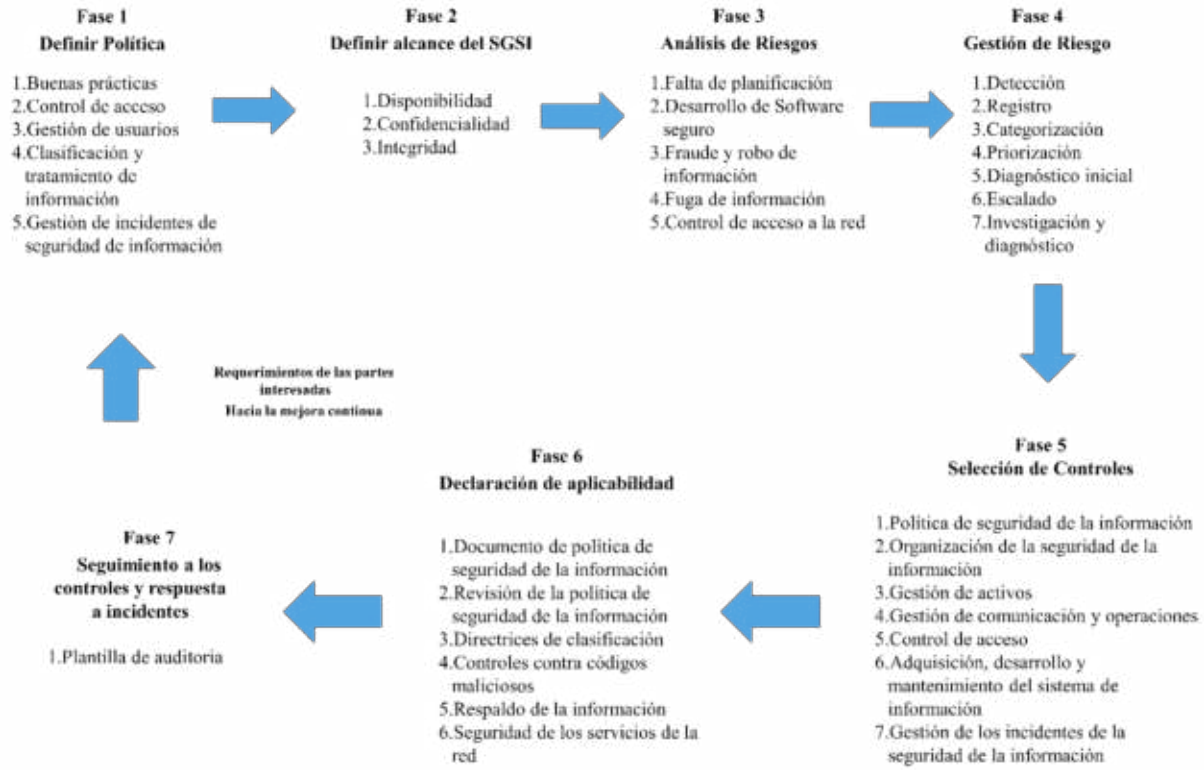
- Declaración de aplicabilidad: Documento que contiene los objetivos de control y los controles contemplados por el SGSI, en este se presentan las exclusiones y la evidencia de cumplimiento.

No obstante, debido a la amplitud del ámbito de aplicación de los componentes del SGSI de la Norma NTC- ISO 27001:2013 para las empresas, se ha realizado una adaptación de acuerdo con los pliegos referidos al desarrollo de 7 fases que se proponen a continuación como resultado de la estructuración de los componentes del sistema de gestión del riesgo en seguridad informática en concordancia con las mejores prácticas de gestión de TI en beneficio de las empresas de Ocaña-Norte de Santander.

4.3.2 Sistema de gestión del riesgo de seguridad informática para beneficiar la operación del servicio en empresas ubicadas en Ocaña norte de Santander.

Con base en la NTC- ISO 27001:2013 se presenta el sistema para que las empresas puedan tomar medidas en su preparación hacia la atención y gestión de los incidentes referentes a la seguridad informática.

Figura 16 Fases para el desarrollo de la gestión de seguridad en sistemas informáticos
Fases para el desarrollo de la gestión de seguridad en sistemas informáticos



Fuente: *Elaboración propia*

4.3.2.1 Fase 1Definir la Política

Las siguientes políticas son generalizadas y pueden ser aplicables a todo tipo de organización, independientemente de su tipo, tamaño o área de actividad, teniendo en cuenta que las investigaciones realizadas son pertinentes para su uso en cualquier entidad para ayudar a mantener la confidencialidad, integridad y disponibilidad (Guachi, 2012).

Asimismo, la gestión de la seguridad de los sistemas informáticos debe ser protegidos evitando toda pérdida de datos pertenecientes a la misma en virtud de mantener la confiabilidad de los datos, la integridad y la disponibilidad (Guamán, 2014). Es necesario entonces, que todo personal adscrito a la empresa sea conocedor del marco normativo que significa la utilización y administración de la información en los diferentes niveles a continuación descritos:

I. **Buenas prácticas:** Se recomiendan manuales que oriente a los usuarios para seguir unas directrices de buenas prácticas dentro y fuera de la organización (Sánchez & Chinchilla, 2020).

II. **Control de acceso:** Se establecen medidas para controlar el acceso a la información (Guano, 2013).

a. Los empleados deben tener un identificador que les permita ingresar a las zonas que requieren de autorización para acceder a dicha información.

b. No permitir que personas ajenas a la organización ingresen sin una previa autorización firmada por el encargado de dicha área.

III. **Gestión de usuarios:** Se establecen medidas para asegurar el acceso a usuarios autorizados y evitar el acceso de usuarios no autorizados a los sistemas de información (Martín, 2021).

a. Cada empleado de la organización con su identificador único, tiene que dejar un registro de las actividades que realice en el área de trabajo asignado.

b. Los empleados tendrán un usuario y contraseña suministrada por el encargado de dicha área, estas credenciales no pueden ser reveladas a personas ajenas a la organización.

IV. **Clasificación y tratamiento de información:** Toda la información manejada por la organización tiene que estar asegurada, y que esta reciba el nivel de protección adecuada (Martínez et al., 2021).

a. La información solo puede ser accedida a los usuarios que estén previamente autorizados y dejar un registro de la fecha que fue consultada.

b. El esquema de clasificación de la información deberá estar diseñado por los encargados del área responsable, en función de los niveles de clasificación determinados por las directrices del control. Estos se refieren a que la información será categorizada según su valor, los requerimientos legales, y la importancia para la empresa.

c. La información será etiquetada y manejada por los miembros de la seguridad informática de la empresa en atención al adecuado tratamiento de la misma.

V. **Gestión de incidentes de seguridad de la información:** Todos los eventos deben ser monitoreados y reportados para mejorar la capacidad de respuesta, y de esta manera, evitar que la operación del servicio se vea comprometida (Mendoza, 2017).

a. Todos los empleados tienen que reportar cualquier incidente de seguridad informática que se presente a la menor brevedad.

b. Crear reportes de las actividades realizadas e informar de las debilidades que estas pueden presentar con respecto a la seguridad.

Tabla 6 Plantilla de políticas específicas

Plantilla de políticas específicas

Políticas de gestión del riesgo de seguridad informática para las empresas de Ocaña-Norte de Santander

Concepto	Definición	Responsables
Cifrado de la información	Hacer efectiva la revisión del correcto funcionamiento de los algoritmos para la encriptación de los datos de la empresa.	Dependencia u oficina de IT y Seguridad
Uso aceptable de equipos	Los equipos destinados como soporte para el almacenamiento y trato de los activos informáticos deben tener uso exclusivo para tales fines evitando actividades de entretenimiento, y otras asociadas al uso de plataformas que pueden ser vehículos para virus informáticos u otras vulnerabilidades con el fin de cuidar los recursos de la empresa.	Administrativos y colaboradores en general.
Pautas para el uso de antivirus	Configurar el filtrado y la instalación de programas que detecten amenazas a través de códigos ejecutables en el sistema informático de la empresa.	Dependencia u oficina de IT y Seguridad
Correo electrónico automático	Hacer uso de un servidor exclusivo para el envío de correos programados como medio de difusión de información. Se resalta el uso del servidor de correo electrónico para uso exclusivamente de las actividades comerciales de la empresa.	Recursos físicos y soporte técnico, colaboradores, administrativos, entre otros.
Medios tecnológicos para las telecomunicaciones	El uso de computadores, celulares y *tablets* de la empresa, así como los respectivos accesorios están disponibles únicamente para el desempeño de las actividades laborales correspondientes a la empresa.	Todo el personal de la empresa
Conectividad y navegación	Las redes de navegación y conectividad a Internet de la empresa son expresas de acuerdo con las necesidades de cada colaborador y ente administrativo, para lo cual, los equipos tecnológicos cuentan con la capacidad de navegación requerida.	Recursos físicos y soporte técnico
Respuesta ante la violación	Se establece que la privacidad de los datos hace parte de las garantías de la empresa hacia los usuarios, por lo cual, ante un inminente acceso no autorizado para el uso de la información se procede notificar a las autoridades sobre el incidente dentro de un	Director de seguridad de

de datos	lapso igual o menor a las 72 horas siguientes al acontecimiento considerando lo promulgado por la Ley 1266 de 2008, la Ley 1581 de 2012, y el Decreto 1377 de 2013.	la información

4.3.2.2 Fase 2 Definir el Alcance del SGSI

Los sistemas de seguridad informáticos ostentados por las empresas de Ocaña-Norte de Santander, presentan características alusivas a los procesos organizacionales en conformidad con los riesgos y exposición de la seguridad informática que se derivan de la identificación del contexto a partir de las amenazas, oportunidades, debilidades y fortalezas, lo cual, permite reconocer que el alcance de las organizaciones está ligado a los requerimientos de sus colaboradores en cuanto al desempeño de las actividades de gestión del riesgo (Caro, 2011).

Por lo cual, el alcance de este sistema pretende conseguir que la implementación de este sistema de seguridad informática, mantenga la integridad de los datos y de los sistemas informáticos, así como, la disponibilidad de estos, cuidando la privacidad y manteniendo el control operativo; de tal suerte que sea posible lograr una mayor integración entre el usuario y el sistema, y a su vez, mitigando las vulnerabilidades y los riesgos asociados.

En este sentido, los objetivos de alcance se centran en torno a sensibilizar a los colaboradores, directivos y usuarios, en relación a la importancia de proteger los activos de cada una de las organizaciones mediante el resguardo de las condiciones de disponibilidad, confidencialidad e integridad (MINTIC, 2016):

I. **Disponibilidad:** Consiste en la cualidad para que la información sea accesible y aprovechablea causa de una solicitud por parte de alguna entidad autorizada.

II. **Confidencialidad:** Atributo que determina si la información se encuentra disponible, a la vez que vela para que ésta no sea descubierta por usuarios, entidades o procesos no autorizados.

III. **Integridad:** Se refiere a las acciones de salvaguardar la exactitud y estado completo de los activos informáticos.

4.3.2.3 Fase 3 Análisis de Riesgos

El análisis de riesgos para la correcta gestión de la seguridad de los sistemas informáticos en las empresas tiene como fundamento la identificación de las amenazas propias del entorno y las vulnerabilidades intrínsecas a las que se encuentran expuestos dichos sistemas, posibilitando, entonces, la formulación de un registro de riesgos con sus respectivas respuestas para aceptar, mitigar o evitar (Chinchilla & Allende, 2017). Los activos de información también son recursos a proteger, para lo cual, es necesario implementar la evaluación del impacto del riesgo sobre tales activos (Claro & Espinel, 2019).

De este modo, Cuellar (2020) considera que, la fase de análisis de riesgos de seguridad informática en las empresas de Ocaña-Norte de Santander se reporta en la tabla 7, en donde se registran los principales riesgos adheridos al contexto de las tecnologías de la información y las comunicaciones. En este sentido, el conocimiento de los activos manejados por las empresas a través de sus responsables otorga la información necesaria para anticiparse a las potenciales amenazas.

Tabla 7 Registro de riesgos

Registro de vulnerabilidades

Vulnerabilidades	Consecuencia	Categoría	Probabilidad	Impacto	Prioridad	Respuesta (mitigación)		Persona Responsable
						Estrategia	Acción	
Falta de planificación de continuidad de negocio	q	o	A	A	A	E	Contar estrictamente con una planificación dentro del negocio.	O
Falta de un software seguro	s	t	A	A	A	M	Realizar chequeos periódicos al software para mantenerlo actualizado	T
Escaso control de acceso a la red	c	o	B	B	B	E	Actualizar las tecnologías de control de acceso a la red y cumplir las políticas para el uso de la conectividad y navegación	T, O
Ausencia de procesos de gestión de incidentes de seguridad	c	t	A	A	A	E	Implementar mejoras en los sistemas de gestión para evitar incidentes de seguridad.	D
Falta de información y concienciación	q	o	M	M	M	M	Potenciar la formación y concienciación en materia de seguridad	O, T
Existencia de vulnerabilidad web	c	d	M	M	M	E	Hacer uso adecuado de los medios y herramientas tecnológicas de acuerdo con las políticas y promover concientización en los empleados de la organización	O, T
Deficiente control de	s	e	M	B	B	M	Efectuar mejoras para el acceso de la	O, T

acceso							información a los empleados	
Insuficiente mantenimiento periódico en los servidores de bases de datos	**s**	**t**	**M**	**A**	**A**	**E**	Actualización periódica de las bases de datos	**T, D, O**
Escaso apoyo y seguimiento a los incidentes de seguridad informática de las empresas	**t**	**e**	**M**	**A**	**M**	**M**	Establecer redes de interacción colaborativa	**E**
Escasa disponibilidad de personal de gestión de riesgos informáticos vinculados a las empresas	**q**	**d**	**M**	**A**	**A**	**E**	Promover la contratación de talento humano para la gestión de la seguridad informática	**D**

Notas:

***Consecuencia*: t**iempo, **c**osto, calidad (**q**), **s**eguridad

***Categoría*: t**écnico, **e**xterno, **d**irección de proyectos, **o**rganizacional

***Probabilidad* e *Impacto*: A**lto, **M**edio, **B**ajo

***Prioridad*: A**lta, **M**edia, **B**aja

Impacto: Alta, **M**edia, **B**aja

***Estrategia*: A**ceptar, **M**itigar, **T**ransferir, **E**vitar

***Acción*:** Qué se realizará para implementar la estrategia

Fuente: Adaptado de Oficina de proyectos de informática

Tabla 8 Registro de riesgos

Análisis de riesgos

Matriz de análisis de riesgos

Elementos de información.	Magnitud de riesgo.	Probabilidad de Amenaza					
		Criminalidad		Sucesos Físicos		Negligencia	
		Robo	Virus	Falla de corriente	Incendios	Compartir códigos de acceso	No cifrado de datos críticos
Información y Datos							
Fuga de información	4	6	9	9	8	12	9
Existencia de cambios regulatorios	3	16	8	6	6	9	6
R.R.H.H	2	9	12	6	12	16	9
Finanzas	4	12	16	9	12	16	12
Sistemas de información							
Fraude y robo de información	3	16	12	9	8	8	6
Computadores y Portátiles	3	9	16	8	16	16	9
Personal							
Personal Técnico	3	12	9	6	9	12	16
Coordinadores y Supervisores	4	9	8	9	8	9	12
Uso inadecuado de las herramientas tecnológicas	4	6	16	12	6	12	9

- **Bajo Riesgo** = 1 – 6 (verde) **Medio Riesgo** = 8 – 9 (amarillo) **Alto Riesgo** = 12 – 16 (rojo)

4.3.2.4 Fase 4 Gestión del Riesgo

La gestión del riesgo se desarrolla bajo las acciones de garantizar el funcionamiento y el buen servicio de las operaciones de las organizaciones, para lo cual, se plantean estrategias que resuelvan cada uno de los riesgos que se pueden presentar, siendo estos mitigados, sin comprometer todo el servicio (Fernández, 2019).

Según Fonseca, (2019), los incidentes pueden ser provocados por algunos de los siguientes elementos:

Error de software o error de hardware

Errores del servicio en cuanto a la operacionalización

Peticiones de servicios (usuarios)

Pedidos.

Consultas.

Por consiguiente, las principales actividades de la Gestión de Incidencias destinadas a generar una buena respuesta acerca del manejo del servicio de la operación, se pueden orientar mediante los siguientes ítems:

Detección: Si la incidencia es detectada a tiempo el impacto de ésta será menor frente al negocio de dicha empresa u organización; es por eso que se debe estar vigilando cada uno de los recursos de la empresa, para así detectar dichas incidencias potenciales y estabilizar el servicio antes de que pueda generar un impacto negativo en todas las actividades del negocio (Pazmiño, 2021).

Registro: Las incidencias del servicio presentadas en la empresa deben ser registradas, y cada una de éstas debe registrarse de manera independiente (Zúñiga, 2021).

Por otra parte, Mayanquer, (2020), expone que, al momento de registrar la información se deberá incluir lo siguiente:

Identificador exclusivo

Clasificación

Exigencia, impacto y prioridad

Fecha y hora

Persona o grupo que reporta la incidencia.

Canal de entrada

Datos del usuario

Sintomatologías

Etapa

CIs asociados (*Configuration Items*, elementos de configuración)

Persona o grupo asignado para la resolución

Problema/*Known* error asociado

Actividades realizadas para la solución

Fecha y hora de la resolución

Categoría del cierre

Fecha y hora de cierre

Categorización.

En este proceso se busca establecer de manera exacta el tipo de incidencia ocurrido en la empresa, lo cual, se establece mediante una caracterización en múltiples niveles con dependencias entre sí, en donde el número de niveles requerirá de la granularidad en la que se necesite organizar los episodios presentados (Inerarity, 2018).

Priorización: En esta actividad, se visualiza la prioridad de la incidencia para mostrar cómo se ha de gestionar. La prioridad de la incidencia depende de:

La urgencia o rapidez con que la incidencia precisa ser resuelta (Suárez, 2015).

El impacto determinado por el número de usuarios afectados, aunque lo realmente importante es la criticidad para el negocio de los usuarios afectados por la incidencia (Giraldo & Pacheco, 2018).

Diagnóstico inicial: En este proceso se considera que el personal de soporte de primer nivel recibe un reporte de incidente, estos la valoran en base a los síntomas, y, si el personal está apto para dicha incidencia, la resuelve (Peñuela, 2018).

Escalado: Existen dos tipos de escalado, tal como el funcional acerca de si el soporte de primer nivel no está capacitado para resolver la incidencia, la asignan inmediatamente al grupo resolutor correspondiente; y, el jerárquico en caso de que se den ciertas circunstancias (incidencias graves o críticas, riesgo de incumplimiento del SLA) que se deban notificar a los responsables del servicio correspondiente (Pereyra, 2021).

Investigación y diagnóstico: Esta actividad hace referencia cuando la incidencia falla en el sistema, lo más sensato es que se necesite investigar más a fondo la causa del fallo.

Para Pérez, (2021), las tareas más comunes dentro de esta actividad son las siguientes:

Establecer el funcionamiento correcto y la secuencia de acciones del usuario (casuística).

Establecer potencial impacto de la incidencia.

Determinar si el riesgo es consecuencia de un cambio.

Realizar la búsqueda de bases de datos de conocimiento acerca del registro de incidencias y sus posibles soluciones y/o *work arounds*, cuyo término se refiere a una alternativa cuando las soluciones tradicionales no son suficientes o efectivas en la superación de inconvenientes de programación de hardware, software, entre otros, siendo esta solución más completa con respecto a la convencionalmente propuesta ante el error encontrado.

Resolución: Se refiere a la detección de una solución potencial, está se deberá aplicar y testear. Una vez comprobada la resolución, la incidencia se da por resuelta y se asigna al equipo de *Service Desk* para su cierre. Asimismo, es necesario registrar todas las acciones realizadas para resolver la incidencia en el historial de la misma (Cotrina, 2020).

Cierre: Previo al cierre de todo acontecimiento, el equipo del *Service Desk*debe validar algunos puntos, según lo expuesto por Izaguirre & León, (2018):

La satisfacción del usuario con la resolución de la incidencia

La categorización del cierre

El cumplimiento de todos los datos necesarios.

4.3.2.5 Fase 5 Selección de controles a implementar

Esta fase tuvo lugar bajo la revisión de la Norma ISO 270001, para la selección de los siguientes controles que pueden ser aplicables de forma general en las organizaciones que se encuentran en el municipio de Ocaña-Norte de Santander.

En atención a ello la tabla 8 plantea los controles que las empresas deben tener en favor de implementar las políticas de seguridad de la información al interior de su organización. Por lo cual, la Política de seguridad de la información pretende dar lineamientos acerca del correcto despliegue de las actividades de las empresas para proteger la información de contenido crítico para el funcionamiento de la entidad y la autenticidad de los registros relacionados con los usuarios, siendo importante tal política para indicar a la estructura organizacional de la empresa la finalidad del SGSI.

Tabla 9 Controles para la Política de Seguridad de la Información

Controles para la Política de Seguridad de la Información

Política de seguridad de la información	
Documento de política de seguridad de la información	La dirección como parte principal de la empresa debe aprobar un documento de política de seguridad de la información y este a su vez, hacer la respectiva publicación para comunicarlo a todos los empleados y partes externas pertinentes.
Revisión de la política de seguridad de la información	Esta política debe estar en constante verificación a partir de los intervalos planificados junto con los cambios significativos presentes en la empresa, para el aseguramiento de su idoneidad, suficiencia y eficacia.
Organización de la seguridad de la información	
Partes internas: Acuerdos sobre la confidencialidad	Es necesario el reconocimiento y valoración de los requisitos de confidencialidad o los convenios de no-divulgación que reflejan las necesidades de la organización para la protección de la información.

Partes externas: Identificación de los riesgos con las partes externas	Los agentes externos a las empresas deben tener conocimiento sobre cada uno de los riesgos de la información y los servicios de procesamiento de información de la organización de los procesos del negocio que involucran partes externas e implementar los controles apropiados antes de autorizar el acceso.
Gestión de activos	
Directrices de clasificación	Requiere que la información sea clasificada de acuerdo con los términos de su valor, así como de los requisitos legales, la sensibilidad y la importancia para la organización.
Gestión de comunicación y operaciones	
Controles contra códigos maliciosos	Hace necesario la implementación de los controles de descubrimiento, prevención y recobro para proteger la información de códigos maliciosos, así como los procedimientos pertinentes para la capacitación de los usuarios.
Respaldo de la información	Es necesario replicar el respaldo de la información y del software, poniéndose a prueba con regularidad de acuerdo con la política de cada empresa.
Seguridad de los servicios de la red	En cualquier acuerdo sobre los servicios de la red se deben identificar e incluir las características de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de la red, sin importar si los servicios se prestan en la organización o se contratan externamente.
Control de acceso	
Registro de usuarios	Debe existir un procedimiento formal para el registro y cancelación de usuarios con el fin de conceder y revocar el acceso a todos los sistemas y servicios de información.
Uso de contraseñas	Se debe exigir a los usuarios el cumplimiento de buenas prácticas de seguridad en la selección y el

	uso de las contraseñas.
Identificación y autentificación de usuarios	Todos los usuarios deben tener un identificador único (ID del usuario) únicamente para su uso personal, y se debe elegir una técnica apropiada de autenticación para comprobar la identidad declarada de un usuario.
Restricción de acceso a la información	Se debe restringir el acceso a la información y a las funciones del sistema de aplicación por parte de los usuarios y del personal de soporte, de acuerdo con la política definida de control de acceso.
Adquisición, desarrollo y mantenimiento de sistema de información	
Integridad del mensaje	Se deben identificar los requisitos para asegurar la autenticidad y proteger la integridad del mensaje en las aplicaciones, así como identificar e implementar los controles adecuados.
Política sobre el uso de controles criptográficos	Se debe desplegar y realizar un manejo sobre el uso de controles criptográficos para la protección de la información.
Control del software operativo	Aplicación de procedimientos para inspeccionar la instalación de software en sistemas operativos.
Gestión de los incidentes de la seguridad de la información	
Reporte sobre las debilidades de la información	Se debe exigir a todos los empleados, contratistas y usuarios de terceras partes de los sistemas y servicios de información que observen y reporten todas las debilidades observadas o sospechadas en los sistemas o servicios.

Asimismo, la Organización de la Seguridad de la Información contemplada bajo la ISO 27001:2013, está destinada a instaurar un referente para la gestión de dicha seguridad con el fin de iniciar y controlar la implementación de la seguridad de acuerdo con los roles y funciones de la organización y su personal, es decir que se considera la organización estructural de la empresa.

En cuanto a la gestión de activos (tabla 9) la normativa ISO-27001 permite a las empresas el acercamiento a la gestión de la seguridad mediante la cuantificación y categorización de los activos proponiendo inventarios de los recursos informáticos dentro del alcance de los SGSI.

Por otro lado, la Gestión de Comunicación y Operaciones se basa en los objetivos de control para que las empresas puedan verificar el cumplimiento de acuerdos, a la vez que, se puede gestionar cambios necesarios para cumplir con los requerimientos operativos. Asimismo, el Control de Acceso puede ser gestionado por las empresas mediante la imposición de límites para el acceso a la información y los soportes de tratamiento y almacenamiento de la información, siendo este punto importante para las compañías que pretendan adquirir la certificación ISO 27001.

De modo que, lo anteriormente consignado también contempla la Adquisición, desarrollo y mantenimiento de sistema de información que considerando la normativa hace referencia a que las empresas pueden generar garantías sobre la seguridad de la información, ya que esta hace parte del ciclo de funcionamiento de los sistemas informáticos. Asimismo, la Gestión de los incidentes de la seguridad de la información reportado en la Tabla 9 da cuenta de la importancia de la identificación de las amenazas informáticas a través de acciones que pueden ser efectuadas por colaboradores en general.

4.3.2.6 Fase 6 Declaración de aplicabilidad

La declaración de la aplicabilidad se constituye como un ítem que puede ser usado por las empresas como parte de la gestión de la seguridad; asimismo, la Política y la Organización de la

seguridad de la información contienen controles para el manejo de los riesgos pudiendo ser adaptado de acuerdo con las condiciones de cada organización (Fernández, 2021).

De manera que, a continuación, se presentan los componentes que pueden ser aplicados por el sector empresarial para el tratado de la seguridad informática, en el que además se contemplan la Gestión de activos, y la Gestión de comunicación y operaciones aunado a otros aspectos en mención en la tabla 10.

Tabla 10 Aplicabilidad de los Sistemas de Gestión de la Seguridad Informática

Aplicabilidad de los Sistemas de Gestión de la Seguridad Informática

DECLARACION DE APLICABILIDAD SGSI					
No.	**Nombre**	**Descripción**	**Exclusión (Si / no)**	**Control implementado**	**Controles a implementar**
1	**Política de seguridad de la información**				
1.1	Documento de política de seguridad de la información	Se debe definir con conjunto de políticas para la seguridad de la información, aprobada por la dirección.	No	Política de seguridad de la información.	Actualizar la política de acuerdo a NTC-ISO/IEC COLOMBIANA 27001
1.2	Revisión de la política de seguridad de la información	Las políticas de seguridad tienen que ser revisadas en intervalos de tiempo planificados, para asegurar se eficacia.	No	Política de seguridad de la información.	Actualizar la política de acuerdo a NTC-ISO/IEC COLOMBIANA 27001
2	**Organización de la seguridad de la información**				
2.1	Acuerdos sobre la confidencialidad	Examinar con regularidad los acuerdos de confidencialidad.	No	Organización interna.	Manejar los activos de control
2.2	Identificación de los	Conocer de	No	Organización	Actualización de

	riesgos con las partes externas	primera los riesgos que están expuesto la información y los servicios.		interna.	la información correspondiente a los usuarios
3	**Gestión de activos**				
3.1	Directrices de clasificación	La información se debe clasificar en términos de su importancia, además de los requisitos legales y de lo importante que es para la organización.	No	Clasificación de la información.	Implementación de política salvaguarda de la información
4	**Gestión de comunicación y operaciones**				
4.1	Controles contra códigos maliciosos	Implementar controles contra códigos maliciosos para la detección y prevención.	No	Protección contra códigos maliciosos y móviles	Antivirus
4.2	Respaldo de la información	Realizar copias de seguridad para respaldar toda la información.	No	Copias de seguridad	Protección contra códigos maliciosos y móviles
4.3	Seguridad de los servicios de la red	Identificar e incluir las características de seguridad. Los niveles de servicio	No	Gestión de la seguridad de las redes	Se protege mediante contraseñas y claves de cifrado, y se controla a través de procedimientos de misión formal se

					mantiene de modo personal para cada usuario.
5	**Control de acceso**				
5.1	Registro de usuarios	Se debe implementar registros y cancelación de usuarios para tener el control a la hora de acceder a los sistemas de información.	No	Requisito del negocio para el control de acceso	Registro de datos personales
5.2	Uso de contraseñas	Se debe exigirles a los usuarios buenas prácticas a la hora de implementar contraseñas. .	No	Responsabilidades de los usuarios. Políticas de seguridad de la información.	Personalizadas y con un nivel de fortaleza apropiado. (“Criptografía – Cifrado y gestión de claves").
5.3	Identificación y autentificación de usuarios	Implementar métodos que estén a la vanguardia de la seguridad para controlar el acceso a los usuarios remotos.	No	Control de acceso a las redes	ID personal
5.4	Restricción de acceso a la información	El acceso a la información y a las funciones de los sistemas de estar restringido de acuerdo a la política de	No	Compromiso del funcionario con las políticas de seguridad de la información.	Políticas de seguridad de la información.

		seguridad.			
6	**Adquisición, desarrollo y mantenimiento de sistema de información**				
6.1	Integridad del mensaje	Desarrollar formas seguras de proteger la autenticidad y la integridad del mensaje.	No	Adquisición, desarrollo y mantenimiento de sistema de información.	Implementar controles que estén alineados a las prioridades.
6.2	Política sobre el uso de controles criptográficos	Desarrollar e implementar una política sobre el uso de los controles criptográficos para salvaguarda la información.	No	Adquisición, desarrollo y mantenimiento de sistema de información	Realizar política que incluya controles criptográficos contemplando gestión de riesgos y marco normativo.
6.3	Control del software operativo	Implementar controles para evitar la instalación de software en los sistemas operativos.	No	Seguridad de los archivos del sistema	Medición y monitoreo de la seguridad de los controles.
7	**Gestión de los incidentes de la seguridad de la información**				
7.1	Reporte sobre las debilidades de la información	Exigirle a todos los involucrados dentro de la organización reportar cualquier debilidad presente en los sistemas.	No	Reporte sobre los eventos y las debilidades de la seguridad de la información	Plan y procedimientos de gestión de incidentes de seguridad de la información

De acuerdo con la ISO 27001:2013 el Control de acceso en la Declaración de aplicabilidad posibilita que las empresas concedan a los usuarios derechos de acceso a la información restringiendo, a su vez, el acceso no autorizado a agentes ajenos al proceso de tratabilidad de información. Por otra parte, la Gestión de los incidentes de la seguridad de la información tiene en consideración a los responsables de reportar las debilidades en el ámbito de la seguridad, permitiendo a las empresas elaborar planes para el tratamiento de incidentes que afecten a la seguridad de la información (Martínez & Rodríguez, 2019). En concordancia con lo anterior, la Declaración de aplicabilidad bajo la perspectiva ISO 27001:2013 presenta los ámbitos de aplicación de acuerdo con los criterios de exclusión y de implementación.

4.3.2.7 Fase 7 Revisión del Sistema: Seguimientos a los controles y Respuestas a incidentes

La última fase de este sistema contempla la revisión de este como una acción de gestión a implementar por parte de la dirección (o administración) que, a su vez, hace parte de los requisitos de la Norma ISO 27001:2013 denominado “Revisión de la Gestión”. De esta manera, la tabla 10 corresponde a la Plantilla de Auditoria, entendida como el formato para la revisión del sistema de acuerdo con el cumplimiento de los puntos tratados.

En cuanto a esto, la revisión del sistema refleja las buenas prácticas de seguridad que las empresas tienen, pudiendo esta acción ser vista como la garantía de que los objetivos del SGSI son oportunos, eficientes y pertinentes, ya que a través de la revisión se corrobora la validez de los incidentes detectados como peligros para la empresa (Meraz-Espinoza, 2018). Por otra parte, el seguimiento a los controles tiene como eje central la salvaguardar la confidencialidad de los datos, la integridad y la disponibilidad; haciendo que las respuestas ante los incidentes puedan

ser ejecutados de manera eficiente y rápida por parte de las empresas, por lo cual se presenta la tabla 11 con los componentes para la auditoría, la cual se puede considerar a la hora de realizar el arbitraje de los SGSI.

Tabla 11 Plantilla de Auditoria de las empresas en Ocaña-Norte de Santander

Plantilla de Auditoria de las empresas en Ocaña-Norte de Santander

Plantilla de Auditoria	
Fecha de la auditoria: Día / Mes /Año	**Responsables:** Oficina de Control Interno
Objetivo	Obtener la información referente a la investigación que se realice dentro de una organización.
Alcance	El arbitraje interno de las empresas Ocañeras pretende detectar los riesgos, amenazas y vulnerabilidades de las mismas para evitar el fraude, robo, y en general, el uso inadecuado y no autorizado de los datos que hacen parte de los movimientos operativos de las empresas como una consecuencia subyacente del objetivo planteado en favor de defender la disponibilidad, confidencialidad, e integridad de la información.
Recursos	Documentos sobre las políticas, el alcance y las fases de la gestión consignados en las plantillas y el "Sistema de Gestión del Riesgo de Seguridad Informática para beneficiar la operación del servicio en empresas ubicadas en Ocaña norte de Santander".
Pasos a seguir	1. Solicitar la estructura orgánica de la empresa. 2. Evaluar los documentos solicitados. 3. Realizar entrevistas o listas de chequeo con todos los empleados de la organización. 4. Registrar o grabar las respuestas dadas con los empleados de la organización 5. Examinar la información recolectada. 6. Evaluar la información recolectada. 7. Realizar un resumen de la información suministrada por la empresa. 8. Mostrar resultados, mediante un informe de gestión.
Hallazgos	Cualquier evento, registrado, documentado o encontrado en el momento que

	se realiza la auditoria, valdrá para valorar el cumpliendo de lo auditado.
Gestión de problemas	Detección de incidentes.

En relación con lo anterior, la tabla 11 se propone un formato de verificación que puede ser usado para la revisión del cumplimiento de los parámetros allí dispuestos, de manera que, los ítems de control pueden ser revisados para rectificar a modo general el cumplimiento del SGSI como un ejercicio de corroboración aplicado de forma general a las empresas del municipio de Ocaña-Norte de Santander en beneficio de sus operaciones.

Tabla 12 Seguimientos a los controles

Seguimientos a los controles

CONTROLES	SI	NO	N/A	OBSERVACIONES
Política de seguridad de la información.				
Organización de la seguridad de la información.				
Gestión de activos.				
Gestión de comunicación y operaciones.				
Control de acceso.				
Adquisición, desarrollo y mantenimiento de sistema de información.				
Gestión de los incidentes de la seguridad de la información.				

De manera sintética, la estructuración de los componentes del sistema de gestión del riesgo en seguridad informática en beneficio de la operatividad de las empresas en Ocaña-Norte de Santander puede ser desarrollada de acuerdo con la normativa señalada en la ISO 27001:2013 en articulación con la mejora de las prácticas de gestión de TI a partir de la mitigación de los

incidentes y sus potenciales impactos en las actividades económicas, financieras y tecnológicas de las empresas.

Por lo cual, la realización y presentación del "Sistema de Gestión del Riesgo de Seguridad Informática para beneficiar la operación del servicio en empresas ubicadas en Ocaña norte de Santander", se constituye como un resultado de amplia implementación en las diferentes organizaciones que componen al sector empresarial del municipio a partir del seguimiento de las distintas fases desarrolladas, siendo esto un importante aspecto de referencia regional con aplicación en los sistemas de gestión de la seguridad informática.

4.4 Aplicación de un Caso de Pruebas en Relación al Sistema de Gestión del Riesgo, Comprobando con ello su Utilidad a Través de una Simulación de Ataques Informáticos

Los espacios virtuales son un método confuso a nivel material, de red y cognoscitivo, debido a la interconexión entre el hombre, *software* y *hardware,* en donde existen altas posibilidades de generarse situaciones no previstas que fácilmente generen riesgos sistemáticos que afecten a las organizaciones y clientes (Villa, 2018); no obstante, son elementos que por su complejidad generan un impacto en la sociedad al inestabilizar de modo financiero a las compañías, las cuales deben estar preparadas y tomar medidas para evitar la vulnerabilidad, al contar con expertos en el área, que les contribuyan a disminuir los riesgos gestionando sus sistemas.

Por ello, y, con el propósito de dar cumplimiento al cuarto objetivo de la investigación, para comprobar la utilidad del Sistema de Gestión del Riesgo, en la simulación de ataques informáticos; se realizó encuentro con una de las empresas participantes del Municipio de Ocaña

y 4 ingenieros informáticos, con quienes se pudo exponer el caso de pruebas del sistema estructurado en fundamento de la NTC- ISO 27001:2013, en donde al conocer lo propuesto, consideraron que es de gran importancia para las organizaciones del municipio, puesto que, su experiencia les permite saber si existen aspectos por mejorar.

Como aplicación caso de pruebas con la empresa de Ocaña, la experta en Riesgos Informáticos de Sistema de Gestión del Riesgo Luzelis Hernández de la empresa Transportadora Regional S.A., localizada en el Municipio de Ocaña, mediante encuentro por Google Meet, en donde se le dio a conocer el Sistema de Gestión del Riesgo de Seguridad Informática para beneficiar la operación del servicio en empresas ubicadas en Ocaña Norte de Santander.

Figura 17 Presentación de la Guía para el sistema de Gestión del Riesgo de Seguridad Informática a la Empresa

Presentación del Sistema de Gestión del Riesgo de Seguridad Informática a la Empresa

Fuente: https://drive.google.com/file/d/10n542SS2VB1u-q3daXBUZulmMZ_NhqA2/view?usp=sharing

En este encuentro se expresó que, como es sabido por los expertos, la ciberseguridad requiere un tratamiento especial, adicional del área técnica de sistemas de una empresa, como parte de las políticas y estrategias que esta emplee, en vista que, actualmente la comunicación y tecnologías son digitales, por tanto, la ciberseguridad no es una opción sino una necesidad. Teniendo esto presente, se aplicó una entrevista realizada a través de la plataforma de Google Forms, mediante la cual expresó su respuesta (Ver anexo 3):

1. Si, considera que las políticas a nivel general se encuentran orientadas a mejorar la calidad del servicio en las organizaciones y asegurar la operación de los mismos

2. El sistema planteado, si es adecuado para realizar un seguimiento a los controles y respuesta a incidentes.

3. Respecto al sistema planteado, si cree que está lo suficientemente estructurado para mitigar los riesgos informáticos en las empresas.

4. De las fases presentadas, ninguna está mal estructurada y viabilizada (debido que se fundamentan en la norma NTC- ISO 27001:2013

5. Como observación general al sistema planteado, considera que: *"Ser muy cuidadosos en la etapa del análisis del riesgo, en especial, en el robo o fuga de la información, que es unos de los principales problemas que se presente en las empresas a nivel informativo".*

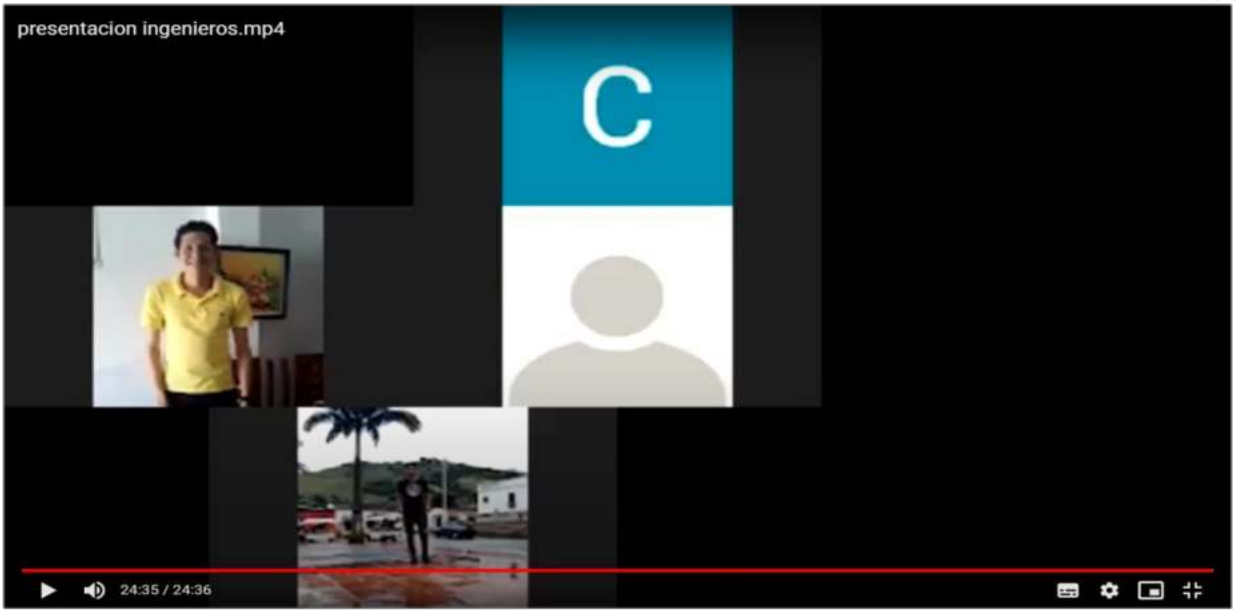
Como se pudo observar, es claro que, pese a la aplicación de sistemas de gestión del riesgo, con base a la normativa de la ISO 27001:2013, es indispensable tener presente que la etapa de análisis del riesgo, es una de las que demanda mayor cuidado, y en donde el sector empresarial es más afectado, teniendo problemas diversos al no tomar las medidas necesarias

adecuándolas de modo personalizado a las necesidades de la organización, así como al entorno en donde se desenvuelve.

Esto tiene gran influencia de los canales digitales, los cuales son empleados constantemente, aún con las ventajas que ofrecen, conllevan a tener mayor riesgo , por lo tanto, se requiere de un trabajo constante para prevenir y enfrentar ataques y fraudes informáticos; confirmándose la importancia que tienen las empresas de tomar y emplear el sistema de gestión de riesgos informáticos, y mantenerse actualizado de las mejora que la norma pueda incorporar, para protegerse como usuarios y a sus clientes, manejando la información de modo adecuado.

Por otra parte, en la aplicación caso de pruebas con Ingenieros Informáticos de Sistema de Gestión del Riesgo, mediante encuentro por Google Meet, y entrevista, se corroboró lo expuesto por la experta de la empresa participante, en donde todos estuvieron atentos y confirmaron que la información plasmada en esta herramienta para las compañías del Municipio de Ocaña, es de gran aporte y contribución para el área cibernética y económica de las mismas.

Figura 18 *Presentación del Sistema de Gestión del Riesgo de Seguridad Informática a los Ingenieros*
Presentación del Sistema de Gestión del Riesgo de Seguridad Informática a los Ingenieros



Fuente:https://drive.google.com/file/d/1pEPbC7gHFQK0E_qUwSXXVuKkykH78F5Z/view?usp=sharing

Figura 19 *Presentación del Sistema de Gestión del Riesgo de Seguridad Informática a los Ingenieros*

Presentación del Sistema de Gestión del Riesgo de Seguridad Informática a los Ingenieros

Fuente:https://drive.google.com/file/d/1pEPbC7gHFQK0E_qUwSXXVuKkykH78F5Z/view?usp=sharing

Posteriormente, mediante entrevista realizada a los 4 ingenieros entre los cuales se encontraron: Ronaldo Duran Amaya, William Fernando Arenas Álvarez, Leandro Quintero Navarro y Danilo Andrés Ascanio Lobo; quienes expusieron su opinión en la plataforma de Google Forms, su respuesta a las siguientes interrogantes (Ver anexo 4), observándose, al presentarles el Sistema de Gestión del Riesgo que lograron participar activamente emitiendo comentarios positivos de la misma; debido que, está se basó en la norma ISO 27001:2013; y tiene como fin contribuir en el gestionamiento del resguardo de datos informáticos de las empresas del Municipio de Ocaña.

1. ¿Considera usted que las políticas a nivel general se encuentran orientadas a mejorar la calidad del servicio en las organizaciones y asegurar la operación de los mismos?

Tabla 13 Operacionalización de variables

Pregunta 1 Ingenieros

Participantes	SI	NO
P1	X	
P2	X	
P3	X	
P4		X

Figura 20 Pregunta 1 ingenieros

Pregunta 1 ingenieros

El 75% de los participantes expuso que si consideran que las políticas a nivel general se encuentran orientadas a mejorar la calidad del servicio de las organizaciones y asegurar la operación de estos, y por el contrario, el 25% expresó que no, debido que, creen que más que políticas debe aplicarse en la práctica diaria, debido que, los sistemas de gestionamiento de resguardo de la información y datos, está compuesto por procedimientos de implementación, mantenimiento y mejora continua, para garantizar el aseguramiento de los datos de una empresa.

2. ¿Con respecto al sistema planteado para realizar un seguimiento a los controles y respuesta a incidentes lo considera adecuado?

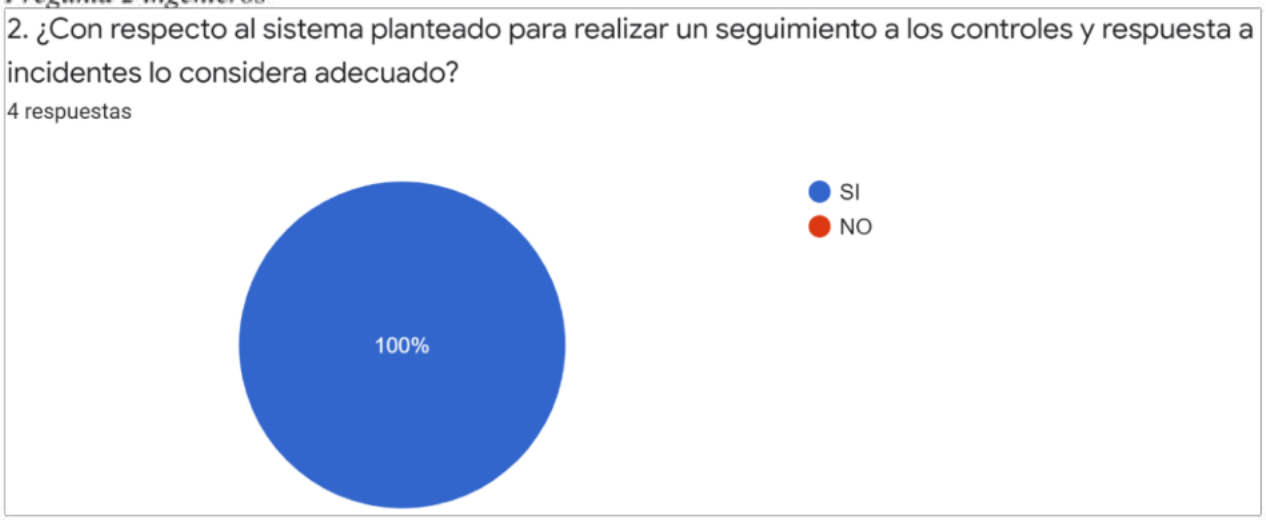
Tabla 14 Pregunta 2 Ingenieros

Pregunta 2 Ingenieros

Participantes	SI	NO
P1	X	
P2	X	
P3	X	
P4	X	

Figura 21 Pregunta 2 ingenieros

Pregunta 2 ingenieros



En esta interrogante, el 100% de los participantes coincidieron que, se considera adecuada la realización del seguimiento a los controles y respuesta a incidentes, puesto que, estas acciones permite la priorización, ampliación y efectividad de los datos, para ser analizados, probados, con el propósito de optimizar el grado seguridad informática, considerándose que, al ser implementado el seguimiento a dichos controles contribuye en la garantía que ofrece las

empresas para certificar su competitividad en el mercado, al contar con instrumentos internos de la organización.

3. ¿Con respecto al sistema planteado creería usted que si está lo suficientemente estructurado para mitigar los riesgos informáticos en las empresas?

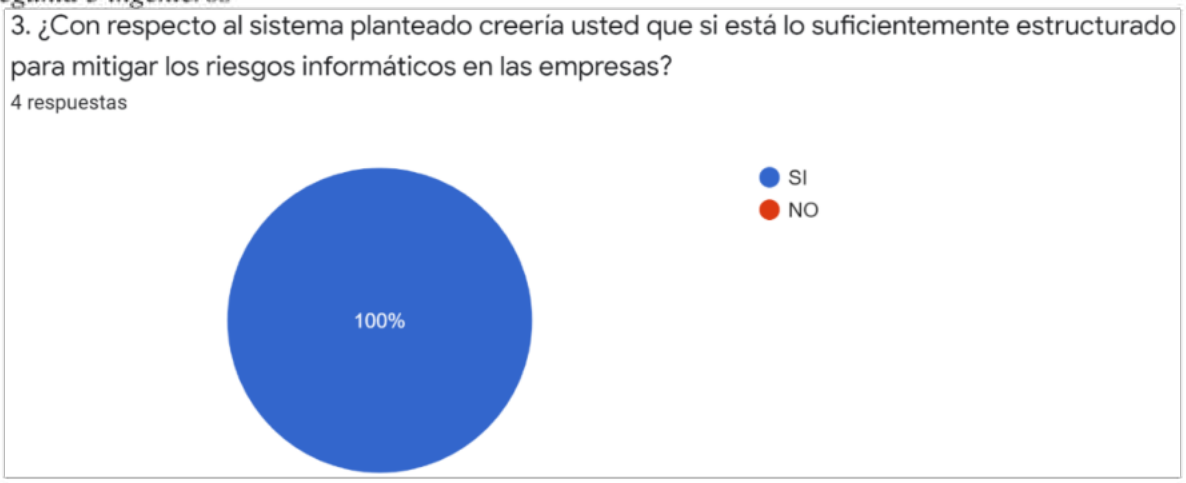
Tabla 15 *Pregunta 3 Ingenieros*

Pregunta 3 Ingenieros

Participantes	SI	NO
P1	X	
P2	X	
P3	X	
P4	X	

Figura 22 *Pregunta 3 ingenieros*

Pregunta 3 ingenieros



Los expertos en seguridad informática expresaron en un 100%, que el sistema planteado si es lo suficientemente estructurado para mitigar los riesgos informáticos en las empresas del Municipio de Ocaña; con fundamento en la insuficiencia en el contexto corporativo, estos instrumentos contribuyen en el resguardo y mitigación de dificultades del área informática;

puesto que, la inoportuna gestión de problemas de este tipo, pueden llegar a generar compromisos que involucren información de la compañía así como de los involucrados, extendiéndose al área legal/penal. Por ello, es necesario basar la protección de los sistemas de información mediante una correcta gestión de riesgos, teniendo en cuenta la evaluación de riesgos y amenazas, controlando y minimizándolos, contar con personal profesional capacitado, así como analizar, evaluar y mantener constantemente un control de los sistemas de seguridad informáticos.

4. ¿Cuál de estas fases cree usted que está mal estructurada y viabilizada? Si su respuesta es alguna de las fases, ¿Por qué? _____

Tabla 16 Pregunta 4 Ingenieros

Pregunta 4 Ingenieros

Participantes	Fase 1	Fase 2	Fase 3	Fase 4	Ninguna
P1					X
P2					X
P3					X
P4					X

Figura 23 Pregunta 4 ingenieros

Pregunta 4 ingenieros

Con el fin de corroborar la información propuesta en el Sistema de Gestión del Riesgo Informático en las empresas del Municipio de Ocaña, se formuló a los expertos si consideraban que tanto la estructura como viabilizarían de las fases presentadas como: "Fase 1. Análisis del riesgo; Fase 2. Clasificación del riesgo; Fase 3. Reducción del riesgo, y, Fase 4. Control del riesgo"; quienes respondieron que ninguno, reflejado en el 100% de la figura anterior, estas fases son las que conlleva a disminuir las amenazas cibernéticas a las que están propensas las organizaciones, y, por ende, requieren de un plan de cubrimiento para certificar las actividades de la empresa de acuerdo a sus necesidades, teniendo en cuenta las 4 fases antes mencionadas, como elementos básicos para generar un impacto positivo en la compañía.

5. ¿Qué observación puedes dar para mejorar el sistema planteado?

Tabla 17 Pregunta 5 Ingenieros

Pregunta 5 Ingenieros

Participantes	Respuesta
P1	Ninguna, creo que el modelo del sistema está estructurado de una manera correcta, que, si se ejecutan en la manera planteada, tendrá un gran impacto positivo a nivel organizacional.
P2	En blanco
P3	El sistema es muy bueno, si se implementa de la mejor manera. Las empresas ocañeras deben ponerse al día con la tecnología para no tener en un futuro inconvenientes con sus datos y activos.
P4	En blanco

En cuanto a las observaciones de mejora para el sistema de gestión del riesgo informático propuesto para las empresas del Municipio de Ocaña, el 50% no emitió opiniones dejando en blanco los espacios, el otro 50%, indicó que, el sistema expuesto es bueno, no obstante, depende de cada empresa si lo implementa y la manera como lo hagan, si lo llevan a cabo como se plantea

y de acuerdo a los lineamientos de la normativa ISO 27001:2013, tendrían un impacto positivo para los empresarios ocañeros, quienes podría brindar seguridad en el manejo de información y datos de los usuarios de sus plataformas en la web.

Para cerrar este apartado, se puede decir que, mediante el Sistema de Gestión del Riesgo, y la opinión de los expertos se ha logrado comprobar la utilidad para prevenir ataques informáticos, teniendo presente que ha sido diseñada bajo la norma ISO 27001:2013, por tanto, su eficacia garantiza seguridad a las empresas del Municipio de Ocaña, consiguiendo la mayores ventajas, e incrementando la confianza de sus aliados y clientes; mejorando su productividad en el manejo de los datos y la optimización de respuesta a las necesidades esenciales de la compañía; dado que, la información hace parte elemental de todas la organizaciones para el alcance de sus metas, y mitigando en gran porcentaje los riesgos, siempre y cuando se aplique de manera correcta.

Capítulo V. Conclusiones y Recomendaciones

5.1 Conclusiones

El análisis del contexto de las empresas ubicadas en el municipio de Ocaña Norte de Santander, dio a conocer que los protocolos usados para la gestión del riesgo de pérdida de información están relacionado con los ataques informáticos que han presentado un 70% de las empresas Ocañeras, durante los últimos dos años; sin embargo, estos incidentes no han representado la inactividad del 100% de las empresas, destacando, además que, los medios tecnológicos usados constan de computadores (60%), celulares (30%) y tablets (10%) lo cual muestra flexibilidad ante las alternativas.

Por su parte, los sistemas operativos empleados por las empresas de Ocaña se componen de Software libre (10%), Linux (30%), Mac OC (20%), y Windows en algunas de sus versiones (40%) siendo este aspecto variado entre la caracterización tecnológica de las empresas; asimismo, el 90% de las empresas cuenta con portal de productos, aunque el 80% de las mismas no cuente con un servidor propio, en donde también se observó que la seguridad interna apunta a que no se han registrado robos de información al interior de las organizaciones. La tercerización como servicio de almacén online por parte de las empresas mostró que en el 60% de los casos no se cuenta con tal herramienta. Aun así, el 70% de las empresas cuenta con personal de gestión de riesgos informáticos como parte de apoyo ante ataques, a lo cual el 70% de las empresas busca personal externo como respuesta ante los incidentes para el manejo del impacto.

La caracterización de los estándares, métodos, técnicas y tecnología requeridos para la proposición de los componentes necesarios en un sistema de gestión del riesgo de seguridad informática, como consecuencia del análisis del contexto de seguridad informática de las empresas de Ocaña-Norte de Santander, se basó en los estándares metodológicos como criterios de análisis, así como, en los aportes realizados por los autores de tesis relacionadas, y la consideración de las tecnologías emergentes como propulsores de la competitividad, productividad y operatividad de las empresas permitiendo diferenciar los potenciales desarrollados a partir de cada metodología, con el fin de seleccionar los criterios técnicos y prácticos acorde con el contexto, la composición, y la caracterización de los elementos necesarios para el adecuado despliegue del sistema de gestión del riesgo en seguridad informática.

Finalmente, la estructuración de los componentes del sistema de gestión del riesgo en seguridad informática bajo la óptica de las mejores prácticas de gestión de TI en beneficio de mitigar los incidentes y sus impactos en las empresas permitió el desarrollo de un sistema para gestionar el riesgo de la seguridad informática, a partir de la definición de la política, del alcance del SGSI, el análisis del riesgo, la gestión del riesgo, la selección de controles a implementar, la declaración de la aplicabilidad, y la revisión del sistema; en adición a esto, se presentó un formato para la verificación y seguimiento a los controles para el cumplimiento del SGSI de acuerdo con la Norma ISO 27001:2013.

Para finalizar, se concluye que se ha comprobado la efectividad y utilidad del Sistema de Gestión del Riesgo, certificada mediante el juicio de los técnicos, confirmando que al llevarse a cabo de manera específica como se planteó, las empresas del Municipio de Ocaña, podrán resguardar su información, puesto que, está se orientó por las pautas de la ISO 27001:2013, por

ende, su eficiencia avala seguridad a las empresas Ocañeras, logrando distinción y desarrollando la fidelización de sus socios y consumidores; optimizando su producción en la administración de información y la mejora del reconocimiento a las insuficiencias fundamentales de los involucrados.

5.2 Recomendaciones

De acuerdo a los resultados obtenidos, se recomienda que, todas las empresas del municipio deben generar protocolos para gestionar el riesgo de daño o pérdida de datos, como consecuencia de los ataques informáticos que usualmente en la actualidad se generan.

Debido a la gran cantidad de organizaciones que emplean el manejo de portales para la promoción de sus productos y servicios en el municipio de Ocaña, es indispensable que mantengan el cuidado que aplican a su información, debido que en cualquier momento pueden ser víctimas de un ataque informático.

Se recomienda contar con personal capacitado en el área de seguridad informática, para ofrecer mayor tranquilidad y seguridad tanto para la compañía como a sus clientes, empleando los pasos planteados en el sistema de gestión de riesgo de seguridad informática, en donde pueden definir su política, alcance, análisis de riesgo, gestión de riesgo, controles, aplicabilidad y revisión constante del sistema, como medida de respaldo para su organización.

Referencias

Aguado García, D. (2018). Analítica de recursos humanos: Explorando oportunidades a partir del big data y la práctica del" human resources analytics". (En línea). Revista Vasca de Gestión de Personas y Organizaciones Públicas. Disponible en: https://repositorio.uam.es/handle/10486/685208

Alama Visitación, M. (2019). Implementación de un sistema de gestión de riesgos basados en el estándar ISO 31000 en el proceso de atención de requerimientos de la empresa Software Enterprise Services en la ciudad de Lima–2018. (En línea). Repositorio Institucional de la UTP. Disponible en: https://repositorio.utp.edu.pe/handle/20.500.12867/1840

Alfaro Gómez, M. (2020). Estrategia de negocio para el servicio de Ciber Seguridad Entel SA. (En línea). Repositorio Académico de La Universidad de Chile. Disponible en: https://repositorio.uchile.cl/handle/2250/176772

Antúnez, V. (2016). Sistemas integrados de gestión: de la teoría a la práctica empresarial en Cuba. Cofin Habana.

Arévalo Ascanio, J., Bayona Trillos, R., & Rico Bautista, D. (2015). Implantación de un sistema de gestión de seguridad de información bajo la ISO 27001: Análisis del riesgo de la información. (En línea). Revista Tecnura, 19(46), 123-134. Disponible en: https://revistas.udistrital.edu.co/index.php/Tecnura/article/view/9551/10782

Aristizábal Arroyave, M., Ruiz Arias, C., & Valencia Ortiz, Y. (2018). Seguridad de la información en una empresa de seguridad privada de Pereira. (En línea). Fundación

Universitaria del Área Andina. Disponible en: https://digitk.areandina.edu.co/repositorio/handle/123456789/2767

Asamblea Nacional Constituyente (1991). Constitución política de Colombia. (En línea) Bogotá, Colombia: Leyer, 1. Disponible en: https://pdba.georgetown.edu/Constitutions/Colombia/colombia91.pdf

Ayala León, F., & López Valencia, F. (2019). Diseño e implementación de la ISO 27035 (gestión de incidentes de seguridad de la información) para el área de plataforma de servicios de una entidad del estado peruano. (En línea). Repositorio Institucional Universidad Tecnológica del Perú. Disponible en: https://repositorio.utp.edu.pe/handle/20.500.12867/2477

Ayala Medrano, A. (2017). Sistema de gestión de seguridad de información para mejorar el proceso de gestión del riesgo en un hospital nacional, 2017. (En línea). Repositorio de la Universidad César Vallejo. Disponible en: https://repositorio.ucv.edu.pe/handle/20.500.12692/13753

Bailón-Lourido, A. (2019). Gestión de riesgos del área informática de las empresas exportadoras de pesca blanca de Manta y Jaramijó. (En línea). Revista Polo del Conocimiento, 4(8), 165-189. Disponible en: https://polodelconocimiento.com/ojs/index.php/es/article/view/1053

Bautista Sarria, A. (2018). Diseño de un sistema de gestión de seguridad informática-SGSI para la Fundación Sabemos Cuidarte en la ciudad de Popayán. (En línea). Repositorio Universidad Nacional Abierta y a Distancia UNAD. Disponible en: https://repository.unad.edu.co/handle/10596/21306

Beltrán, C. (2021). Análisis De La Seguridad Informática En Las Transacciones Electrónicas Para El Comercio Electrónico. (En línea). Universidad Nacional Abierta y a Distancia UNAD. Disponible en: https://repository.unad.edu.co/handle/10596/44132

Bermúdez, K., & Bailón, E. (2015). Análisis en seguridad informática y seguridad de la información basado en la norma ISO/IEC 27001-Sistemas de gestión de seguridad de la información dirigido a una empresa de servicios financieros. (En línea). Universidad Politécnica Salesiana, Sede Guayaquil-Ecuador. Disponible en: https://dspace.ups.edu.ec/bitstream/123456789/10372/1/UPS-GT001514.pdf

Betancourth García, V. (2020). Modelo para la gestión de seguridad de la información en el sector de microfinanzas en Guatemala. (En línea). Tesis de Grado en Universidad de San Carlos de Guatemala. Disponible en: http://www.repositorio.usac.edu.gt/15383/

Briñez Bautista, L. (2017). Diseño de un sistema de gestión de seguridad informática para la alcaldía municipal de la Jagua de Ibirico–Cesar basado en la Norma ISO 27001: 2013. (En línea). Repositorio Universidad Nacional Abierta y a Distancia UNAD. Disponible en: https://repository.unad.edu.co/bitstream/handle/10596/14253/1003165759.pdf?sequence=1&isAllowed=y

Buitrago Giraldo, E. (2020). Sistemas de gestión en seguridad informática SGSI en universidades públicas del eje cafetero-Colombia. (En línea). Repositorio Universidad Nacional Abierta y a Distancia UNAD. Disponible en: https://repository.unad.edu.co/handle/10596/34357

Cabas Cortes, P. (2021). Usos del Big data en auditorias financieras en Latinoamérica. (En línea). Repositorio Institucional UCC. Disponible en: https://repository.ucc.edu.co/handle/20.500.12494/33203

Cajusol Santisteban, F., & Céspedes Deza, D. (2019). Procesamiento digital y transmisión de imágenes radiográficas para ayudar en el diagnóstico y tratamiento oportuno de enfermedades pulmonares en localidades rurales de Lambayeque. (En línea). Repositorio Institucional UNPRG. Disponible en: https://repositorio.unprg.edu.pe/handle/20.500.12893/4070

Cámara de Comercio de Ocaña (2017). Estudio económico jurisdicción Cámara de Comercio de Ocaña año 2016. (En línea). [Consultado el 15 de enero de 2022]. Disponible en: https://camaraocana.com/wp-content/uploads/2020/03/Estudio-economico-2016.pdf

Caracol Cúcuta. (18 de mayo de 2017). Autoridades reportan primeros casos de ciberataques en Cúcuta. (En línea). [Consultado el 12 de enero de 2022]. Disponible en: https://caracol.com.co/emisora/2017/05/18/cucuta/1495119940_627460.html

Caro, M. (2011). Alcance y ámbito de la seguridad nacional en el ciberespacio. (En línea). Ciberseguridad. Retos y amenazas a la seguridad nacional en el ciberespacio, 49-82. Cuadernos de estrategia, 147. España: Ministerio de Defensa. Disponible en: file:///D:/Documents/Downloads/Dialnet-AlcanceYAmbitoDeLaSeguridadNacionalEnElCiberespaci-3837251%20(1).pdf

Castillo Plata, R. (2020). Actualización norma ISO/IEC 27001: 2005 para la versión 2013 en caracol televisión. (En línea). Fundación Universitaria Los Libertadores. Disponible en: https://repository.libertadores.edu.co/handle/11371/2722

Ceballos, A. (2020). Tendencias Cibercrimen en Colombia 2019-2020. (En línea). Informe de las Tendencias del Cibercrimen en Colombia 2019-2020. Disponible en: https://www.ccit.org.co/wp-content/uploads/informe-tendencias-cibercrimen_compressed-3.pdf

Chinchilla, E., & Allende, J. (2017). Riesgos de ciberseguridad en las empresas. (En línea). Revista Tecnología y desarrollo, 15. Disponible en: file:///D:/Documents/Downloads/1174-1054-1-SM.pdf

Claro Ropero, P., & Espinel Blanco, E. (2019). Plan de gestión de seguridad de la información para el motel Dubái, como medida de protección a las áreas vitales de la empresa. (En línea). Trabajo de Grado, Universidad Francisco de Paula Santander, Ocaña. Disponible en: http://repositorio.ufpso.edu.co/handle/123456789/2906

Congreso de Colombia (2012) Ley 1581 de 2012, Artículo 1-2. (En línea) Ley Estatutaria Reglamentada por el Decreto Nacional 1377 de 2013. Diario Oficial No. 48.587 de 18 de octubre de 2012. Disponible en: https://www.defensoria.gov.co/public/Normograma%202013_html/Normas/Ley_1581_2012.pdf

Congreso de Colombia. (2009). Ley 1273 de 2009, Artículo 269 (En línea) Código Penal. Disponible en: https://www.sic.gov.co/recursos_user/documentos/normatividad/Ley_1273_2009.pdf

Cotrina Roldan, E. (2020). El espionaje corporativo y su incidencia en el funcionamiento interno de las empresas privadas del periodo 2007-2013. (En línea). Repositorio Institucional UPN. Disponible en: https://repositorio.upn.edu.pe/handle/11537/26127

Criollo Tasinchana, M. (2017). Análisis e Implantación de la norma ISO/IEC 27002: 2013 para el departamento informático del Gobierno Autónomo Descentralizado Municipal del Cantón Salcedo. (En línea). Repositorio Universidad Técnica de Ambato. Disponible en: http://repositorio.uta.edu.ec/handle/123456789/26537

Cruz, G., & Cerrillo, F. (2020). Requisitos que deben cumplirse para proteger los datos personales en la contratación de servicios de cómputo en la nube en la administración pública federal. (En línea). Repositorio INFOTEC. Disponible en: https://infotec.repositorioinstitucional.mx/jspui/handle/1027/422

Cuellar Castrillón, E. (2020). Diseño de un Sistema de Gestión de Seguridad de la Información (SGSI) para la Institución Edutec de los Andes Pitalito, argumentada en la norma ISO/IEC 27001. (En línea). Trabajo de especialización, Universidad Nacional Abierta y a Distancia UNAD. Disponible en: https://repository.unad.edu.co/bitstream/handle/10596/34804/jecuellarc.pdf?sequence=2&isAllowed=y

Desarrollo y Gestión de Seguridad de Redes (2022). Fundamentos de Seguridad. (En línea). [Consultado el 10 de enero de 2022]. Disponible en: https://sites.google.com/site/desygestiondeseguridadderedes/home/fundamentos-de-seguridad

Díaz Quiceno, D. (2018). Diseño de políticas para la gestión de la información de la alcaldía de Montecristo Bolívar. (En línea). Universidad Nacional Abierta y a Distancia UNAD. Disponible en: https://repository.unad.edu.co/bitstream/handle/10596/33256/jddiazq.pdf?sequence=1&isAllowed=y

Doncel Ortegón, W., Pinto Barreto, M., & Perozo León, M. (2019). Diagnóstico para la mitigación de riesgos informáticos de la empresa LYD Colombia SAS (En línea). Doctoral dissertation. Disponible en: http://repository.unipiloto.edu.co/handle/20.500.12277/6485

Erickson, J. (2008). Hacking: the art ofexploitation. No starchpress. (En línea). Edición ilustrada, ISBN 1593271441, 9781593271442, pp. 488. Disponible en: https://books.google.es/books?hl=es&lr=&id=0FW3DMNhl1EC&oi=fnd&pg=PP13&ots=tw2uGTH__t&sig=i9goGkfwPXp5njG-y2Z11xuHGAE#v=onepage&q&f=false

ESET (2018). Security Report. (En línea). [Consultado el 5 de enero de 2022]. Disponible en: https://www.welivesecurity.com/wp-content/uploads/2018/06/ESET_security_report_LATAM2018.pdf

ESET (2020). Security Report. (En línea). [Consultado el 5 de enero de 2022]. Disponible en: https://www.welivesecurity.com/wp-content/uploads/2020/08/ESET-Security-Report-LATAM_2020.pdf

Estándar Australiano AS/NZS, 4. (1999). Administración de Riesgos. (En línea). Estándar Australiano. Disponible en: https://ucipfg.com/Repositorio/MATI/MATI-01/Unidad2/lecturas/standard__adm_risk_as_nzs_4360_1999.pdf

Fases de Gestión de Riesgo (enero de 2022). Gestión de Riesgo en la Seguridad Informática. (En línea). [Consultado el 13 de enero de 2022]. Disponible en: //protejete.wordpress.com/gdr_principal/gestion_riesgo_si/

Fernández-Alarcón, V. (2021). Desarrollo de sistemas de información: una metodología basada en el modelado. (En línea). Universitat Politècnica de Catalunya. Disponible en: https://www.mdx.cat/handle/2099.3/36751

Fernández-Ramos, G. (2021). Análisis y diseño de un sistema de gestión de seguridad de la información basado en la norma NTP–ISO/IEC 27001: 2014 en la empresa consultora N&V asesores SAC. (En línea). Repositorio DSpace Principal. Disponible en: https://repositorio.uss.edu.pe/handle/20.500.12802/8928

Figueroa Rodríguez, N., Rodríguez Sáez, S., & Wong Rendon, S. (2019). Plan de mejora de procesos, basado en tecnología Blockchain para afrontar fraudes en pagos electrónicos. (En línea). Repositorio Fundación Universitaria Compensar. Disponible en: https://repositoriocrai.ucompensar.edu.co/handle/compensar/3493

Fonseca Herrera, A. (2019). Modelo de un sistema de gestión de seguridad de la información en la organización Geoconsult CS. (En línea). Tesis de Maestría, Universidad EAN, Bogotá D.C., Colombia. Disponible en: https://repository.ean.edu.co/bitstream/handle/10882/9521/FonsecaOmar2019.pdf?sequence=1&isAllowed=y

Giraldo Martínez, P., & Pacheco Duarte, G. (2018). Ingeniera social: Técnica de ataque Phishing y su impacto en las empresas colombianas. (En línea). Universidad Nacional Abierta y a Distancia UNAD. Disponible en: https://repository.unad.edu.co/handle/10596/27050

Gómez Bautista, A., & Rey Sepúlveda, A. (2019). Diseño de red bayesiana para la predicción de ataques informáticos de tipo Ransomware. Caso de estudio PYMES prestadoras de servicios. (En línea). Repositorio Universidad Autónoma de Bucaramanga. Disponible en: https://repository.unab.edu.co/handle/20.500.12749/7312

Gómez, F., Duchimaza, J., Holguín, R., & Lindao, A. (2019). Plan de contingencia para los equipos y sistemas informáticos utilizando la metodología MAGERIT. (En línea). Revista

Científica y Tecnológica UPSE, 6(1), 34-41. Disponible en: http://incyt.upse.edu.ec/ciencia/revistas/index.php/rctu/article/view/429

Gonzales Castillo, A., & Soles Cavero, G. (2021). E-commerce web para agilizar el proceso de atención de pedidos de clientes en La Valentina Restaurante-Trujillo. (En línea). Repositorio Universidad Nacional de Trujillo. Disponible en: https://dspace.unitru.edu.pe/handle/UNITRU/17737

González Agudelo, M., & García Castaño, E. (2010). Contratación y comunicación: variables estratégicas en la gestión del capital humano en las pymes. (En línea). Repositorio Universidad de Medellín. Disponible en: https://repository.udem.edu.co/handle/11407/49

Guachi Aucapiña, V. (2012). Norma de seguridad informática ISO 27001 para mejorar la confidencialidad, integridad y disponibilidad de los sistemas de información y comunicación en el Departamento de Sistemas de la Cooperativa de Ahorro y Crédito San Francisco Ltda. (En línea). Trabajo de Grado, Universidad Técnica de Ambato. Disponible en: http://repositorio.uta.edu.ec/handle/123456789/2361

Guamán Seis, A. (2014). Diseño de un sistema de gestión de seguridad de la información para instituciones militares. (En línea). Tesis de Maestría, Escuela Politécnica Nacional, Ecuador. Disponible en: https://bibdigital.epn.edu.ec/handle/15000/10439

Guano Guerrero, M. (2013). Aplicación del sistema SAP (sistemas, aplicaciones y productos en procesamiento de datos.) para el control del inventario. (En línea). Repositorio de la Universidad Estatal de Milagro. Disponible en: http://repositorio.unemi.edu.ec/handle/123456789/1130

Hernández Marín, Y. (2020). Análisis y diseño de un mecanismo de cifrado de correo electrónico para garantizar y proteger la información enviada de las pymes. (En línea).

Universidad Nacional Abierta y a Distancia UNAD. Disponible en: https://repository.unad.edu.co/handle/10596/36604

Inerarity Rodríguez, J. (2018). Contribución al mejoramiento del nivel de integración programación de la producción-programación del mantenimiento en la UEBCentroplast. (En línea). Repositorio Dspace. Disponible en: https://dspace.uclv.edu.cu/handle/123456789/9790

Ingunza Lastra, K., & Valdivia Jaimes, A. (2018). Implementación del modelo Arsi para optimizar la seguridad de la información en la cooperativa de ahorro y crédito san francisco Ltdo. 289. (En línea). Repositorio Institucional UNHEVAL. Disponible en: https://repositorio.unheval.edu.pe/handle/20.500.13080/4335

Izaguirre Olmedo, J., & León Gavilánez, F. (2018). Análisis de los ciberataques realizados en América Latina. (En línea). INNOVA Research Journal, 3(9), 172-181. Disponible en: https://doi.org/10.33890/innova.v3.n9.2018.837

Maldonado, E. (2020). Teoría de la información y complejidad. La Tercera Revolución Científica. (En línea). Universidad del Bosque. Disponible en: https://repositorio.unbosque.edu.co/handle/20.500.12495/3574

Maldonado, O. (2019). El Proceso de Comunicación del fenómeno de Marea Roja que involucra a los trabajadores de organizaciones de salud de la Provincia de Tierra del Fuego, en el marco de la promoción de la salud y la prevención de enfermedades. (En línea). Tesis de Maestría, Universidad Nacional del Rosario. Disponible en: http://rephip.unr.edu.ar/handle/2133/17176

Martín, R. (2021). Automatización de un sistema de gestión de seguridad de la información basado en la Norma ISO/IEC 27001. (En línea). Revista Universidad y Sociedad, 13(5),

495-506. Disponible en: http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S2218-36202021000500495

Martínez Rodríguez, F., & Rodríguez Mancera, A. (2019). Formulación de acciones de mejora para los servicios de seguridad informática brindados por INDRA-Colombia mediante la implementación de ITIL v3 y SCRUM para el I-CSOC en la sede de Bogotá. (En línea). Repositorio Universidad Cooperativa de Colombia. Disponible en: https://repository.ucc.edu.co/handle/20.500.12494/8233

Martínez, C., Páez, L., Gutiérrez, J., Sepúlveda, C., Mantilla, H., Giraldo, M., & Tojas, L. (2021). Sistema de Gestión de Seguridad Informática y Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información. (En línea). Gobierno Digital. Instituto departamental de salud de Norte de Santander, Cúcuta, Colombia. Disponible en: https://ids.gov.co/web/2021/PLAN_INTEGRADO/SGSI_Plan_Tratamiento_v3_2021.pdf

Mayanquer Andino, A. (2020). Análisis de seguridad de la información basado en las normas ISO/IEC 27001, para identificar vulnerabilidades en la sala de cómputo de la carrera de Ingeniería en Computación y Redes. (En línea). Trabajo de grado, Universidad Estatal del Sur de Manabí. Disponible en: http://repositorio.unesum.edu.ec/bitstream/53000/2581/1/MAYANQUER%20ANDINO%20JAVIER%20ANIBAL.pdf

Melchor Medina, J., Lavín Verástegui, J., & Pedraza Melo, A. (2012). Seguridad en la administración y calidad de los datos de un sistema de información contable en el desempeño organizacional. (En línea). Revista Contaduría y administración, 57(4), 11-34. Disponible en: http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S0186-10422012000400002

Mendoza Penagos, P. (2017). Diseño de un sistema de gestión de seguridad informática para la Empresa GED (Gestión Estrategia y Desarrollo) de la ciudad de Bogotá. (En línea). Repositorio Universidad Nacional Abierta y a Distancia UNAD. Disponible en: https://repository.unad.edu.co/bitstream/handle/10596/20723/39583963.pdf?sequence=1&isAllowed=y

Mendoza, M. (2020). Ciberataques: Una de las principales amenazas para el 2020. (2020, 13 febrero). (En línea). Welivesecurity. [Consultado el 15 de enero de 2022]. Disponible en: https://www.welivesecurity.com/la-es/2020/02/13/ciberataques-principales-amenazas-2020/

Meraz-Espinoza, I. (2018). Empresa y privacidad: el cuidado de la información y los datos personales en medios digitales. (En línea). Revista IUS, 12(41), 293-310. Disponible en: http://www.scielo.org.mx/pdf/rius/v12n41/1870-2147-rius-12-41-293.pdf

Miranda Cairo, M., Valdés Puga, O., Pérez Mallea, I., Portelles Cobas, R., & Sánchez Zequeira, R. (2016). Metodología para la implementación de la gestión automatizada de controles de seguridad informática. (En línea). Revista Cubana de Ciencias Informáticas, 10(2), 14-26. Disponible en: http://scielo.sld.cu/scielo.php?pid=S2227-18992016000200002&script=sci_arttext&tlng=en

Morales, F., Toapanta, S., & Toasa, M. (2020). Implementación de un sistema de seguridad perimetral como estrategia de seguridad de la información. (En línea). Revista Ibérica de Sistemas e Tecnologías de Información, (E27), 553-565. Disponible en: https://www.researchgate.net/profile/Renato-Mauricio-Toasa-G/publication/339956501_Implementacion_de_un_sistema_de_seguridad_perimetral_como_estrategia_de_seguridad_de_la_informacion/links/5e95ffa5a6fdcca78915c13f/Imple

mentacion-de-un-sistema-de-seguridad-perimetral-como-estrategia-de-seguridad-de-la-informacion.pdf

Muñoz Molina, V. (2021). Propuesta de diseño de seguridad informática a empresa registral de inmuebles de Durán, basado la ISO 27001: 2013 para área tecnológica. (En línea). Bachelor's thesis, Universidad de Guayaquil. Facultad de Ingeniería Química. Disponible en: http://repositorio.ug.edu.ec/handle/redug/57847

Nieves, C. (2017). Diseño de un sistema de gestión de la seguridad de la información (SGSI) basados en la norma ISO/IEC 27001: 2013. (En línea). Trabajo de grado de Especialización, Institución Universitaria Politécnico Grancolombiano, Valledupar, Colombia. Disponible en: https://alejandria.poligran.edu.co/handle/10823/994

Norma ISO 27001 (2013). Tecnología de la información. Técnicas de Seguridad. (En línea). Sistemas de Gestión de la Seguridad de la Información. Disponible en: file:///D:/Documents/Downloads/Norma._NTC-ISO-IEC_27001%20(1).pdf

Norma ISO 27032. (2012). Ciberseguridad utilizando la norma ISO 27032:2012. (En línea). Sisteseg Consulting Services, Bogotá-Colombia. Disponible en: https://sisteseg.com/blog/wp-content/uploads/2018/12/ISO-27032-v-2.pdf

Norma ISO 27032. (2012). Gestión de la Ciberseguridad. (En línea). Grupo ACMS consultores. Disponible en: https://www.grupoacms.com/imprimir/norma-iso-27032.pdf

Norma ISO 31000 (2011). Gestión del Riesgo. Principios y Directrices. (En línea). Norma Técnica Colombiana NTC. Disponible en: http://simudatsalud-risaralda.co/normatividad_inv9/normas_tecnicas/NTC-ISO31000_Gestion_del_riesgo.pdf

Ospina, M., & Sanabria, P. (2020). Desafíos nacionales frente a la ciberseguridad en el escenario global: un análisis para Colombia. (En línea). Revista Criminalidad, 62(2), 199-217. Disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=7667839

Pangalima Albán, A. (2018). Auditoría basada en cobit 4.1 para el uso óptimo de las TIC y la seguridad informática en la empresa Arcopa SA Paita; 2017. (En línea). Tesis de Maestría, Universidad Católica Los Ángeles Chimbote. Disponible en: http://repositorio.uladech.edu.pe/handle/123456789/10619

Pardo Cuenca, M. (2015). Modelo de Gestión de Seguridad de la Información para la Universidad Nacional de Loja basado en la norma ISO/IEC 27001. (En línea). Trabajo de Grado, Universidad Nacional de Loja, Ecuador. Disponible en: https://dspace.unl.edu.ec/jspui/bitstream/123456789/11277/1/Pardo%20Cuenca%2c%20Mar%c3%ada%20Gabriela.pdf

Pastrana Arango, A. (2000) Decreto número 599 de 2000, Artículo 195. (En línea) Departamento Administrativo de la Presidencia de la República. “Por la cual se expide el Código Penal”. Disponible en: https://www.oas.org/juridico/spanish/mesicic2_col_ley_599_2000.pdf

Patiño, R. (2017). Afectación del cibercrimen en las pymes. (En línea). En Congreso Internacional: Crimen económico y fraude financiero y contable (pp. 59-66). Disponible en: https://www.uniremington.edu.co/wp-content/uploads/2019/01/memorias-crimen-economico-2017.pdf#page=59

Pazmiño Salazar, W. (2021). Análisis comparativo de diversas metodologías de detección de malware y nivel de eficiencia en su detección. (En línea). Repositorio de la Universidad

Internacional SEK Ecuador. Disponible en: https://repositorio.uisek.edu.ec/handle/123456789/4384

Peñuela Vásquez, D. (2018). Análisis e identificación del estado actual de la seguridad informática, dirigido a las organizaciones en Colombia, que brinde un diagnóstico general sobre la importancia y medidas necesarias para proteger el activo de la información. (En línea). Repositorio Universidad Nacional Abierta y a Distancia UNAD. Disponible en: https://repository.unad.edu.co/handle/10596/17260

Pereyra Acosta, A. (2021). La ley de gobierno digital y su implicancia en la ciberdefensa del Estado Peruano, 2021. (En línea). Repositorio de la Universidad César Vallejo. Disponible en: https://repositorio.ucv.edu.pe/handle/20.500.12692/68971

Pérez Castro, C. (2021). Estudio Monográfico Sobre La Amenaza Ransomware, Su Impacto En Las Organizaciones y Buenas Prácticas Para Su Prevención y Manejo. (En línea). Universidad Nacional Abierta y a Distancia UNAD. Disponible en: https://repository.unad.edu.co/handle/10596/42143

Pineda Combariza, R., & Burbano Ortiz, M. (2019). Diseño del sistema de gestión por procesos para la empresa diseño, ingeniería, automatización y control DINACOL SA. (En línea). Repositorio Digital Univalle. Disponible en: https://bibliotecadigital.univalle.edu.co/handle/10893/12985

Pinzón Parada, I. (2014). Gestión del riesgo en Seguridad Informática. (En línea). Artículo de especialización, Universidad Piloto de Colombia. Disponible en: http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/2840/Gestion%20del%20riesgo%20en%20seguridad%20informatica.pdf?sequence=1&isAllowed=y

Polanco Calvachi, D. (2019). Desarrollo e implementación de un sistema de generación de documentos operacionales y control de inventario para la empresa Antonoil Service Company Sa De Quito. (En línea). Repositorio Digital Universidad Israel. Disponible en: http://repositorio.uisrael.edu.ec/handle/47000/1672

Puello Flórez, O. (2012). Operación del servicio. (En línea). Ingeniería del software, 5-9. Disponible en: http://manglar.uninorte.edu.co/bitstream/handle/10584/2209/Operaci?sequence=1

Quiroz, S., & Macías, D. (2017). Seguridad en informática: consideraciones. (En línea). Revista Científica Dominio de las Ciencias, 5-6. Disponible en: file:///D:/Documents/Downloads/663-1786-2-PB.pdf

Remolina Becerra, L. (2019). Diseño de un modelo de seguridad informática a una empresa en su sistema de monitoreo del área de tecnología. (En línea). Trabajo de Grado, Universidad Cooperativa de Colombia-Bogotá D.C. Disponible en: https://repository.ucc.edu.co/bitstream/20.500.12494/18082/1/2020_Dise%c3%b1o_modelo_seguridad.pdf

Robalino Chiriboga, P. (2020). Plan estratégico para el mejoramiento administrativo de la empresa de seguridad informática "Blue Hat Consultores Cia. Ltda.". (En línea). Doctoral dissertation, Quito/UIDE/2020.Disponible en: https://repositorio.uide.edu.ec/handle/37000/4324

Romero, M., Figueroa, G., Vera, D., Álava, J., Parrales, G., Alava, C., y otros. (2018). Introducción a la seguridad informática y el análisis de vulnerabilidad. (En línea). Alicante: Área de Innovación y Desarrollo, S.L.

Rouhiainen, L. (2018). Inteligencia artificial. Madrid. (En línea). Alienta Editorial. Disponible en: https://static0planetadelibroscom.cdnstatics.com/libros_contenido_extra/40/39308_Inteligencia_artificial.pdf

Rubiano, R., Garzón, L., Cabanzo, L., &Chávez, L. (2020). El código Hamming en la cuarta revolución industrial. (En línea). Revista Vínculos: Ciencia, tecnología y sociedad, 17(2), 104-111. Disponible en: file:///D:/Documents/Downloads/Dialnet-ElCodigoHammingEnLaCuartaRevolucionIndustrial-8080451.pdf

Rubio Silvera, M. (2019). Técnicas de ciberataque y su relación con el espionaje industrial y económico. (En línea). Universidad Nacional Abierta y a Distancia UNAD. Disponible en: https://repository.unad.edu.co/handle/10596/31843

Samaniego Zanabria, A. (2018). Evaluación de Algoritmos Criptográficos para mejorar la Seguridad en la Comunicación y Almacenamiento de la Información. (En línea). Universidad Ricardo Palma. Disponible en: http://repositorio.urp.edu.pe/handle/URP/1509

Sánchez Ávila, A. (2019). Hacking ético: impacto en la sociedad. (En línea). Repositorio Universidad Piloto de Colombia. Disponible en: http://repository.unipiloto.edu.co/handle/20.500.12277/4919

Sánchez Vega, Y., & Chinchilla Ruedas, K. (2020). Innovación en las asociaciones productivas de Ocaña: prácticas, limitaciones y retos. (En línea). Disponible en: http://repositorio.ufpso.edu.co/bitstream/123456789/461/1/33293.pdf

Sánchez-Paredes, E. (2021). Modelo de Gestión de la Seguridad de la Información adaptado a las Cooperativas de Ahorro y Crédito de la ciudad de Guayaquil. (En línea). Repositorio Dspace. Disponible en: http://181.39.139.68:8080/handle/123456789/1533

Seguridad y Privación de la Información-MINTIC (2016). Guía Técnica. (En línea). Ministerio de las Tecnologías y la Información. Disponible en: https://www.mintic.gov.co/gestionti/615/articles-5482_Guia_Seguridad_informacion_Mypimes.pdf

Solano, M., & Alpízar, R. (2019). Modelo para la preservación de documentos digitales.(En línea). Revista del Archivo Nacional, 83(1-12), 129-182.Disponible en: http://dgan.go.cr/ran/index.php/RAN/article/view/453

Suárez Padilla, Y. (2015). Análisis y diseño de un sistema de gestión de seguridad informática en la empresa aseguradora Suárez Padilla & Cía. Ltda., que brinde una adecuada protección en seguridad informática de la infraestructura tecnológica de la organización. (En línea). Repositorio Universidad Nacional Abierta y a Distancia UNAD. Disponible en: https://repository.unad.edu.co/handle/10596/3777

Sweigart, A. (2013). Hacking Secret Cipherswith Python (pp. 378-420). Create Space. (En línea). 1stEdition. Disponible en: https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.645.5528&rep=rep1&type=pdf

Tamayo Reinel, A. (2020). Adaptación de una metodología para el análisis y gestión de riesgos informáticos para organizaciones del sector salud en Colombia. (En línea). Repositorio Universidad Nacional Abierta y a Distancia UNAD. Disponible en: https://repository.unad.edu.co/handle/10596/35868

Toapanta, T., Campuzano, M., &Gallegos, M. (2020). An Approachof Security Modelto Mitigate Riskof Cyberattackson Public Institutions in Ecuador. (En línea). In Proceedings of the 2020 the4th International Conference on Information System and Data Mining (pp. 51-57). Disponible en: https://pure.ups.edu.ec/es/publications/an-approach-of-security-model-to-mitigate-risk-of-cyberattacks-on

Torres Robles, A. (2016). La importancia de realizar un análisis de riesgo en las empresas. Trabajo de Grado, Universidad Piloto de Colombia. Disponible en: http://repository.unipiloto.edu.co/handle/20.500.12277/2728

Urrego Urrego, J. (2019). Método criptográfico para cifrar información usando los estados cuánticos de polarización de fotones individuales. (En línea). Repositorio Institucional ITM. Disponible en: https://repositorio.itm.edu.co/bitstream/handle/20.500.12622/2090/Rep_Itm_mae_Urrego.pdf?sequence=1&isAllowed=y

Vásquez Mejía, I., & Valencia Mesa, A. (2019). Límites de la normatividad en materia de comercio electrónico en Colombia. (En línea). Repositorio Universidad EAFIT. Disponible en: https://repository.eafit.edu.co/handle/10784/13825

Veglia, E. (2018). Sistemas de comunicación robustos para infraestructuras avanzadas de medición de energía implementadas sobre PLC (power line communications). (En línea). Tesis de Maestría, Universidad Nacional del Nordeste. Disponible en: https://repositorio.unne.edu.ar/handle/123456789/27884

Vélez Serrano, S., & Vélez Vintimilla, A. (2021). Propuesta de Plan estratégico para la empresa PROTIRES en la ciudad de Cuenca. (En línea). Repositorio Dspace de la Universidad del Azuay. Disponible en: https://dspace.uazuay.edu.ec/handle/datos/11308

Vereau, V. (2021). Los delitos informáticos y su relación con la criminalidad económica. (En línea). Revista Ius et Praxis, (053), 95-110. Disponible en: https://revistas.ulima.edu.pe/index.php/Ius_et_Praxis/article/view/4995

Vergel, C. (2019). El conocimiento en agricultura sostenible y el interés ambiental en la zona rural del Municipio de Ocaña. (En línea). Repositorio RIDUM Principal. Disponible en: https://ridum.umanizales.edu.co/xmlui/handle/20.500.12746/3635

Villa Mesa, S. (2018). Impacto del riesgo cibernético en el segmento mipyme (En línea). Doctoral dissertation, Universidad EAFIT. Disponible en: https://repository.eafit.edu.co/handle/10784/12890

Zúñiga Arguedas, M. (2021). Modelo de gestión organizacional basado en la administración de servicios de ITIL 4, para la ejecución de los procesos técnicos operativos del programa de aprendizaje en línea de la UNED. (En línea). Repositorio Institucional de la Universidad de Costa Rica. Disponible en: https://www.kerwa.ucr.ac.cr/handle/10669/84491

Apéndice

Apéndice A. Estructura de la encuesta

Estructura de la Encuesta

Pregunta A. ¿Han tenido ataques informáticos en los dos (2) últimos años?

Si

No

Pregunta B. Si han sufrido ataques informáticos ¿éstos han detenido la operación del servicio de la empresa?

Si

No

Pregunta C. ¿Qué tipo de medio de tecnología utilizan en su empresa (Tablet, computadores, celulares)?

Tablet

Computador

Celular

Pregunta D. ¿Qué tipo de sistema operativo utilizan en la empresa?

Software libre

Linux

Mac OS

Windows (10, 8, 7)

Pregunta E. ¿Utilizan algún portal donde brindan sus productos o servicios?

Sí

No

Pregunta F. ¿Ha sufrido robo o secuestro de su información dentro de la empresa?

Sí

No

Pregunta G. ¿Han sufrido algún tipo de extorsión a causa de robo de información?

Sí

No

Pregunta H. ¿Actualmente cuentan con algún servidor propio?

Si

No

Pregunta I. ¿Cuentan con algún servicio de tercerización dónde monten su almacén de forma online?

Sí

No

Pregunta J. ¿Cuentan con personal idóneo dentro de la empresa para atender ataques informáticos?

Sí

No

Pregunta K. ¿Si no cuentan con personal idóneo dentro de la empresa para atender ataques informáticos buscan una persona fuera de la empresa para atender esa clase de inconvenientes?

Sí

No

Pregunta L. Cuándo sufren algún ataque informático dentro de la empresa ¿han conseguido en Ocaña apoyo para atender dicho problema (algún grupo de especialistas en el tema o la Universidad Francisco de Paula Santander)?

Sí

No

Pregunta M. ¿A usted, como empresa le gustaría que la Universidad Francisco de Paula Santander-Ocaña, desde el observatorio de innovación tecnológica y en conjunto con el programa de ingeniería de sistema se le brindara apoyo y seguimiento a los incidentes de seguridad informática que presente la empresa?

Sí

No

Tal vez

Apéndice B. Estructura de la entrevista a expertos

1. ¿Considera usted que las políticas a nivel general se encuentran orientadas a mejorar la calidad del servicio en las organizaciones y asegurar la operación de los mismos?

SI NO

2. ¿Con respecto al sistema planteado para realizar un seguimiento a los controles y respuesta a incidentes lo considera adecuado?

SI NO

3. ¿Con respecto al sistema planteado creería usted que si está lo suficientemente estructurado para mitigar los riesgos informáticos en las empresas?

SI NO

4. ¿Cuál de estas fases cree usted que está mal estructurada y viabilizada? Si su respuesta es alguna de las fases, ¿Por qué? _____

Fase 1. Análisis del riesgo

Fase 2. Clasificación del riesgo

Fase 3. Reducción del riesgo

Fase 4. Control del riesgo

Ninguna

5. ¿Qué observación puedes dar para mejorar el sistema planteado?

_____

Apéndice C. Resultados entrevista a empresa

Guía para el sistema de gestión del riesgo de seguridad informática para beneficiar la operación del servicio en empresas ubicadas en Ocaña norte de Santander

Nombre y Apellido *

Luzelis Hernandez

Nombre de la empresa *

Transportadora Regional S.A

Municipio de la Empresa *

Ocaña

1 ¿Considera usted que las politicas a nivel general se encuentran orientadas a mejorar la calidad del servicio en las organizaciones y asegurar la operación de los mismos?

- (●) Sí
- ( ) No

2 ¿Con respecto al sistema planteado para realizar un seguimiento a los controles y respuesta a incidentes lo considera adecuado?

- (●) Sí
- ( ) No

3 ¿Con respecto al sistema planteado creería usted que si está lo suficientemente estructurado para mitigar los riesgos informáticos en las empresas?

- (●) Sí
- ( ) No

4 ¿Cuál de estas fases cree usted que está mal estructurada y viabilizada?

Ninguna ▾

¿Si su respuesta es alguna de las fases porque?

5 ¿Qué observación puedes dar para mejorar el sistema planteado?

Ser muy cuidadosos en la etapa del análisis de riesgo, en especial en el robo y fuga de la información, que es unos de los principales problemas que se presente en las empresas a nivel informativo.

Apéndice D. Resultados encuesta a ingenieros

Guía para el sistema de gestión del riesgo de seguridad informática para beneficiar la operación del servicio en empresas ubicadas en Ocaña norte de Santander

Nombre y Apellido *

Ronaldo Duran Amaya

1 ¿Considera usted que las políticas a nivel general se encuentran orientadas a mejorar la calidad del servicio en las organizaciones y asegurar la operación de los mismos?

- (●) Sí
- ( ) No

2 ¿Con respecto al sistema planteado para realizar un seguimiento a los controles y respuesta a incidentes lo considera adecuado?

- (●) Sí
- ( ) No

3 ¿Con respecto al sistema planteado creería usted que si está lo suficientemente estructurado para mitigar los riesgos informáticos en las empresas?

- (●) Sí
- ( ) No

4 ¿Cuál de estas fases cree usted que está mal estructurada y viabilizada?

Ninguna

¿Si su respuesta es alguna de las fases porque?

5 ¿Qué observación puedes dar para mejorar el sistema planteado?

Ningina, creo que el modelo del sistema esta estructurado de una manera correcta, que si se ejecutan en la manera planteada, tendra un gran impacto positivo a nivel organizacional

Guía para el sistema de gestión del riesgo de seguridad informática para beneficiar la operación del servicio en empresas ubicadas en Ocaña norte de Santander

Nombre y Apellido *

WILLIAM FERNANDO ARENAS ALVAREZ

1 ¿Considera usted que las políticas a nivel general se encuentran orientadas a mejorar la calidad del servicio en las organizaciones y asegurar la operación de los mismos?

- (●) Sí
- ( ) No

2 ¿Con respecto al sistema planteado para realizar un seguimiento a los controles y respuesta a incidentes lo considera adecuado?

- (●) Sí
- ( ) No

3 ¿Con respecto al sistema planteado creería usted que si está lo suficientemente estructurado para mitigar los riesgos informáticos en las empresas?

- (●) Sí
- ( ) No

4 ¿Cuál de estas fases cree usted que está mal estructurada y viabilizada?

Ninguna

¿Si su respuesta es alguna de las fases porque?

5 ¿Qué observación puedes dar para mejorar el sistema planteado?

Guía para el sistema de gestión del riesgo de seguridad informática para beneficiar la operación del servicio en empresas ubicadas en Ocaña norte de Santander

Nombre y Apellido *

Leandro Quintero Navarro

1 ¿Considera usted que las políticas a nivel general se encuentran orientadas a mejorar la calidad del servicio en las organizaciones y asegurar la operación de los mismos?

- (●) Sí
- ( ) No

2 ¿Con respecto al sistema planteado para realizar un seguimiento a los controles y respuesta a incidentes lo considera adecuado?

- (●) Sí
- ( ) No

3 ¿Con respecto al sistema planteado creería usted que si está lo suficientemente estructurado para mitigar los riesgos informáticos en las empresas?

- (●) Sí
- ( ) No

4 ¿Cuál de estas fases cree usted que está mal estructurada y viabilizada?

Ninguna

¿Si su respuesta es alguna de las fases porque?

5 ¿Qué observación puedes dar para mejorar el sistema planteado?

El sistema es muy bueno, si se implementa de la mejor manera. Las empresas ocañeras deben ponerse al día con la tecnología para no tener en un futuro inconvenientes con sus datos y activos.

Guía para el sistema de gestión del riesgo de seguridad informática para beneficiar la operación del servicio en empresas ubicadas en Ocaña norte de Santander

Nombre y Apellido *

Danilo Andrés Ascanio lobo

1 ¿Considera usted que las políticas a nivel general se encuentran orientadas a mejorar la calidad del servicio en las organizaciones y asegurar la operación de los mismos?

- ○ Sí
- ◉ No

2 ¿Con respecto al sistema planteado para realizar un seguimiento a los controles y respuesta a incidentes lo considera adecuado?

- ◉ Sí
- ○ No

3 ¿Con respecto al sistema planteado creería usted que si está lo suficientemente estructurado para mitigar los riesgos informáticos en las empresas?

- ◉ Sí
- ○ No

4 ¿Cuál de estas fases cree usted que está mal estructurada y viabilizada?

Ninguna

¿Si su respuesta es alguna de las fases porque?

5 ¿Qué observación puedes dar para mejorar el sistema planteado?