Análisis costo - beneficio de la implementación de gestión de riesgos de la seguridad de la información en las empresas de Colombia

Elaborado por:

Jessica Paola Quintero Sopo

Natalia Palacio Arrieta

Yenny Paola Franco Gutiérrez

Universidad Ean

Especialización en Gerencia de Procesos y Calidad

Seminario de Investigación de Postgrado

Bogotá

07/03/2023

CONTENIDO

LISTADO DE TABLAS

LISTADO DE FIGURAS

LISTA DE GRÁFICOS

LISTA DE ANEXOS

1. RESUMEN

Debido al aumento de los ataques cibernéticos, muchas empresas colombianas se han visto afectadas en cuanto a la seguridad de la información a través del robo de datos confidenciales, contraseñas poco seguras donde se facilita el ingreso de los delincuentes, distintas modalidades de robo donde las información corporativa y personal es vulnerable. Esto debido a que durante los últimos años el manejo que se la ha dado a la información se ha realizado por medios digitales, pero estos han sido un riesgo para las empresas colombianas porque no se cuenta con las estrategias o herramientas que permitan reaccionar a un ataque cibernético, recuperarse del ataque o prevenirlo.

Por consiguiente, la investigación presenta como objetivo determinar si la implementación de la gestión de riesgos en seguridad informática genera beneficios o costos a nivel empresarial en Colombia.

Palabras Clave: Seguridad, Información, Riesgo, Empresa, Gestión

2. PROBLEMA DE INVESTIGACIÓN

La llegada de la cuarta revolución industrial a Colombia ha incluido un importante avance tecnológico lo cual ha implicado una modernización de nuevos desarrollos y capacidades tecnológicas, sin embargo, esto también ha conllevado casi de forma paralela el incremento durante los últimos años de los ciberdelitos causando un impacto de coste económico en las empresas ya que no solo trasciende a pérdidas económicas, sino también afectaciones productivas, implicaciones legales por perdida de información exclusiva y data sensible, incapacidad en la prestación de servicios , entre otros.

Por otro lado, según los resultados de un estudio realizado y expuesto por el Tanque de Análisis y Creatividad de las TIC sobre los modos del cibercrimen durante los años 2019 y 2020 se presentaron las cifras, modalidades y tendencias de ciberdelito que se encuentran enfrentando las empresas colombianas y los ciudadanos mostrando un incremento del 54% en las denuncias (Seguridad Aplicada al Fortalecimiento Empresarial [SAFE], 2021, p. 7).

Por otra parte, se evidencia en el resultado del informe correspondiente a los años 2021 y 2022 que fue desarrollado por el Tanque de Análisis y Creatividad de las Tic Tac, donde se describe que se revelaron 46.527 acontecimientos de ciberdelitos a finales de noviembre del 2021 en el país, en el cual se registra un crecimiento del 21% respecto al año 2020. (Seguridad Aplicada al Fortalecimiento Empresarial [SAFE], 2021, p. 13). De acuerdo con esto la seguridad cibernética se ha posicionado con mayor firmeza en las compañías haciéndose indispensable que estas identifiquen, evalúen y controlen los riesgos que se pueden presentar ante estas nuevas modalidades de robo con el fin de evitar la materialización de estos riesgos.

En estudios previos se ha identificado que durante los últimos tiempos han existido investigaciones enfocadas al riesgo definiendo su terminología, naturaleza, componentes y acciones de tratamiento (Tamayo y Gonzalez, 2020). Sin embargo, no tomó mucha fuerza en las empresas hasta la adopción del pensamiento basado en riesgos propuesta en la ISO 9001:2015; llevando a las empresas a crear actividades, procesos y/o áreas de la gestión de riesgos, incurriendo en nuevos costos dentro de los procesos empresariales internos. Lo que llevo a generar diferentes opiniones en las empresas y sus colaboradores

debido a que mantener un área dentro de la organización enfocada en riesgos es costoso. Así mismo, Colombia es uno de los países que ha presentado un gran avance de la tecnología, ya que se ha observado un porcentaje considerable del uso de dispositivos móviles, computadores, redes sociales, redes inalámbricas Wifi, correos electrónicos, entre otros. Esta aceptación de la tecnología ha sido importante para el desarrollo tecnológico del país. Sin embargo, en los últimos años varias empresas han sido víctimas de ciberataques, una tendencia que ha afectado a todas las industrias del país, empresas como Audifarma, Sanitas, Carvajal, Keralty y la Fiscalía General de la Nación han sufrido de hackeo en los últimos meses, los riesgos que se han presentado son ataques cibernéticos externos en infraestructura tecnológica, afectaciones en los activos y filtración de la información privada de las organizaciones (Vargas, 2023).

Por otro lado, actualmente en Colombia se encuentran riesgos para el negocio donde los problemas se relacionan con la digitalización acelerara, estos problemas van desde la obsolescencia de habilidades como de los riesgos de ciberseguridad y privacidad de los datos, estos riegos se han visto como una amenaza comercial por 3 de 4 (75%) de las empresas en Colombia (Business Of Marsh Mclennan [MMC],2022 p. 3).

Por otra parte, los ataque evolucionan y por ende los desarrollos en ciberseguridad por eso las empresas colombianas han implementado las medidas de seguridad con el fin de estructurar un mejor servicio, como bloqueo de páginas, instalaciones de antivirus, monitoreo de equipos con el fin de evitar robos, sin embargo, la temática de la ciberseguridad en algunas empresas aún no ha cobrado la importancia necesaria por lo que ha hecho que se identifique su vulnerabilidad y se presenten los casos de robo o ataques cibernéticos, así mismo, se ha evidenciado que las empresas no implementan los sistemas de gestión en ciberseguridad, no tienen conocimiento de las herramientas o instrumentos adecuados para la gestión y tratamiento de los riesgos, incluso, desconocen las consecuencias que pueden tener al enfrentarse a un ataque cibernético, los impactos financieros, los efectos que pueden ocasionar, no establecen las herramientas para fortalecer el recurso humano de acuerdo con políticas, prácticas y estándares y/o requisitos de la ciberseguridad y de la y no desarrollan y establecen procesos fuertes para el sistema de seguridad de datos e información.

El presente proyecto se soporta por medio de la siguiente pregunta de investigación: ¿El sistema de gestión de riesgos en seguridad informática en las organizaciones es un costo o un beneficio?

3. OBJETIVOS

3.1 Objetivo general

Determinar si la implementación de la gestión de riesgos en seguridad informática genera beneficios o sobre costos a nivel empresarial en Colombia.

3.2 Objetivos específicos

- Establecer las ventajas de la implementación de la gestión de riesgos de seguridad informática.
- Identificar los riesgos potenciales que afectan la seguridad informática.
- Evaluar los costos de la materialización de los riesgos potenciales de seguridad la informática.
- Determinar los costos de implementación de la gestión de riesgos de seguridad informática.

4. JUSTIFICACIÓN

Durante esta última década la gestión de riesgos en las industrias se ha robustecido con la llegada en la ISO 9001:2015 del pensamiento basado en riesgos, llevando a invertir montos grandes en esta gestión y poniendo en duda si todo este capital tiene una retribución igual o mayor en beneficios a la compañía. Actualmente se pueden encontrar en Colombia muchas empresas con áreas de riesgos bien consolidadas, donde generan mejoras y actualizan su gestión en riesgos día a día. Sin embargo, también se pueden encontrar empresas en diferentes sectores de la industria con gestión de riesgos débiles o nulas sin afectar la cadena de valor y su promesa de valor frente al cliente.

Por otro lado, los hackeos y las diferentes afectaciones de la seguridad informática en diferentes y grandes compañías fueron de gran relevancia durante el año 2022, afectando a miles de colaboradores de compañías, clientes y usuarios. Con esta investigación se busca determinar qué tan viable y beneficioso es implementar una gestión de riesgos de la ciberseguridad en las empresas en Colombia. Ampliando el conocimiento de los estudiantes, profesionales interesados y autores de la relación de los costos incurridos, los

beneficios y un análisis de las problemáticas que se han presentado en Colombia durante los últimos años en cuanto a temáticas de seguridad cibernética.

Esta investigación ayudara a los gerentes y directivos de las empresas en Colombia a tomar decisiones sobre el manejo interno que se debe dar frente a la administración de riesgos de seguridad informática; creando instrumentos de análisis adecuados que ayuden a tomar la decisión fundamentado en el estudio de los beneficios vs costos de ejecución de la gestión de riesgos de ciberseguridad. Al tomar decisiones adecuadas del manejo de la ciberseguridad, mitigara a nivel social la vulnerabilidad de los datos otorgados a las empresas.

Campo de investigación: Ciencia, Tecnología e Innovación

Grupo de investigación: Tecnológico Ontare

Línea de investigación: Tecnología de la información y comunicaciones

5. MARCO TEORICO

5.1 ¿Qué es la seguridad informática?

A medida que la tecnología avanza de una manera acelerada, muchas compañías tanto privadas como de orden público están sometidas cada vez más a la tecnología informática con el objeto de llevar a cabo sus actividades esenciales, no solo en la administración del capital económico y humano, sino también para la adecuada prestación de sus servicios. Dicho crecimiento tecnológico ha representado un importante progreso y a su vez ha generado un creciente número de retos respecto a la dependencia tecnológica, vulnerabilidad de la información y aumento en la protección de los sistemas que administran datos, ya que el daño a estos puede ocasionar graves pérdidas a cualquier sociedad y/o gobierno.

Actualmente los sistemas informáticos, el internet y la reserva de información y acceso de esta en la nube de cómputo son claves para almacenar, administración y ejecución de datos personales y corporativa, volviéndose la finalidad para aquellos que la pretenden hurtar, adulterar o destruir, buscando perjudicar a los dueños. Debido a que las organizaciones y las personas generan como una costumbre sobre la forma de mantención de en esta información, de tal modo que la mínima adulteración o falla termina afectándolos grotescamente, tanto a nivel colectivo como a nivel individual. (Ospina y Sanabria, 2020)

Así mismo, existen enormes implicaciones en cuanto a la información que se maneja mediante los E-Mails, redes sociales, bases de datos, entre otros, sufran ataques, daños, pérdidas, los cuales no solo representan la vulneración de la integridad de una persona sino también las consecuencias que se pueden presentar por carencia de información estratégica y funcional de las compañías, y afectación en la prestación de servicio según corresponda.

Debido a esto se incrementa la consideración de la seguridad en la información, que inicia para tomar precauciones en la protección de hardware, infraestructura y software, neutralizando las probables amenazas cibernéticas, y desarrollando estrategias para reaccionar ante cualquier ataque. (Reyna y Olivera, 2017)

En el año 2010 la ITU Unión Internacional de Telecomunicaciones presenta la definición de la Ciberseguridad como un grupo de métodos, políticas, técnicas, direccionamientos de gestión de riesgos, acciones, capacitación, conceptos de seguridad, seguros, buenas prácticas, salvaguardas de seguridad y ciencias que pueden emplearse para salvaguardar el patrimonio de una organización e individuos en el ambiente cibernético. El patrimonio de la corporación y los consumidores representan los ordenadores informáticos conectados, los servicios, las aplicaciones, las redes de comunicación, los usuarios, y el total de la información difundida y/o salvaguardada en el ambiente cibernético. (Unión Internacional de Telecomunicaciones, 2010, p. 748)

5.2 Historia de la gestión de riesgos

La primera vez que se empezó a hablar de Gestión de Riesgos empresariales fue en la segunda guerra mundial, donde surgen algunos términos, pero como tal la disciplina no. En 1974 se crea el Comité de Basilea por los presidentes de los principales bancos de los países que conforman el G-10, el cual tiene como objetivo supervisar los bancos, estableciendo condiciones mínimas que una institución bancaria debe tener con el fin que sea sostenible en el tiempo y es en este momento se empiezan a evaluar los riesgos que influyen en gran magnitud en la sostenibilidad de los bancos. (Buchtik, 2012).

En 1985 surge COSO (Committee of Sponsoring Organizations of the Treadway Commission) el cual busca contrarrestar el fraude corporativo, basados en el control interno. (Abu, Massadeh y Bshayreh, 2023)

Pero es en el año 1986 donde nace el primer instituto de gestión de riesgos, llamado “Institute of Risk Managment (IRM), el cual sigue vigente en la actualidad. Con la creación de este instituto se empiezan a escribir pequeñas guías y artículos de riesgos. En 1995 se construyen los Estándares nacionales de gestión de riesgos Aus/NZ Risk creados y adoptados en países como Canadá, Japón y Reino Unido. (Buchtik, 2012)

COSO ERM (Framework de Gestión Empresarial de Riesgos) surge en el año 2004, la segunda versión de COSO se introducen los conceptos de control interno a las tareas

que se deben realizar para la correcta ejecución de riesgos, implicando a todas las personas de las organizaciones. (Abu, Massadeh y Bshayreh, 2023)

En el año 2005 se renueva la normatividad ISO 9001:2015, el cual es un estándar internacional del sistema de gestión de calidad de los diferentes sectores empresariales, estableciendo un enfoque en la gestión de riesgos. Puche, et al. (2021) indica que la renovación de esta norma con lleva a que en los siguientes años se expanda la gestión de riesgos en las diferentes industrias, debido a que las empresas que se quieran certificar o recertificar con altos estándares de calidad deben cumplir unos parámetros mínimos de gestión de riesgos.

En el 2007 y 2008 ocurre la crisis financiera, lo que hace que las industrias adopten la gestión de riesgos como una de las estrategias para reducir el impacto de esta crisis y crear planes de acción para que no vuelva a ocurrir con una magnitud grande en el futuro. (Casares, 2021)

Desde el 2005 a hoy se ha robustecido en las compañías que hacen parte del sector financiero la gestión de riesgos y se ha adoptado en los diferentes sectores de las industrias, construyendo áreas con personas especializadas en la identificación, evaluación, tratamiento y monitoreo de los riesgos.

En el año 2020 la pandemia aceleró el conocimiento de la gestión de riesgos, debido a las grandes problemáticas presentadas como consecuencia de la aparición del COVID -19 a nivel internacional.

En el presente se encuentra una gran variedad de instituciones, libros y artículos que hablan de la correcta ejecución de los riesgos en las empresas de los diferentes sectores; en la actualidad es un tema que sigue en construcción y expansión dentro de las organizaciones.

5.3 Tipos de ataques cibernéticos

Los inconvenientes en la ciberseguridad se presentan dado que no es posible identificar los bandos atacantes, ya que esto puede involucrar contiendas entre gobiernos, partidos políticos, gremios, etc. Además, la ciberseguridad se ha convertido en un asunto global debido a que el ciberespacio no se encuentra establecido por algún país en específico por lo cual es un asunto que no discriminación ni presenta fronteras.

De acuerdo con lo descrito en el libro *"Ciberseguridad: Los datos tienen la respuesta" Pagina 25* "Un ataque informático resulta de la motivación de un personaje que ejecuta al menos un método sobre una o varias vulnerabilidades de un punto objetivo; dependiendo del escenario, el atacante puede realizar varios tipos de ataques informáticos".

De acuerdo con los autores Urcuqui, C. C. y Navarro C. A. (2022) estos tipos de ataques se pueden clasificar en:

Pasivos: Son los ataques donde no se relaciona directamente un atacante con el objetivo. Un ejemplo es cuando se monitorea un tráfico de la red y un flujo de datos los cuales son transmitidos en una red de computadores.

Activos: Estos ataques generan una acción que conlleva a la suspensión de un mensaje o servicios de un sistema o quebrantan los métodos de seguridad digital, dentro de los cuales se encuentran los ataques de secuestros de sesión *(sessions hijacking)*, inyección SQL *(SQL injection)* y los correspondientes a la denegación de servicios (*Denegation of Services DoS)*.

Cercano: En este tipo de ataque a diferencia de los anteriores el atacante sostiene una cercanía física al objetivo, como por ejemplo los casos de los ataques realizados a través de la ingeniería social, como lo son: búsqueda en la basura (*dumpster diving*), escuchar a escondidas (*eavesdropping*) y Mirar por encima del hombro (*shoulder surfing*).

Explotación de Privilegios: Se presenta cuando algunos empleados o personas con algún tipo de privilegios al interior de una organización forman parte de un grupo de atacantes, de allí el peligro que genera ya que cuentan con una alta disposición de acceso al perímetro del propósito de ataque.

Distribuido: En este ataque se genera una alteración del software y/o hadware antes de su adquisición o instalación por el usuario. (Urcuqui, y Navarro, 2022a)

Hoy en día existen una amplia gama de familias (Tabla 1) pertenecientes al software malicioso conocido como *malware* el cual se caracteriza por causar fallas a un computador, servidor, teléfono inteligente, u otro dispositivo electrónico en que la gran mayoría de los delincuentes cibernéticos utilizan principalmente por activismo político o fines de lucro.

Tabla 1. Gama de Familia Malware.

FAMILIA	CARACTERISTICA
Gusanos de Red	Emplea redes globales como también redes locales y con el fin de distribuirse, propagándose velozmente y tendiendo a acabar con los recursos de la máquina que atacan.
Troyanos	Incorpora una amplia gama de programas que realizan movimientos sin darse cuenta el usuario, razón por la cual no cuentan con su consentimiento, en este se agrupan los datos y los envían a los delincuentes los cuales alteran o destruyen estos datos de manera delictiva.
Spyware	Este software permite obtener la información de una compañía o usuario de forma no autorizada, en el cual se obtienen datos sobre las actividades del usuario, software instalado, velocidad de la conexión, contenido del disco duro, calidad, entre otros.
Adware	Está vinculado con la propaganda que se transmite al usuario, gran parte de estos programas se instalan mediante un software de distribución gratuita.
Rootkit	Recopilación de programas utilizados por una persona con el fin de evitar ser detectada, mientras logra obtener acceso a un computador no autorizado, después de que se logra instalar el Rootkit como administrador del sistema se genera un acceso igual al del usuario.

Fuente: Urcuqui, C. C. y Navarro C. A. (2022b).

Los Botnets hacen parte de los ataques informáticos, estos se componen por equipos comprometidos ilegalmente, los cuales se denominan zombies o *bots* utilizados para diversos fines entre los cuales se encuentran: ataques de degeneración de servicios distribuidos conocido comúnmente como robo de información, minado ilegal de criptomonedas, *Distribuited Denial of Services*, DDoS, *spam*. Estos mecanismos son complejos de erradicar debido a que mediante técnicas innovadoras diariamente los ciberdelincuentes tienden a aumentar aún más la red volviéndola mucho más madura y fuerte. (Urcuqui, y Navarro, 2022c)

Otro de los ataques más populares son el DoS y DDoS, tiempos pasados se conocían los ataques DoS, los cuales estaban dirigidos para deshabilitar la disponibilidad de un recurso, dificultando así el ingreso a los usuarios durante un lapsus de tiempo. Los recursos a los cuales está dirigido un ataque DoS incluyen desde las redes normales o empresariales hasta los nodos de procesamiento únicos o grupos de dispositivos, en este

tipo de ataques DDoS el delincuente cibernético sincroniza y controla los nodos computacionales con el fin de rechazar el servicio a la víctima. (Urcuqui y Navarro, 2022d)

También existe el Cryptojacking el cual consiste en ejecutar en un segundo plano, debido a que no requiere de archivos binarios para contagiar un equipo, lo puede hacer mediante uso de *malvare,* cuenta con una amplia versatilidad en los vectores de transmisión del ataque, mediante uso de llamadas al sistema utiliza procesos aprobados y también se presenta como multiplataforma. Suele evitar los mecanismos causando un tráfico de red pasando desapercibido en una grande red.

5.4 Histórico de ataques cibernéticos

Las principales organizaciones en seguridad informática, de acuerdo con sus informes los cuales han revelado que el 2017 fue el año de los ataques cibernéticos más sofisticados y potentes en estos últimos tiempos, los cuales han desencadenado enormes desastres económicos, sociales, políticos, financieros a nivel global. (Conner, 2018)

De acuerdo con el informe emitido por Sonic Wall de amenazas cibernéticas presentadas durante el 2017, en el cual notifica el reporte de 9.200 millones de ataques a nivel global de tipo malware, representando este un 18,4% anual de ataques cibernéticos en el mismo año en todo el mundo, así mismo fueron identificadas 12.500 nuevos tipos de vulneraciones y exposiciones.

En Estados Unidos para el año 2020 hubo aproximadamente 200.000 millones de conexión de dispositivos con tan solo un 50% de presupuesto asignado para los servicios de ciberseguridad, de acuerdo a esto las empresas pequeñas estuvieron expuestas a un 43% de posibles ciberataques, han sufrido ataques basados en la web el 64% de las empresas, los ataques de suplantación de identidad e ingeniería social han representado el 62%, los ataques causados por códigos maliciosos y redes de bot han representado el 59% y las negaciones de servicio en un 51%. (Miranda et.al., 2021, p. 734 - 749)

Así mismo, las estadísticas y cifras en Colombia fueron desfavorables durante el mismo periodo, de acuerdo con lo informado por el periódico portafolio el 59% de las compañías colombianas disminuirían los fondos destinados para los productos y/o actividades referentes a seguridad informática. (Cano, 2017).

Colombia se ubica en el tercer país con mayor número de ataques cibernéticos en América Latina, después de Brasil y México para el año 2022, esto ha encendido las alarmas con el fin de priorizar la incorporación de una gestión individual y colectiva con el fin de establecer un sistema de seguridad cibernética y así lograr mitigar los innumerables riesgos a los cuales nos estamos enfrentando. (Rey, 2023).

De acuerdo con el informe emitido el 16 de diciembre de 2022 por el Ministerio de Tecnologías de la Información y las Comunicaciones mediante el COLCERT – Equipo de respuestas a Emergencias Cibernéticas de Colombia, fueron recibidos desde el mes de noviembre 36 reportes de sucesos de ataques cibernéticos, entre los cuales 19 de estos se presentaron por falsificación de sitios web y usurpación de dominios de E-mails con un estimados de 8 denuncias. El restante de los ataques informados se efectuó mediante actuaciones de responsabilidades de cuentas, información secuestrada o ransomware, aplicaciones web vulneradas, y negaciones de servicios.

Dentro estas 36 arremetidas informáticas, las entidades públicas de orden nacional fueron impactadas por 18 de estos, de orden territorial 5, y las restantes 18 corresponden a compañías y empresas del sector privado (Ministerio de Tecnologías de la Información y las Comunicaciones,2022)

5.5 Gestión de riesgos en la seguridad informática

Conservar la información de una manera segura ha cobrado una gran importancia cada vez más, dado a que prácticamente el adecuado funcionamiento de cualquier compañía que emplee moderna tecnología para el almacenamiento, procesamiento y recopilación de la información conlleva a que este proceso ejecute un análisis frecuente de los riesgos de la información permitiendo así identificar las principales amenazas a esta seguridad y la vulnerabilidad que pueda tener cualquier sistema, por lo tanto se deben implementar las acciones correctas y efectivas necesarias con el fin de impedir la materialización de estos riesgos y la mitigación de los mismos.

Por tal razón estas actividades deben ser llevadas a cabo de manera continua ya que las compañías constantemente se encuentran expuestas a múltiples riesgos de incidentes que alteran la seguridad informática, lo cual no solo genera daños inesperados e impredecibles sino que también detonan daños importantes y pérdidas financieras, El

llevar a cabo la gestión de riesgos tiene por objeto reducir la probabilidad de que se presenten esos posibles eventos de seguridad como la severidad en sus procesos empresariales, el llevar a cabo una eficaz gestión del riesgo minimiza estas amenazas y por lo tanto optimiza el éxito de las empresas. (Palko, et al.2023, p 13).

5.6 Normatividad de gestión de riesgos y seguridad de la información

A lo largo de la historia se han creado normativas con estándares internacionales relacionadas a la administración de riesgos y seguridad de la información, estas son actualizadas con mejoras en la gestión, teniendo en cuenta los principales cambios externos e internos en las organizaciones; Las principales normas son:

- ISO 31000: Esta normativa implanta los criterios que debe tener un Sistema de Gestión de Riesgos, la última versión es del año 2018. Es importante resaltar que esta normativa no indica como se puede realizar la gestión de riesgos, pero si indica que se requiere, como lo deja ver los autores Ramírez y Ortiz (2011).
- ISO 9001: Esta normativa establece en el Sistema de Gestión de Calidad los criterios y su relación con riesgos empieza en la versión 2015, donde se incluye el pensamiento basado en riesgos. (López, 2016)
- ISO 55000: Esta compuesta por tres normas que estableces un sistema de Gestión de Riesgos de Activos, tanto tangibles como intangibles:
    1. Gestión de activos ISO 55000: Descripción general, principios y terminología.
    2. ISO 55001: Requerimientos.
    3. ISO 55002: Directrices para la aplicación. (Hasting, 2015)
- ISO 27001: Esta normativa establece los criterios para ejecutar un sistema de Gestión de Seguridad de la Información (SGSI); busca proteger los datos que en su gran mayoría se encuentran guardados de forma digital, teniendo presente que de los activos que más valor tiene en las organizaciones son los datos, debido a que la pérdida, indisponibilidad o fuga de la información puede traer repercusiones muy graves, como lo expone Tonysé de la Rosa (2021)

La implementación de la Gestión de Riesgos de Seguridad de la información debe estar fundamentadas en los criterios de las normas anteriores, de manera que los

resultados en las diferentes organizaciones logren estar alineados a los estándares internacionales.

5.7 Recursos necesarios para la ejecución de la gestión de riesgos de ciberseguridad

Autores como Gómez, et al. (2005) afirman que el recurso financiero es fundamental en la ejecución de la gestión de riesgos de ciberseguridad, debido a que se necesita adquirir diferentes elementos que suplan servicios de tecnología de la información que respalden los controles y planes de acción asociados al tratamiento de los riesgos evidenciados en la gestión. Por lo cual es necesario utilizar sistemas de costeo basado en actividades.

También se debe tener en cuenta que es indispensable otros recursos, como tiempo, colaboradores con conocimientos especializados en riesgos y ciberseguridad, computadores con programas ofimáticos y/o software especializado en riesgos para el registro de información. (Calder, 2017)

6. METODOLOGIA

Primer Nivel

6.1. Enfoque, alcance y diseño de la investigación

El alcance y enfoque para la investigación es de tipo cuantitativa, transversal, correlacional y no exploratoria.

- Cuantitativa: El estudio de la investigación se va a desarrollar a través de mediciones numéricas.
- Transversal: Se realizará debido a que solo hay un momento de recolección de datos debido a que se realizará en un solo tiempo y no se realizará evaluación de su evolución.
- Correlacional: Se revisarán los resultados y la relación entre las variables de la investigación.
- No experimental: No existirá manipulación de las variables, solo se tendrá en cuenta su comportamiento.

Por otro lado, en cuanto al diseño de la investigación se realizará de la siguiente manera;

1. Análisis del tiempo de implementación de un sistema de gestión de riesgo en seguridad informático.

2. Diagnostico cuantitativo de costos por implementación del sistema, y costos excesivos por materialización de riesgos
3. Identificación y análisis del nivel de importancia e impacto de los riesgos de ciberseguridad dentro de las organizaciones colombiana.
4. Análisis de la implementación de herramientas tecnológicas e aplicación de normatividad legal en cuanto la seguridad de la información.

6.2. Definición de Variables

Las variables que se tendrán en cuenta para la investigación son las siguientes:

Tabla 2. Determinación de variables

Variable	Definición Conceptual	Definición Operacional
Tiempo	Magnitud que se encarga de medir la duración del restablecimiento de las actividades después de un ciber ataque.	La unidad de medida para esta variable serán las semanas.
Costo de la implementación del sistema de gestión de riesgos	Cálculo monetario determinado para la implementación y gestión de los riesgos de ciberseguridad.	La unidad de medida será en pesos se determinará por el número de empleados que tienen en la organización para analizar los riesgos y el salario de estos.
Impacto de la materialización de los riesgos de ciberseguridad	Nivel de impacto de los riesgos que se materializaron en las empresas que presentaron ciberataques	Este nivel de impacto se determinará en los siguientes niveles 1 menor, 2 moderado, 3 mayor.
Importancia de la ciberseguridad en las organizaciones colombianas	El nivel de importancia y prioridad de la implementación del sistema de gestión de riesgos de ciberseguridad en las empresas colombianas	Este nivel de importancia se determinará en los niveles 1 bajo, 2 medio, 3 alto.
Herramientas tecnológicas	Determinar si dentro de las organizaciones se dispone de las herramientas o dispositivos que protejan la información	Se medirá a través de la escala de medición entre 1 a 5, donde 1 es nunca, 2 es ocasionalmente, 3 es siempre.

Fuente: Elaboración propia

Tabla 2. Determinación de variables (continuación)

Variable	Definición Conceptual	Definición Operacional
Aplicación de políticas de la ciberseguridad de la legislación colombiana	Determinar si dentro de las organizaciones se aplican las leyes, políticas y/o regulaciones que rigen los riesgos de ciberataques	Se medirá a través de la escala de medición entre 1 a 2, donde 1 es nunca, 2 siempre.
Costo de la materialización de los riesgos de la seguridad informática	Determinar el nivel de costos cuando se presenta la materialización de riesgos	Se medirá a través de la escala de medición 1 bajo, 2 medio y 3 alto.

Fuente: Elaboración propia

6.3. Población y Muestra

Para la investigación se va a realizar dos encuestas; con la primera encuesta se busca recolectar información de la implementación de la gestión de riesgos de ciberseguridad y con la segunda encuesta se busca recolectar información de la materialización de los riesgos en empresas grandes de Colombia:

1. En la primera encuesta se va a utilizar como referencia las empresas grandes en Colombia que fueron víctimas de ataques cibernéticos en el año 2022. Según las cifras de la Policía Nacional de Ciberseguridad de Colombia en el año 2022, 34 empresas grandes fueron hackeadas (Ministerio de Defensa Nacional Policía Nacional de Colombia, 2023)

   Se utiliza la fórmula de muestreo aleatorio simple, para identificar la cantidad de empresas en las cuales se tiene que aplicar la primera encuesta:

$$n = \frac{N * Z_{\propto}^{2} p * q}{d^{2} * (N-1) + Z_{\propto}^{2} * p * q}$$

Fuente: Cortés et al. (2020)

   Donde se establece:

Tabla 3: Variables de muestreo aleatorio simple encuesta #1

Tabla 4. Variables de muestreo aleatorio simple encuesta.

VARIABLES DE MUESTREO ALEATORIO SIMPLE ENCUESTA #1		
N	Tamaño de la población	N= 34
Z	Nivel de confianza del 90%	Z= 1.645
p	Probabilidad de que un evento se presente	p= 0,5
q = 1-p	Probabilidad de que el evento no se presente	q= 0,5
d	Margen de error	d= 25%

Fuente: Cortés et al. (2020)

$$n = \frac{34 * 1{,}645^2_{\propto} * 0{,}5 * 0{,}5}{25\%^2 * (34 - 1) + 1.645^2_{\propto} * 0{,}5 * 0{,}5}$$

$$n = 8$$

Después de aplicar la formula, se obtiene que se debe realizar la encuesta #1 a 8 empresas.

2. En la segunda encuesta se va a utilizar como referencia las empresas grandes en Colombia, las cuales son empresas que tienen más de 250 trabajadores. Según las cifras del DANE del "Directorio estadístico de empresas" a final del año 2021 habían registradas 6.267 empresas grandes en el país (Ortiz, 2022, pp. 40).
   Se utiliza la fórmula de muestreo aleatorio simple, para identificar la cantidad de empresas en las cuales se tiene que aplicar la primera encuesta:

$$n = \frac{N * Z^2_{\propto} p * q}{d^2 * (N - 1) + Z^2_{\propto} * p * q}$$

Fuente: Cortés et al. (2020)

Donde se establece:

Tabla 5 Variables de muestreo aleatorio simple encuesta #2

VARIABLES DE MUESTREO ALEATORIO SIMPLE		
N	Tamaño de la población	N= 6.267
Z	Nivel de confianza del 90%	Z= 1.645
P	Probabilidad de que un evento se presente	p= 0,5
q = 1-p	Probabilidad de que el evento no se presente	q= 0,5
D	Margen de error	d= 25%

Fuente: Cortés et al. (2020)

$$n = \frac{6.267 * 1{,}645_{\propto}^{2} * 0{,}5 * 0{,}5}{25\%^{2} * (6.267 - 1) + 1.645_{\propto}^{2} * 0{,}5 * 0{,}5}$$

$$n = 11$$

Después de aplicar la formula, se obtiene que se debe realizar la encuesta #2 a 11 empresas.

Segundo Nivel – Diseño de encuesta

6.4. Selección de métodos o instrumentos para recolección de información

Con el fin de poder obtener la información respecto a los impactos generados en las organizaciones que han sido víctimas de ciberataques lo cual repercutió en la afectación de la prestación de servicios, se pretende desarrollar una seria de preguntas relacionadas con variables asociadas a la gestión del riesgo y a las fallas generadas para la prestación de los servicios, estas variables se describen en la tabla 3, las preguntas serán aplicadas mediante dos encuestas para así mismo obtener información respecto a si las organizaciones tienen implementada y controlada la Gestión de Riesgos en cuanto a seguridad informática y materialización de los riesgos.

Tabla 6. Determinación de variables en la encuesta 1.

Variable		Pregunta asociada	Definición Operacional
Encuesta # 1:			
Impacto del Ciberataque: Corroborar si al presentarse el ataque cibernético hubo repercusión en la continuidad de la prestación de los servicios por la organización y costos asociados al restablecimiento de las actividades.	**Impacto de la materialización de los riesgos de ciberseguridad**	1. ¿Ante la situación presentada en su organización respecto al ciberataque ocasionado, el desarrollo de sus actividades propias de su cargo fue impactada?	Se medirá a través de la escala de medición entre 1 a 3, en donde: 1. Menor: No fueron impactadas. 2. Moderado: Parcialmente impactadas. 3. Mayor: Totalmente impactadas.

Fuente: Elaboración propia.

Tabla 6. Determinación de variables en la encuesta 1. (continuación)

Variable		**Pregunta asociada**	**Definición Operacional**
Encuesta # 1:			
	Impacto de la materialización de los riesgos de ciberseguridad	2. ¿El ataque cibernético ocasionado hacia su organización generó perdida de la información?	Se medirá a través de la escala de medición entre 1 a 3, en donde 1. Menor: No se perdió la información. 2. Moderado: Parcialmente. 3. Mayor: Totalmente.
	Tiempo	3. ¿En qué periodo de tiempo fueron restablecidas las actividades posteriores al ciberataque?	Se medirá a través de la escala de medición entre 1 y 4, en donde 4. No mayor a una semana. 3. Entre 1 y 2 semanas. 2. Entre 3 y 4 semanas. 1. Más de 4 semanas.
	Impacto de la materialización de los riesgos de ciberseguridad	¿Qué impacto tuvo el ataque cibernético en la organización?	Este nivel de impacto se determinará en los siguientes niveles 1. Menor. 2. Moderado. 3. Mayor.
	Costo de la materialización de los riesgos de la seguridad informática	4. ¿El costo destinado para el restablecimiento de las actividades posterior al ataque cibernético fue de?	La unidad de medida será en pesos, se medirá a través de la escala de medición entre 1 y 4, donde se cataloga 1. Menor, 2. Moderado, 3. Mayor, 4. Catastrófico: D Discriminado en los siguientes valores. 4. Mayor a 4.000 millones. 3. Entre 15 y 235 millones. 2. Entre 2 y 15 millones. 1. Entre 1 y 2 millones.

Fuente: Elaboración propia

Tabla 7. Determinación de variables en la encuesta 2.

Variable		**Pregunta asociada**	**Definición Operacional**
Encuesta # 2:			
Importancia en Seguridad Cibernética: Evidenciar si en las organizaciones es prioritaria e importante la seguridad cibernética.	**Importancia de la ciberseguridad en las organizaciones colombianas.**	1. ¿Su organización cuenta con políticas o procedimientos para el respaldo de la información?	Se categorizará a través de selección única. Donde sí tiene importancia alta, no lo sé no se va a tener en cuenta, no importancia baja: Si No No lo se
		2. ¿En su organización se ejecutan Auditorías Internas a nivel de Tecnología de Información?	Se medirá definiendo entre alto, medio y bajo a través de la escala de medición entre 1 a 5, donde bajo será entre Nunca y Casi nunca, medio Ocasionalmente y Alto entre Frecuentemente y Siempre: 1. Nunca. 2. Casi nunca. 3. Ocasionalmente. 4. Frecuentemente. 5. Siempre.
		3. ¿En su organización se establecen programas de formación al personal respecto a seguridad informática?	Se categorizará a través de selección única, donde si es alta y no es baja. Si No.
Gestión del Riesgo:	**Herramientas tecnológicas**	4. ¿Conoce si al interior de su organización se cuenta con la implementación de Gestión del Riesgo respecto a Seguridad Informática?	Se categorizará a través de selección única. Si se cuenta con la implementación y es evaluada constantemente. Si se cuenta con la implementación, pero no es evaluada constantemente. No. No lo sé.

Fuente: Elaboración propia.

Tabla 7. Determinación de variables en la encuesta 2. (continuación)

Variable		Pregunta asociada	Definición Operacional
Encuesta # 2:			
		5. ¿Se encuentra asignado un presupuesto dentro de su organización para la adquisición y mantención de tecnología para la protección de la información?	Se categorizará a través de selección única mediante las siguientes variables. 1. Siempre: Si, se adquiere y se mantiene. 2. Ocasionalmente: Si, se compró la licencia, pero no se renovó en su vencimiento. 1. Nunca: No
	Aplicación de políticas de la ciberseguridad de la legislación colombiana	6. ¿Cuándo le llega un E-Mail de una cuenta de correo electrónico desconocido, en el cual se le solicita ingresar a un sitio web mediante un link agregado, usted ingresa?	Se categorizará a través de selección única, donde 1 es nunca: No y 2 es siempre: Si: Si No
		7. ¿Al interior de su organización se rigen por políticas regulatorias en los sistemas de información?	Se categorizará a través de selección única, donde 1 es siempre: Si y 2 es nunca: No: Si No
	Herramientas tecnológicas	8. ¿En los computadores asignados por su organización cuentan con dispositivos de control de software para la seguridad de la información en cada uno de estos?	Se categorizará a través de selección única. 3. Siempre: Si 1.Nunca: No No lo sé: No se tendrá en cuenta

Fuente: Elaboración propia.

Tabla 7. Determinación de variables en la encuesta 2. (continuación)

Variable		**Pregunta asociada**	**Definición Operacional**
Encuesta # 2:			
	Aplicación de políticas de la ciberseguridad de la legislación colombiana	9. ¿En su organización cuentan con direccionamiento respecto al ingreso a email personal y redes sociales?	Se categorizará a través de selección única. Si No
	Costo de la implementación del sistema de gestión de riesgos	10. ¿Cuántos colaboradores en su organización componen el área de gestión de riesgos?	Se medirá a través de la escala de medición entre 1 a 5, donde: 1. Entre 1 y 2 colaboradores 2. Entre 3 y 4 colaboradores 3. Entre 4 y 5 colaboradores 4. Más de 5 colaboradores

Fuente: Elaboración propia

La herramienta de medición para llevar a cabo la recolección de la información es mediante una encuesta diseñando un cuestionario en el cual se establecen preguntas de selección única dicotómicas y politómicas.

6.5. Técnicas de análisis de datos

Las encuestas se realizarán de forma virtual, obteniendo resultados cuantitativos los cuales serán analizados a través de estadística descriptiva e inferencial:

Tabla 8: Técnicas de análisis de datos

Instrumento	**Técnica de análisis**	**Descripción**
Herramienta SPSS	Estadística descriptiva	A través de la herramienta SPSS los datos serán organizados en tablas y en gráficos, los cuales ayudarán a entender los resultados de una forma clara y precisa.
Excel	Estadística inferencial	Con los resultados obtenidos en la encuesta se deducirán algunos datos, como los costos en los que están incurriendo las empresas grandes en Colombia actualmente en la implementación de la gestión de riesgos de seguridad informática.

Fuente: Elaboración propia

7. ANÁLISIS Y DISCUSIÓN DE LOS DATOS

7.1 Análisis de los datos cuantitativos

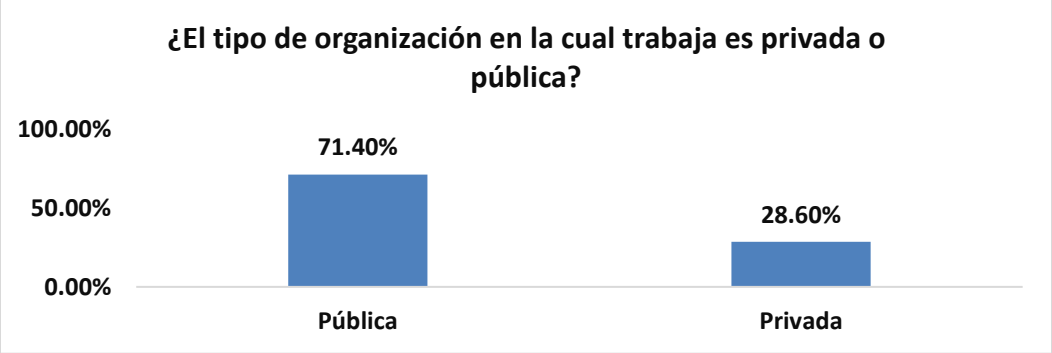
En el siguiente apartado, se expondrá el análisis de los resultados de las encuestas realizadas como herramienta de recolección de datos, esto con el fin de dar cumplimiento al objetivo principal de la presente investigación. Se aplicaron dos encuestas una denominada Análisis costo beneficio de la implementación de gestión de riesgos de la seguridad de la información en las empresas en Colombia donde se obtuvieron 14 respuestas y la otra denominada Costo beneficio de la implementación de Gestión de Riesgos de la Seguridad de la información en las empresas en Colombia donde se obtuvieron 11 respuestas. Con la información obtenida de los formularios de Google, se organizó en un Excel y se importaron los datos al software SPSS donde se realizó el análisis de los datos mediante tablas y gráficos. De esta recolección de datos, se realizará el siguiente análisis:

1. Grafica de porcentaje por cada una de las preguntas
2. Análisis de relación de las variables utilizados.

7.1.1 Grafica de porcentaje por cada pregunta

A continuación, se presenta una tabla de frecuencia por cada pregunta y un análisis a través de graficas de barras, para las preguntas de las dos encuestas realizadas. Se presentará el análisis de la encuesta denominada Análisis costo beneficio de la implementación de gestión de riesgos de la seguridad de la información en las empresas en Colombia.

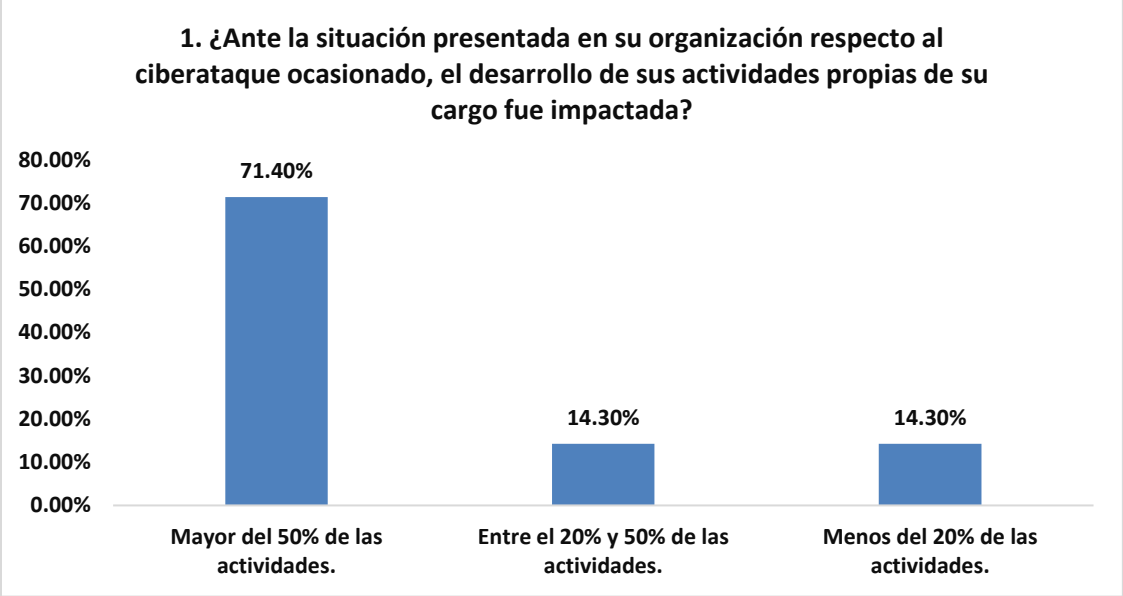
Gráfico 1. Resultado pregunta general



Fuente: elaboración propia

Se puede evidenciar que el 71,4% de los encuestados pertenecen a organizaciones públicas.

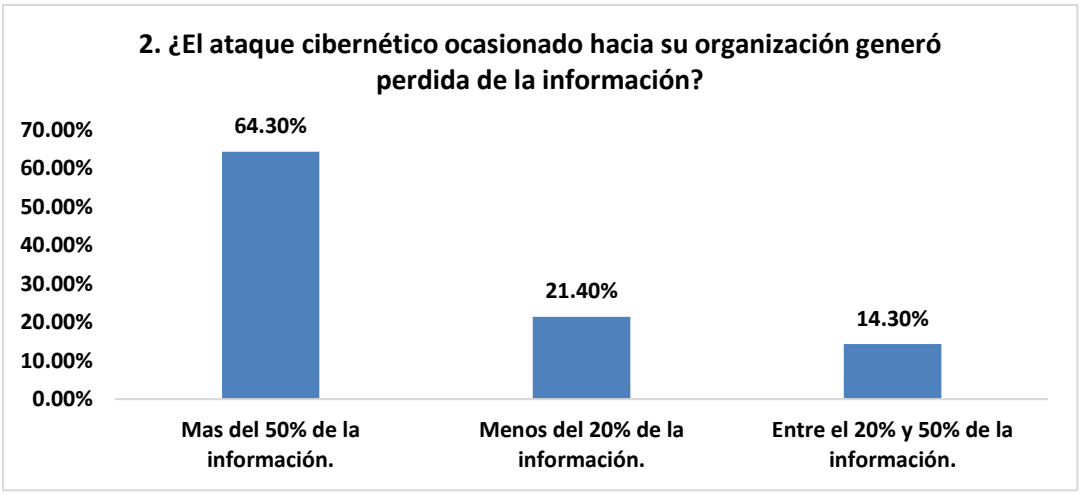
Gráfico 2. Resultado pregunta 1.



Fuente: Elaboración propia

Se puede evidenciar que al 71,4% de los encuestados la presencia de un ciberataque impacto en más del 50% de las actividades que desarrollan diariamente. El 14,30 % de los encuestados se vieron impactados entre el 20 y 50% de sus actividades.

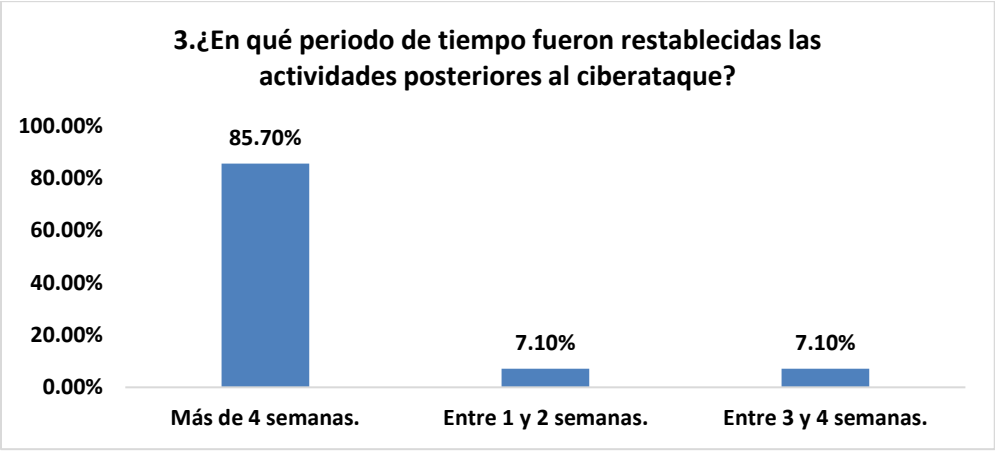
Gráfico 3. Resultado pregunta 2.



Fuente: Elaboración propia

Se puede evidenciar que al 64,30 % de los encuestados el ataque cibernético ocasionado en la organización generó más del 50% de perdida de la información. El 21,4% de los encuestados perdió menos del 20% de la información.

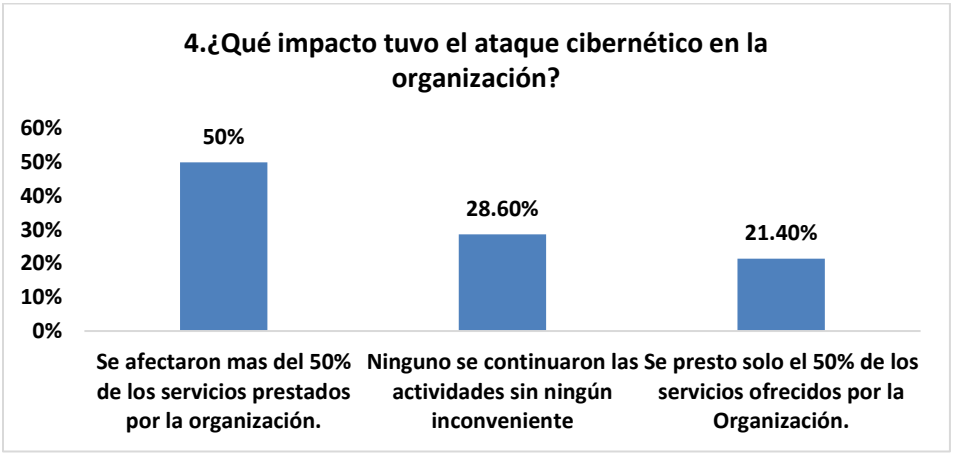
Gráfico 4. Resultado pregunta 3.



Fuente: Elaboración propia

Se puede evidenciar que el 85,70% de los encuestados restableció sus actividades en más de 4 semanas posteriores el ciberataque, el 7,10% entre 1 y 2 semanas y el 7,10% entre 3 y 4 semanas.

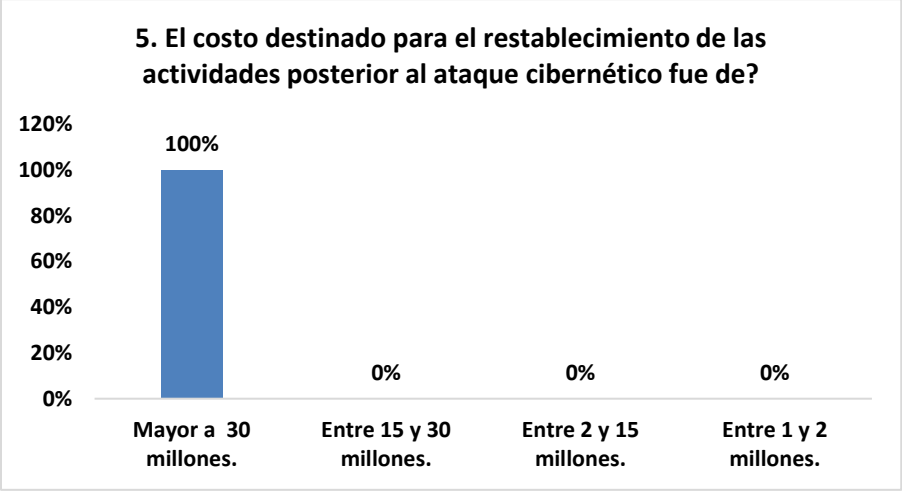
Gráfico 5. Resultado pregunta 4.



Fuente: Elaboración propia

Se puede identificar que al 50% de los encuestados un ataque cibernético les afecto en más del 50% de los servicios prestados por la organización. El 28,60% no tuvo ningún impacto y continuaron con sus actividades sin presentar inconvenientes.

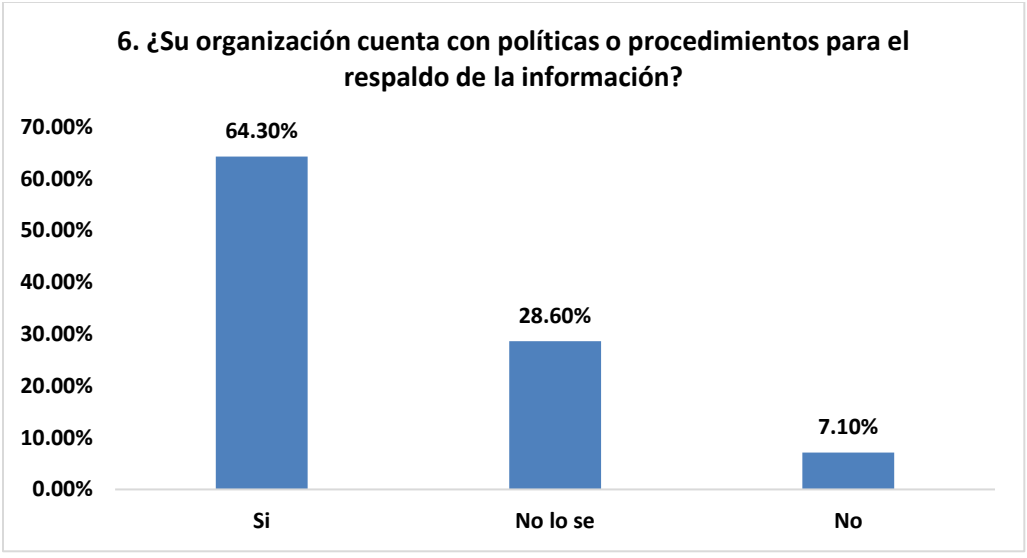
Gráfico 6. Resultado pregunta 5.



Fuente: Elaboración propia

Al 100% de los encuestados el costo para el restablecimiento de las actividades por un ataque cibernético fue mayor a 30 millones de pesos.

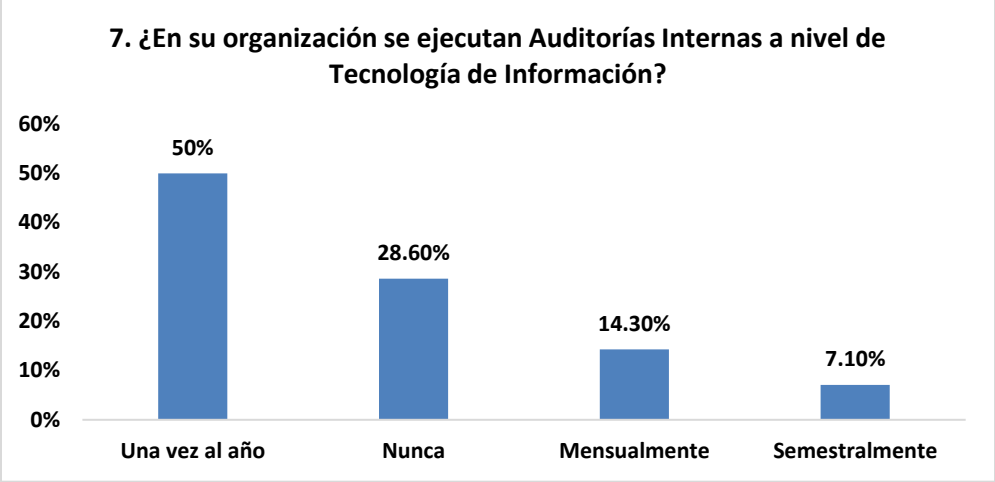
Gráfico 7. Resultado pregunta 6.



Fuente: Elaboración propia

De esta pregunta, se puede identificar que el 64,30% de las organizaciones cuentan con políticas o procedimientos para el respaldo de la información.

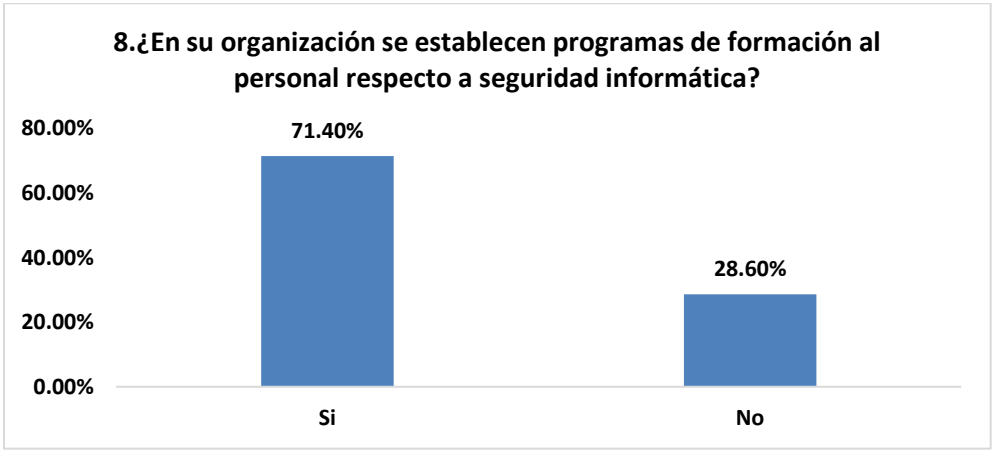
Gráfico 8. Resultado pregunta 7.



Fuente: Elaboración propia

La grafica permite identificar que el 50% de las organizaciones ejecutan las auditorías internas a nivel de tecnología de información, una vez al año, el 28,60% nunca las ejecuta, el 14,30% las ejecuta mensualmente y el 7,10% semestralmente.

Gráfico 9. Resultado pregunta 9.



Fuente: Elaboración propia

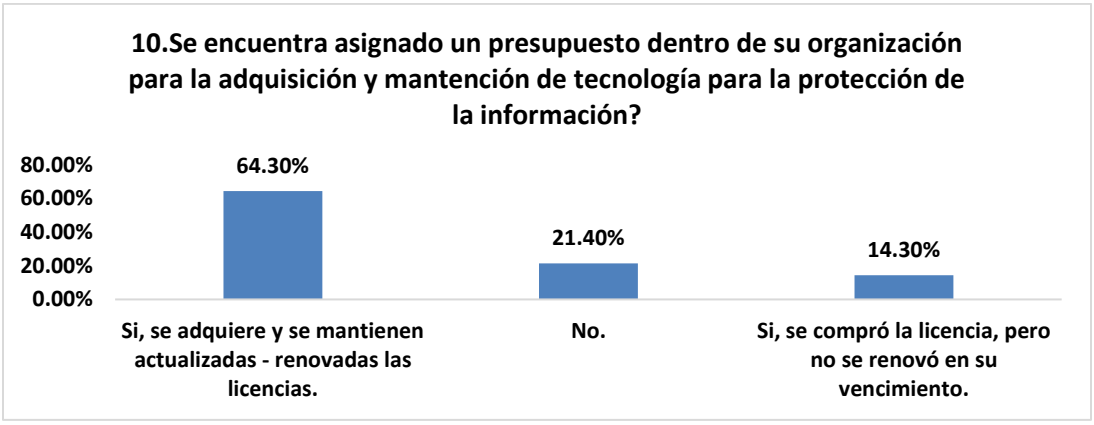
A partir de la gráfica, se puede evidenciar que el 71,40% de los encuestados reconoce que en su organización se establecen programas de formación al personal respecto a seguridad informática. El 28,60% no conoce los programas de formación.

Gráfico 10. Resultado pregunta 9.

Fuente: Elaboración propia

De la gráfica se puede deducir, que el 50% de los encuestados no conoce si al interior de su organización se cuenta con la implementación de Gestión del Riesgo respecto a Seguridad Informática, el 21,40% conoce que la organización si cuenta con la implementación y se evalúa constantemente y el 14,30% conoce que la organización si cuentan con la implementación, pero no es evaluado constantemente.

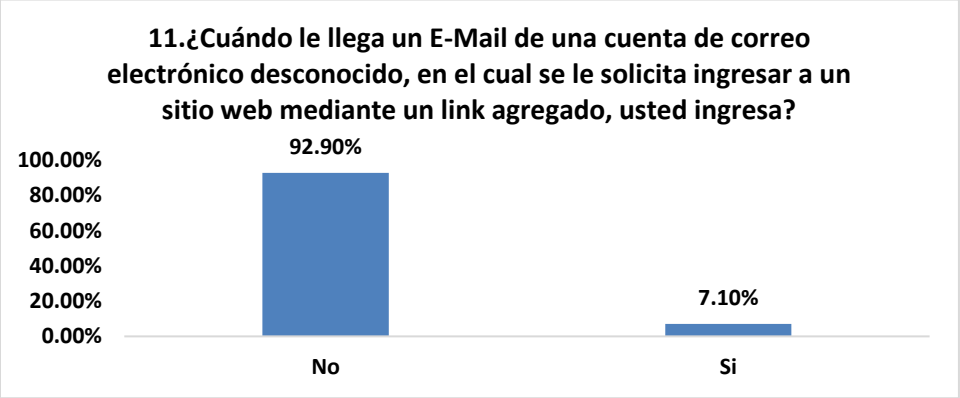
Gráfico 11. Resultado pregunta 10.



Fuente: Elaboración propia

De la gráfica se identificar, que el 64,30% de los encuestados conoce que dentro de la organización se encuentra un presupuesto asignado para la adquisición y mantención de la tecnología de la información, además se adquiere el presupuesto, se mantiene actualizado, además las licencias son renovadas. El 14,30% si establece el presupuesto, pero no renovó su vencimiento y el 21,40% no establece presupuesto.

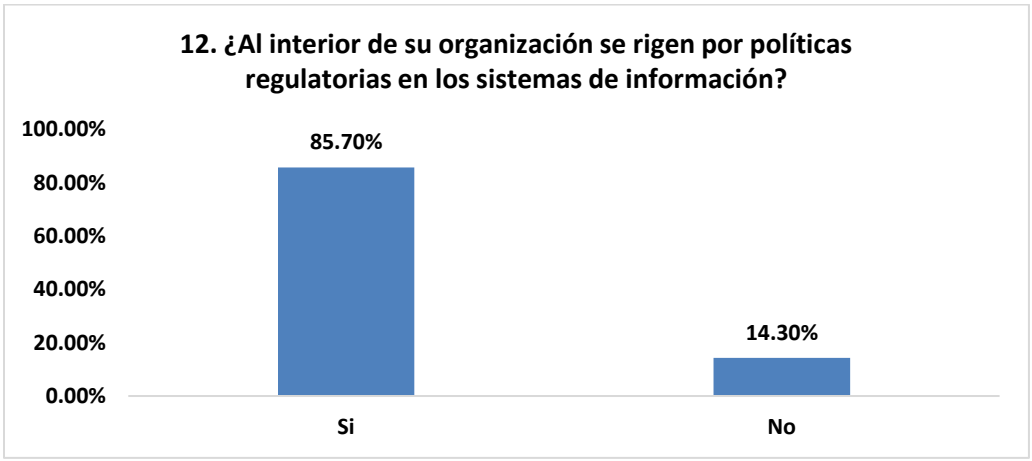
Gráfico 12. Resultado pregunta 11.



Fuente: Elaboración propia

De la gráfica anterior, se puede evidenciar que el 92,90% de los encuestados no ingresa al enlace que llega a través de un E- mail de una cuenta de correo electrónico desconocido y el 7,10% de los encuestados si ingresa.

Gráfico 13. Resultado pregunta 12.



Fuente: Elaboración propia

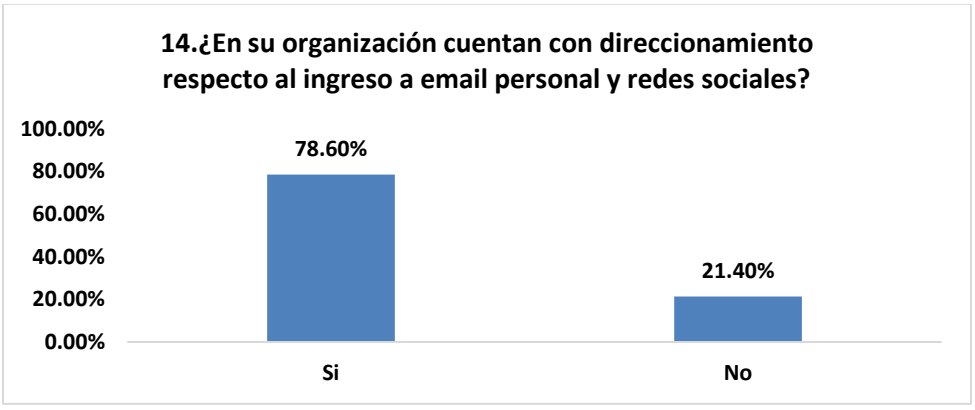
De la gráfica anterior, se puede deducir que el 85,70% de los encuestados conoce que dentro de su organización se rigen políticas regulatorias en los sistemas de información. El 14,30% de los encuestados no identifica que se rijan por políticas dentro de su organización.

Gráfico 14. Resultado pregunta 13.

Fuente: Elaboración propia

De la gráfica anterior, se puede deducir que el 85,70% de los encuestados cuenta con dispositivos de control de software para la seguridad de la información en sus computadores, el 7,10% no conoce esta información y el 7,10% no cuenta con dispositivos de control.

Gráfico 15. Resultado pregunta 14.



Fuente: Elaboración propia

De la gráfica anterior, se evidencia que el 78,60% de los encuestado cuentan con direccionamiento respecto al ingreso a email personal y redes sociales pero el 21,40% no cuenta con esto.

Gráfico 16. Resultado pregunta 15.

Fuente: Elaboración propia

Se evidencia que dentro de las organizaciones encuestadas el 85,70% cuenta con más de 5 colaboradores el área de gestión de riesgos a nivel de seguridad informática. El 7,10% entre 4 y 5 colaboradores y el 7,10% entre 1 y 2 colaboradores.

A continuación, se presentan los resultados de la encuesta denominada --_Costo beneficio de la implementación de Gestión de Riesgos de la Seguridad de la información en las empresas en Colombia.

Gráfico 17. Resultado pregunta general 2.

Fuente: Elaboración propia

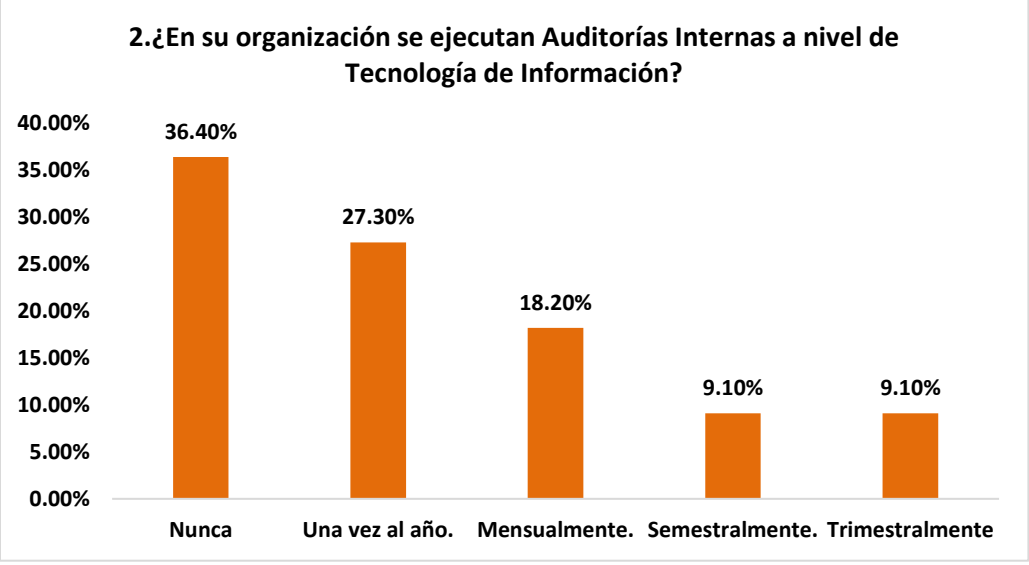
Se evidencia que el 81,80% de los encuestados trabajan en una organización privada, el 9,10% en una organización publica y el 9,10% en una organización multilateral.

Gráfico 18. Resultado pregunta 1 encuesta 2.

Fuente: Elaboración propia

Se evidencia que el 90,90 % de los encuestados conoce que dentro de su organización se cuenta con políticas o procedimientos para el respaldo de la información.

Gráfico 19. Resultado pregunta 2 encuesta 2.



Fuente: Elaboración propia

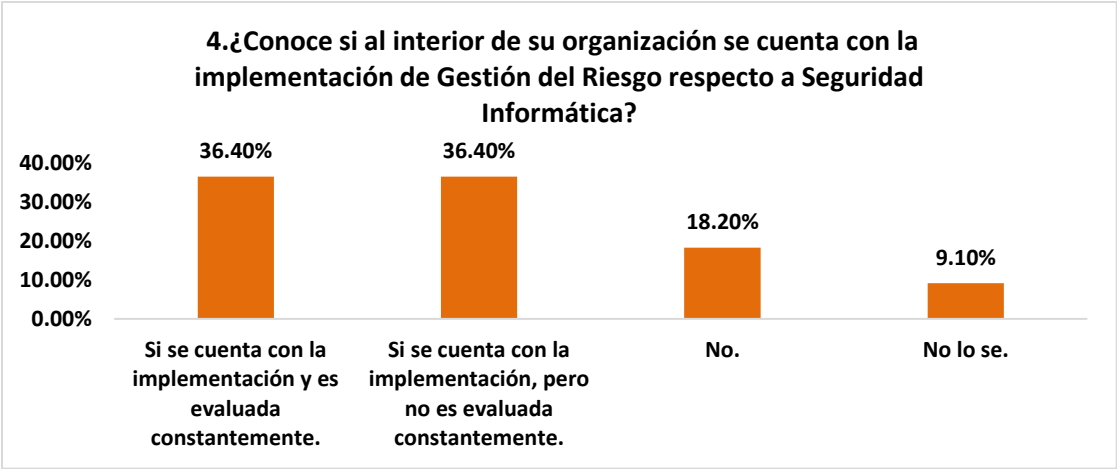
De la gráfica, se puede deducir que en las organizaciones del 36,40% de los encuestados no se ejecutan auditorías internas a nivel de Tecnología de Información, el 27,30% ha recibido una auditoria una vez al año, el 18,20% mensualmente recibe una auditoria y el 9,10% recibe una auditoria semestralmente y el 9,10% trimestralmente.

Gráfico 20. Resultado respuesta 3 encuesta 2.

Fuente: Elaboración propia

La grafica permite evidenciar que el 54,50% de los encuestados conoce que en su organización establecen programas de formación al personal respecto a seguridad informática, mientras que el 45,50% no conoce que en su organización establezcan programas.

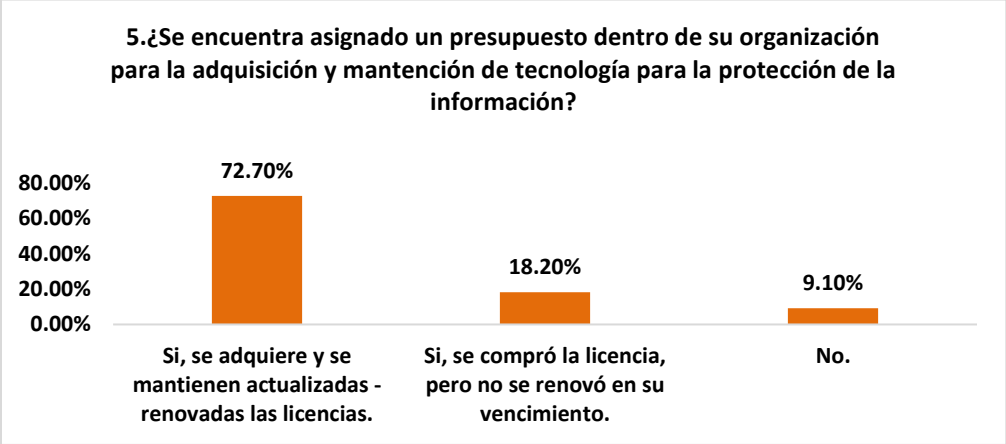
Gráfico 21. Respuesta 4 encuesta 2.



Fuente: Elaboración propia

Se puede evidenciar en la gráfica, que el 36,40% de los encuestados conoce que dentro de su organización se cuenta con la implementación de Gestión del Riesgo respecto a seguridad informática y se evalúa constantemente, así mismo, 36,40% también conoce la implementación dentro de la organización, pero no se evalúa constantemente, el 18,20 % no conoce y el 9,10% no sabe si se implementa dentro de su organización.

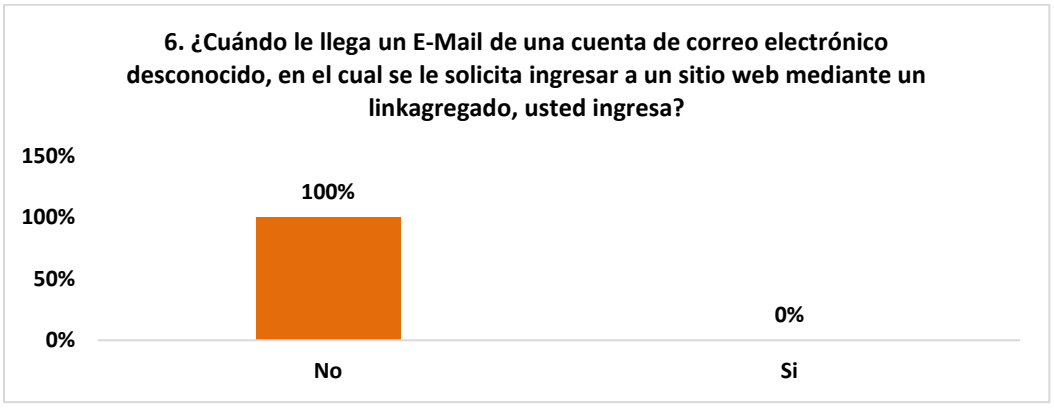
Gráfico 22. Resultado pregunta 5 encuesta 2.



Fuente: Elaboración propia

Se puede evidenciar en esta pregunta que el 72,70% de los encuestados conoce que, dentro de sus organizaciones, se encuentra un presupuesto asignado y se mantienen actualizadas y renovadas las licencias, el 18,20% si asigna el presupuesto, compro la licencia, pero no la renovó y el 9,10% no cuenta con presupuesto asignado.

Gráfico 23. Resultado pregunta 6 encuesta 2.



Fuente: Elaboración propia

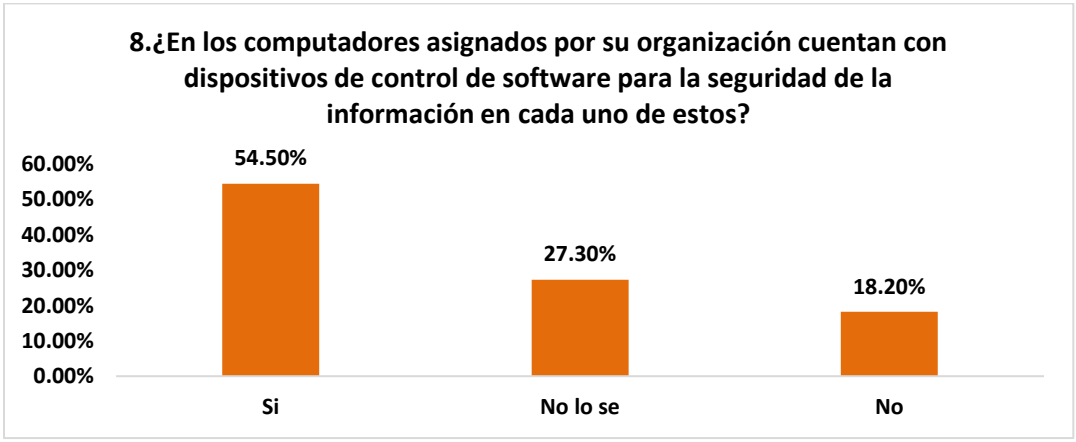
Se puede evidenciar que el 100% de los encuestados no ingresa a un sitio web cuando les llega un E-Mail de una cuenta de correo electrónico desconocido con un enlace.

Gráfico 24. Resultado pregunta 7 encuesta 2.

Fuente: Elaboración propia

A partir de la gráfica anterior, se puede deducir que el 90,90% de los encuestados conoce que dentro de su organización se rigen por políticas regulatorias en los sistemas de información. Mientras que el 9,10% de los encuestados no conoce si dentro de su organización se rigen por políticas regulatorias los sistemas de información.

Gráfico 25. Resultado pregunta 8 encuesta 2.



Fuente: Elaboración propia

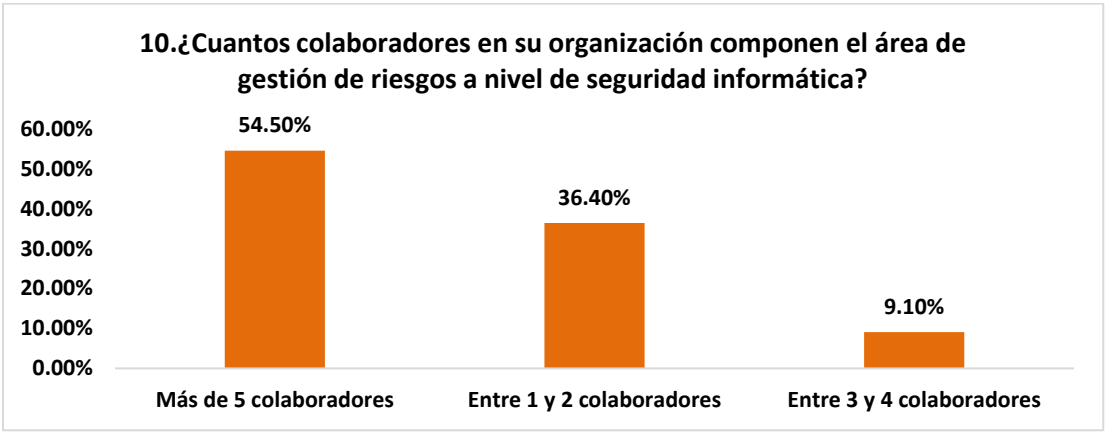
Se puede evidenciar que el 54.50% de los encuestados cuenta dentro de sus organizaciones con computadores que tienen dispositivos de control de software para la seguridad de la información. El 27,30% de los encuestados no conoce esta información y el 18,20% indica que sus computadores no cuentan con dispositivos de control de software.

Gráfico 26. Resultado pregunta 9 encuesta 2.

Fuente: Elaboración propia

Se identifica en la gráfica que el 63,60% de los encuestados cuenta con direccionamiento respecto al ingreso a email personal y redes sociales, mientras el 36,40% no cuenta con este direccionamiento.

Gráfico 27. Resultado pregunta 10 encuesta 2.



Fuente: Elaboración propia

Se puede evidenciar que el 54,50% de los encuestado indica que dentro de sus organizaciones se encuentran más de 5 colaboradores en el área de gestión de riesgos de nivel de seguridad informática, el 36,40% indica que entre 1 y 2 colaboradores y el 9,10% entre 3 y 4 colaboradores.

7.1.2 Análisis de relación de variables

A continuación, se presenta el análisis de relación de unas variables seleccionadas dentro de las encuestas realizadas, el análisis se realizará a través de la prueba Chi-cuadrado. Se prueba en la encuesta de análisis costo beneficio de la implementación de Gestión de Riesgos de la Seguridad de la información en las empresas en Colombia si son independientes las variables, impacto de la materialización de los riesgos de ciberseguridad en las actividades de desarrollo diario y el impacto de materialización de la organización. Se plantean las siguientes hipótesis

H0: No existe relación entre las variables entre las dos variables. Es decir, las dos variables son independientes

Ha: Existe relación entre las variables entre las variables

Figura 1. Relación entre variables impacto en actividades e impacto en la organización

Tabla cruzada 1. ¿Ante la situación presentada en su organización respecto al ciberataque ocasionado, el desarrollo de sus actividades propias de su cargo fue impactada?*4.¿Qué impacto tuvo el ataque cibernético en la organización?

Recuento

		4.¿Qué impacto tuvo el ataque cibernético en la organización?			
		Ninguno se continuaron las actividades sin ningún inconveniente.	Se afectaron mas del 50% de los servicios prestados por la organización.	Se presto solo el 50% de los servicios ofrecidos por la Organización.	Total
1. ¿Ante la situación presentada en su organización respecto al ciberataque ocasionado, el desarrollo de sus actividades propias de su cargo fue impactada?	Entre el 20% y 50% de las actividades.	1	0	1	2
	Mayor del 50% de las actividades.	2	7	1	10
	Menos del 20% de las actividades.	1	0	1	2
Total		4	7	3	14

Pruebas de chi-cuadrado

	Valor	gl	Significación asintótica (bilateral)
Chi-cuadrado de Pearson	5.833[a]	4	.212
Razón de verosimilitud	7.387	4	.117
N de casos válidos	14		

a. 8 casillas (88.9%) han esperado un recuento menor que 5. El recuento mínimo esperado es .43.

Fuente: Elaboración propia con uso de SPSS

Como el valor-p de la prueba es 0.212 el cual es mayor que el nivel de significancia 0.05, entonces no se rechaza la hipótesis nula y se concluye que no existen suficientes evidencias que demuestren a un nivel de significancia del 5%, que existe relación entre las dos variables.

Por otro lado, también se prueba en la encuesta si son independientes las variables, impacto de materialización de riesgo organización y el tiempo de restablecimiento de las actividades.

Se plantean las siguientes hipótesis

H0: No existe relación entre las variables entre las dos variables. Es decir, las dos variables son independientes

Ha: Existe relación entre las variables entre las variables

Figura 2. Impacto de materialización de riesgo organización y el tiempo de restablecimiento de las actividades

Tabla cruzada 2. ¿El ataque cibernético ocasionado hacia su organización generó perdida de la información?*3. ¿En qué periodo de tiempo fueron restablecidas las actividades posteriores al ciberataque?

Recuento

		3. ¿En qué periodo de tiempo fueron restablecidas las actividades posteriores al ciberataque?			
		Entre 1 y 2 semanas.	Entre 3 y 4 semanas.	Más de 4 semanas.	Total
2. ¿El ataque cibernético ocasionado hacia su organización generó perdida de la información?	Entre el 20% y 50% de la información.	1	0	1	2
	Mas del 50% de la información.	0	0	9	9
	Menos del 20% de la información.	0	1	2	3
Total		1	1	12	14

Pruebas de chi-cuadrado

	Valor	gl	Significación asintótica (bilateral)
Chi-cuadrado de Pearson	10.306[a]	4	.036
Razón de verosimilitud	7.664	4	.105
N de casos válidos	14		

a. 8 casillas (88.9%) han esperado un recuento menor que 5. El recuento mínimo esperado es .14.

Fuente: Elaboración uso de SPSS

Como el valor-p de la prueba es 0.036 el cual es menos que el nivel de significancia 0.05, entonces se rechaza la hipótesis nula y se concluye que existen suficientes evidencias que demuestren a un nivel de significancia del 5%, que existe relación entre las dos variables. Por otro lado, se realiza la relación de variables importante de la encuesta costo beneficio de la implementación de Gestión de Riesgos de la Seguridad de la información en las empresas en Colombia, si son independientes las variables importancia de la ciberseguridad en las organizaciones colombianas y aplicación de políticas de la ciberseguridad de la legislación colombiana.

Figura 3. Relación entre la importancia de la ciberseguridad en las organizaciones colombianas y aplicación de políticas de la ciberseguridad de la legislación colombiana

Tabla cruzada 1. ¿Su organización cuenta con políticas o procedimientos para el respaldo de la información?*7. ¿Al interior de su organización se rigen por políticas regulatorias en los sistemas de información?

Recuento

		7. ¿Al interior de su organización se rigen por políticas regulatorias en los sistemas de información?		
		No	Si	Total
1. ¿Su organización cuenta con políticas o procedimientos para el respaldo de la información?	No lo se	0	1	1
	Si	1	9	10
Total		1	10	11

Pruebas de chi-cuadrado

	Valor	gl	Significación asintótica (bilateral)	Significación exacta (bilateral)	Significación exacta (unilateral)
Chi-cuadrado de Pearson	.110[a]	1	.740		
Corrección de continuidad[b]	.000	1	1.000		
Razón de verosimilitud	.200	1	.654		
Prueba exacta de Fisher				1.000	.909
N de casos válidos	11				

a. 3 casillas (75.0%) han esperado un recuento menor que 5. El recuento mínimo esperado es .09.

b. Sólo se ha calculado para una tabla 2x2

Fuente: Elaboración uso de SPSS

Como el valor-p de la prueba es 0.740 el cual es mayor que el nivel de significancia 0.05, entonces no se rechaza la hipótesis nula y se concluye que no existen suficientes evidencias que demuestren a un nivel de significancia del 5%, que existe relación entre las dos variables.

Así mismo, se analizaron las variables de presupuesto asignado para herramientas tecnologías y numero de colaboradores de la organización.

Figura 4. Relación entre el de presupuesto asignado para herramientas tecnologías y numero de colaboradores de la organización.

Tabla cruzada 5.¿Se encuentra asignado un presupuesto dentro de su organización para la adquisición y mantención de tecnología para la protección de la información?*10. ¿Cuantos colaboradores en su organización componen el área de gestión de riesgos a nivel de seguridad informática?

Recuento

		10. ¿Cuantos colaboradores en su organización componen el área de gestión de riesgos a nivel de seguridad informática?			
		Entre 1 y 2 colaboradores	Entre 3 y 4 colaboradores	Más de 5 colaboradores	Total
5.¿Se encuentra asignado un presupuesto dentro de su organización para la adquisición y mantención de tecnología para la protección de la información?	No.	1	0	0	1
	Si, se adquiere y se mantienen actualizadas - renovadas las licencias.	3	1	4	8
	Si, se compró la licencia, pero no se renovó en su vencimiento.	0	0	2	2
Total		4	1	6	11

Pruebas de chi-cuadrado

	Valor	gl	Significación asintótica (bilateral)
Chi-cuadrado de Pearson	3.552[a]	4	.470
Razón de verosimilitud	4.573	4	.334
N de casos válidos	11		

a. 9 casillas (100.0%) han esperado un recuento menor que 5. El recuento mínimo esperado es .09.

Fuente: Elaboración uso de SPSS

Como el valor-p de la prueba es 0.47 el cual es mayor que el nivel de significancia 0.05, entonces no se rechaza la hipótesis nula y se concluye que no existen suficientes evidencias que demuestren a un nivel de significancia del 5%, que existe relación entre las dos variables.

7.1.3. Análisis de Variables (Inferencial)

7.1.3.1 Tiempo

Según las encuestas realizadas a los colaboradores de empresas grandes en Colombia que fueron víctimas de ciberataque en el año 2022 se puede evidenciar que en la mayoría de los casos se necesitan más de 4 semanas para restablecer las actividades

después de un ciber ataque, debido a que el 85,70% de los encuestados indicaron que las actividades se restablecieron en más de 4 semanas posteriores el ciberataque.

7.1.3.2. Costo de la implementación del sistema de gestión de riesgo

La implementación de la gestión de riesgos tiene diferentes componentes claves, los cuales se explicarán en la siguiente tabla con los costos promedio según las encuestas, cotizaciones e investigación:

Tabla 9. Costo de la implementación del sistema de gestión de riesgo

ITEM	RANGO DE COSTOS		OBSERVACIONES
	COSTO MENOR	COSTO MAYOR	
Talento Humano	$ 15.600.000	$ 38.000.000	Salario promedio de Analistas de Gestión de Riesgos de Seguridad de la información y un Gerente: * Costo menor: 1 Gerente y 2 analistas * Costo mayor: 1 Gerente y 10 analistas - Sueldo promedio de Gerente de Gestión de Riesgos de Seguridad de la información: $10.000.000 - Sueldo promedio de Analista de Gestión de Riesgos: $2.800.000
Renta de computadores	$ 660.000	$ 2.420.000	Renta de computadores portátiles HP Core i5-7200U con licencia de Office (Ver Anexo 1)
Costo de adquisición de software	$ 8.000.000	$ 870.000.000	Rango de implementación de un software de gestión de riesgos. Dependiendo el programa, las funcionalidades, las cantidades de licencias y parametrizaciones. (Ver Anexo 2)
Costo de auditoría y certificación ISO 27001	$ 18.000.000	$ 56.000.000	*Costo menor: Certificación ISO 27001 * Costo mayor: Certificación más asesoría
Costo de mantenimiento de licencias de software	$ 500.000	$ 5.000.000	Rango de licencias y soporte de un software de gestión de riesgos. Dependiendo el programa (Ver Anexo 2)

Fuente: Talent.com. (2023), Bureau Veritas (2023)

Los primeros dos item son fundamentales para la implementación de la gestión de riesgos de seguridad de la información en las empresas grandes; el ítem 3, 4 y 5 se pueden ir implementando a medida que la gestión tenga una madurez más grande.

7.1.3.3. Impacto de la materialización de los riesgos de ciberseguridad

Según las encuestas realizadas a los colaboradores de empresas grandes en Colombia que fueron víctimas de ciberataque en el año 2022 se puede evidenciar que los impactos de la materialización de riesgos afecto:

- Más del 50% de las actividades desarrolladas diariamente dentro de la compañía, evidenciado en el 71,4% del total de los encuestados
- Más del 50% de perdida de la información, evidenciado en el 64,30% de los encuestados
- El costo para el restablecimiento de las actividades después del ataque cibernético fue mayor a 30 millones de pesos, evidenciado en el 100% de los encuestados.

7.1.3.4. Importancia de la ciberseguridad de las organizaciones colombianas

Según las encuestas realizadas a los colaboradores de empresas grandes en Colombia que fueron víctimas de ciberataque en el año 2022 y a los colaboradores de empresas grandes en Colombia se puede evidenciar que:

- El 64,3% de los colaboradores encuestados de las empresas victimas de ciber ataque en el 2022 cuentan con políticas o procedimientos para el respaldo de la información y el 90,90 % de los colaboradores encuestados de grandes empresas conoce que dentro de su organización se cuenta con políticas o procedimientos para el respaldo de la información.
- Estos datos permiten analizar que la implementación de políticas o procedimientos para el respaldo de la información es de vital importancia para mitigar los riesgos de ataques cibernéticos, debido a que las encuestas realizadas a los colaboradores de las empresas que no han sido hackeadas cuentan con un

mayor número de respuestas que indican que cuentan con estas políticas en comparación con las empresas víctimas de ataque cibernéticos en el 2022.

- Tanto en empresas grandes en Colombia, como en empresas grandes en Colombia que han sido víctimas de ciber ataques se evidencia que la implementación de la gestión de riesgos respecto a seguridad informática es muy baja con unos resultados del 36,4% y 35,7%.

7.1.3.5. Herramientas tecnológicas

La mayoría de las organizaciones encuestadas indican que cuentan con la implementación de la Gestión del Riesgo en Seguridad Informática y que esta es evaluada constantemente. Esto demuestra que existe una conciencia sobre la importancia de gestionar los riesgos en este ámbito. Sin embargo, es preocupante que un porcentaje de las organizaciones encuestadas no está seguro si cuentan con la implementación de la Gestión del Riesgo en Seguridad Informática. Esto puede indicar una falta de conocimiento a nivel organizacional o comprensión sobre la importancia de esta Gestión.

Aunque la mayoría de las organizaciones encuestadas indican contar con la implementación de la Gestión del Riesgo en Seguridad Informática, es necesario fomentar una mayor conciencia sobre su importancia en aquellas organizaciones que no estén seguras o no la hayan implementado. La Gestión del Riesgo en Seguridad Informática es clave para proteger los activos de información y garantizar la continuidad del negocio en un entorno cada vez más digital y vulnerable a las amenazas cibernéticas. La mayoría de las organizaciones encuestadas asignan presupuesto para la adquisición y mantención de tecnología para la protección de la información, no obstante, es importante hacer un seguimiento adecuado para renovar las licencias en su vencimiento. Así mismo en un menor porcentaje se evidencian organizaciones que aún no asignan presupuesto dado que no consideran la importancia de invertir en seguridad cibernética para proteger la información y mitigar los riesgos asociados a esta. Un alto porcentaje de las organizaciones encuestadas también indicaron que los computadores asignados por su organización cuentan con dispositivos de control de software para la seguridad de la información. Esto es muy positivo, ya que estos dispositivos son herramientas

fundamentales para proteger los sistemas y datos de posibles amenazas y ataques cibernéticos. Sin embargo, en una menor proporción de las personas encuestadas mencionaron que no saben si los computadores asignados cuentan con dispositivos de control de software. Esto puede indicar una falta de conocimiento o supervisión en cuanto a las medidas de seguridad implementadas en los equipos.

Es importante que todas las organizaciones estén conscientes de la importancia de contar con dispositivos de control de software en los computadores asignados. Estos dispositivos pueden incluir antivirus, firewalls, sistemas de detección de intrusiones, entre otros. Estas medidas de seguridad ayudan a prevenir y mitigar los riesgos de seguridad informática.

7.1.3.6. Aplicación de políticas de la ciberseguridad de la legislación colombiana

La mayor parte de las personas encuestadas muestran una actitud responsable al no ingresar a un sitio web mediante un enlace en un correo electrónico desconocido. Sin embargo, es necesario que las empresas continúen promoviendo la conciencia y educación en seguridad cibernética para que más personas adopten prácticas seguras y eviten caer en posibles ataques de phishing. A su vez también indicaron que se rigen por políticas regulatorias en los sistemas de información. Esto es una señal positiva, ya que contar con políticas regulatorias establecidas es fundamental para garantizar la seguridad y protección de la información dentro de una organización. Es importante destacar que un pequeño porcentaje de las organizaciones encuestadas mencionaron que no se rigen por políticas regulatorias en los sistemas de información. Esto puede ser un factor de riesgo, ya que la falta de políticas claras y regulaciones en materia de seguridad de la información puede exponer a la organización a posibles brechas de seguridad y vulnerabilidades.

7.1.3.7. Costo de la materialización de los riesgos de la seguridad informática

Al 100% de los colaboradores encuestados de empresas que sufrieron ciberataques en el 2022 contesto que el costo para el restablecimiento de las actividades por un ataque cibernético fue mayor a 30 millones de pesos.

- Evaluar los costos de la materialización de los riesgos potenciales de seguridad la informática.

7.1.4 Análisis de resultados

Basándonos en los resultados obtenidos a través de la aplicación de las dos encuestas, para el caso de las empresas que han sufrido ataques cibernéticos experimentaron un impacto significativo en la continuidad de sus actividades y la pérdida de información. Más del 50% de las actividades y la disponibilidad de información se vieron afectadas por estos ataques. Estos resultados resaltan la importancia de implementar medidas de ciberseguridad efectivas para mitigar el impacto de posibles incidentes.

Además, se observó que el tiempo requerido para restablecer las actividades posteriores a un ciberataque fue en la mayoría de los casos mayor a 4 semanas. Este período prolongado destaca la necesidad de que las organizaciones cuenten con planes de contingencia y recuperación para acelerar la recuperación y minimizar el tiempo de inactividad.

El impacto experimentado por las organizaciones en la continuidad de sus servicios fue significativo, afectando más del 50% de su prestación. Esto resalta la importancia de proteger los sistemas y datos críticos para garantizar la continuidad de los servicios y la confianza de los usuarios.

Asimismo, se observó que el costo destinado para restablecer las actividades posteriores al ataque cibernético fue mayor a 30 millones en la mayoría de los casos. Esta materialización de los riesgos en temas de seguridad informática indica que las consecuencias económicas de un ciberataque son significativas, especialmente para las pequeñas empresas que quizás pueden no contar con la capacidad financiera para hacer frente a estos elevados y no proyectados costos, lo que puede afectar su continuidad. Esto enfatiza la importancia de asignar un presupuesto adecuado para la ciberseguridad y la protección de la información en cualquier compañía.

Aunque la mayoría de las organizaciones encuestadas cuentan con políticas o procedimientos para el respaldo de la información, también se observa cierto grado de desconocimiento en algunos casos. Esto crea susceptibilidad hacia los ataques

cibernéticos y destaca la importancia de establecer políticas claras de respaldo de información y garantizar su implementación y cumplimiento en toda la organización.

Es alentador ver que la mayoría de las organizaciones establecen y cumplen con programas de formación en seguridad informática. La capacitación adecuada del personal es fundamental para crear conciencia sobre los riesgos cibernéticos y promover prácticas seguras en el manejo de la información. Esto beneficia tanto a las compañías como a las personas, ya que la delincuencia cibernética no solo afecta a las empresas, sino a cualquier individuo.

Aunque exista cierto desconocimiento sobre la implementación de la Gestión del Riesgo en Seguridad Informática en algunas organizaciones, es prometedor ver que varias de ellas tienen este enfoque implementado y lo evalúan de manera constante. La Gestión del Riesgo en Seguridad Informática es fundamental para identificar y mitigar los riesgos de seguridad de manera proactiva.

Respecto a las Empresas en las que se evaluó si cuentan con la implementación de Gestión de Riesgos en tema de Ciberseguridad, se observa que la mayoría de las organizaciones encuestadas cuentan con políticas y procedimientos para el respaldo de la información, realizan auditorías internas de Tecnología de Información, asignan presupuesto para la protección de la información y tienen implementada la Gestión del Riesgo en Seguridad Informática. Esto indica que existe cierto nivel de conciencia y medidas de seguridad implementadas en las algunas organizaciones en Colombia.

7.1.4.1 Beneficios vs sobrecostos de la gestión de riesgos

Dentro de las organizaciones es importante conocer los beneficios y sobrecostos de la implementación del sistema de gestión de riesgos de la seguridad informática. La siguiente tabla resume los beneficios y sobrecostos.

Tabla 10. Beneficios vs sobrecostos de la gestión de riesgos

Beneficios	Sobrecostos
• Facilita la detección y gestión de los riesgos y peligros que enfrenta la empresa en el corto y largo plazo. • Proporciona de manera efectiva la protección de la privacidad de la información personal de los empleados y clientes. • Preserva la integridad de los dispositivos al aplicar medidas de seguridad en el software y el hardware, garantizando su protección y un rendimiento óptimo a largo plazo • Minimiza la probabilidad de ocurrencia de pérdidas de información en las empresas, abarcando tanto situaciones de robo como de manipulación corrupta de los datos. • Proporciona un enfoque metodológico que permite administrar de manera clara y concisa la seguridad de la información. • Mejora la eficiencia de los procesos de información, lo que conlleva una disminución de los costos asociados.	• La implementación de un sistema de gestión de seguridad informática puede representar un costo considerable para las empresas. Aquellas organizaciones que no cuentan con los recursos financieros necesarios para salvaguardar sus datos y sistemas pueden verse en desventaja significativa. • Costos de adquisición: Los gastos relacionados con la adquisición de software, hardware y herramientas especializadas para la seguridad informática pueden representar una inversión inicial significativa. • Costos de personal: Es posible que se requiera contratar personal especializado en seguridad informática o capacitar al personal existente para que adquiera las habilidades necesarias. Esto puede implicar costos de contratación, salarios más altos o gastos de formación. • Costos de auditoría y certificación: Si la empresa decide obtener una certificación o realizar auditorías periódicas para garantizar el cumplimiento de los estándares de seguridad, habrá costos asociados a estos procesos.

Fuente: Elaboración propia

Tabla 13. Beneficios vs sobrecostos de la gestión de riesgos (continuación)

Beneficios	Sobrecostos
• Contar con un sistema de gestión de seguridad de la información que cumpla con la norma ISO 27001 es una valiosa herramienta que desbloquea oportunidades en nuevos mercados y atrae a nuevos clientes. En otras palabras, brinda a la empresa una ventaja competitiva significativa, especialmente en aquellas organizaciones que manejan información altamente confidencial. • Se produce un aumento en el compromiso interno, ya que el sistema asegura la efectividad de los esfuerzos realizados en la gestión de la seguridad de la información.	• La implementación de un sistema de gestión de seguridad informática puede representar un costo considerable para las empresas. Aquellas organizaciones que no cuentan con los recursos financieros necesarios para salvaguardar sus datos y sistemas pueden verse en desventaja significativa. • Costos de adquisición: Los gastos relacionados con la adquisición de software, hardware y herramientas especializadas para la seguridad informática pueden representar una inversión inicial significativa. • Costos de personal: Es posible que se requiera contratar personal especializado en seguridad informática o capacitar al personal existente para que adquiera las habilidades necesarias. Esto puede implicar costos de contratación, salarios más altos o gastos de formación.

Fuente: Elaboración propia

Tabla 13. Beneficios vs sobrecostos de la gestión de riesgos (continuación)

Beneficios	Sobrecostos
• Se garantiza el cumplimiento de las leyes nacionales e internacionales que regulan el manejo y la protección de datos en todos los niveles de la organización.	• Costos de auditoría y certificación: Si la empresa decide obtener una certificación o realizar auditorías periódicas para garantizar el cumplimiento de los estándares de seguridad, habrá costos asociados a estos procesos. • Costos de mantenimiento y actualización: Los sistemas de seguridad informática requieren un mantenimiento regular y actualizaciones para mantenerse al día con las nuevas amenazas y vulnerabilidades. Estos costos pueden incluir licencias de software, renovaciones de hardware y servicios de soporte técnico. • Costos de tiempo y productividad: La implementación y gestión de un sistema de gestión de riesgos de seguridad informática puede requerir tiempo y recursos de personal, lo que puede afectar la productividad en otras áreas de la empresa

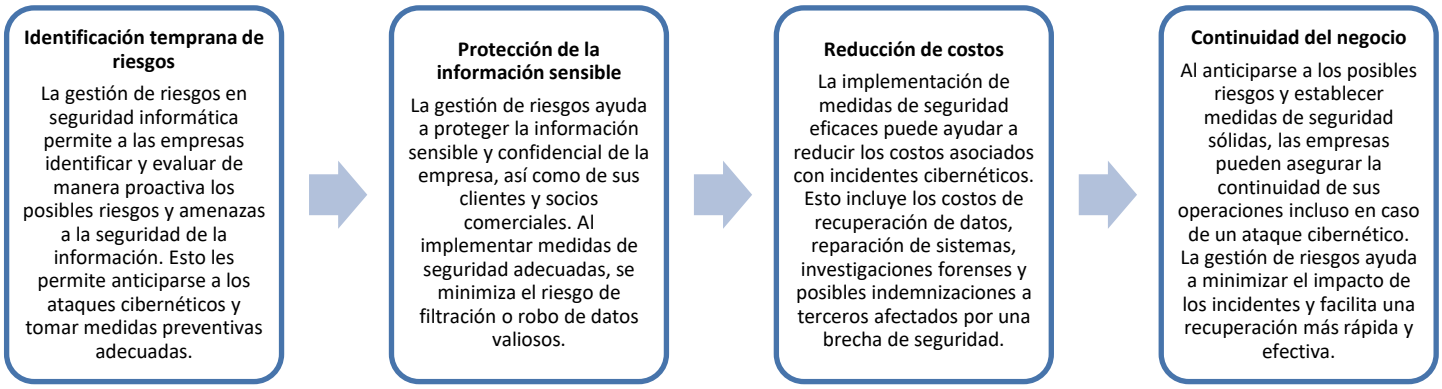
Fuente: Elaboración propia

7.1.4.2 Ventajas de la implementación de la gestión de riesgos en seguridad informática

Las ventajas de la implementación de la gestión de riesgos de seguridad informática se reflejan en la capacidad de las organizaciones para respaldar la información, ejecutar auditorías internas, establecer programas de formación en seguridad informática, contar con políticas regulatorias, implementar dispositivos de control de software y asignar presupuesto para la adquisición y mantenimiento de tecnología de protección de la información., con el fin de resguardar la información la cual es clave para la continuidad de cualquier compañía, así como el poder prestar sus servicios oportunamente.

Otras de las principales ventajas que conlleva la implementación de la gestión de riesgos en seguridad informática se describen en la siguiente figura.

Figura 5. Ventajas de la Implementación de la Gestión de Riesgos en Seguridad Informática.



Fuente: Elaboración propia.

7.1.4.3 Riesgos potenciales que afectan la seguridad informática

Los riesgos potenciales que afectan la seguridad informática se evidencian en las respuestas relacionadas con el desconocimiento de políticas de respaldo de información, la falta de ejecución de auditorías internas, la ausencia de programas de formación en

seguridad informática, la falta de evaluación constante de la implementación de la Gestión del Riesgo, la falta de renovación de licencias y la falta de direccionamiento hacia el personal respecto al ingreso de los email personal y redes sociales.
En cuanto a los costos, se observa que las organizaciones asignan presupuesto para la adquisición y mantenimiento de tecnología de protección de la información, lo cual indica que existe una inversión en este aspecto. Sin embargo, también se identifican casos en los que no se renuevan adecuadamente las licencias, lo que puede generar costos adicionales en caso de incidentes de seguridad los cuales no todas las compañías podrían estar en la capacidad de afrontar.

7.1.4.4 Costos de la materialización de los riesgos potenciales de seguridad informática

Al presentarse la materialización de los riesgos potenciales en temas de seguridad informática las compañías que son víctimas en ataques cibernéticos deben disponer de presupuesto para poder reactivar las actividades y dar continuidad a la prestación de los servicios de esta. Dentro de estos costos se pueden relacionar:

- Costos de recuperación y reparación: Estos costos están relacionados con las acciones necesarias para restablecer y reparar los sistemas y la infraestructura afectada por un incidente de seguridad. Incluyen la contratación de servicios de expertos en seguridad informática, la adquisición de software y hardware de seguridad, y la restauración de datos y sistemas comprometidos. Estos costos pueden variar dependiendo de la magnitud del incidente y la complejidad de la infraestructura tecnológica de la organización.
- Costos de interrupción del negocio: Cuando ocurre un incidente de seguridad, es común que las operaciones comerciales se vean afectadas y se produzca una interrupción parcial o total en la prestación de servicios. Esto puede resultar en pérdida de ingresos, pérdida de clientes y daños a la reputación de la empresa.

Estos costos pueden variar ampliamente dependiendo del tamaño y la industria de la organización, así como de la naturaleza y la gravedad del incidente de seguridad, sin embargo, de acuerdo con los resultados obtenidos en las encuestas realizadas los costos para la recuperación, reparación de la información y continuidad en la prestación de los

servicios supero los 30.000.000. millones de pesos colombianos, generando así un impacto significativo para las empresas que no contemplaron la asignación de recursos con el fin de evaluar e implementar las medidas necesarias para evitar la materialización de estos riesgos y mantener medidas de ciberseguridad adecuadas.

7.1.4.5 Costo de la implementación del sistema de gestión de riesgos

Los costos de la implementación del sistema de gestión de riesgos varían según el número de colaboradores, la complejidad del software y la cantidad de licencias que se vayan a adquirir.

Como mínimo se necesita 1 gerente y 2 analistas de riesgos de seguridad de la información con su respectivo computador lo que representa una inversión inicial de $16.260.000 COP.

Si se requiere implementar una gestión de riesgos de seguridad de la información más madura se debe adquirir adicionales certificaciones, un software con sus respectivas licencias y mantenimiento lo que representa una inversión inicial de $42.760.000.

Es importante recordar que los anteriores costos pueden aumentar dependiendo la robustez de la gestión que se requiera implementar.

8. CONCLUSIONES

La ciberseguridad es una preocupación que se ha incrementado en el entorno empresarial. La implementación de medidas de ciberseguridad efectivas es fundamental para proteger los sistemas, datos e información de las organizaciones contra posibles amenazas y ataques cibernéticos. Los ciberataques representan un riesgo significativo para la continuidad de las operaciones de las organizaciones. De acuerdo con los resultados obtenidos en las encuestas realizadas demuestran que los ciberataques tienen un impacto significativo en la ejecución de actividades y la disponibilidad de información, afectando la productividad y generando costos significativos de recuperación en las compañías víctimas de estos ataques.

La gestión de riesgos en seguridad informática juega un papel fundamental en la mitigación de los posibles incidentes de seguridad. Establecer políticas claras, implementar medidas de seguridad adecuadas y contar con planes de contingencia y recuperación son aspectos clave para minimizar el impacto de los ciberataques y acelerar la recuperación de las operaciones. Para ello la asignación de un presupuesto adecuado para la adquisición y mantenimiento de tecnología de protección de la información es esencial ya que las organizaciones que invierten en tecnología de seguridad, como licencias actualizadas y renovadas, tienen una mayor capacidad para proteger sus sistemas y datos, los cuales muy difícilmente podrán ser vulnerados.

La concienciación y formación del personal son aspectos cruciales en la ciberseguridad, también se resalta la importancia de establecer políticas claras de respaldo de información y garantizar su implementación y cumplimiento en toda la organización.

Colombia, al igual que muchos otros países, enfrenta desafíos en materia de ciberseguridad. Los costos de materialización de los riesgos potenciales en seguridad informática pueden variar, pero los resultados de las encuestas revelan que estos costos pueden ser significativos, con casos en los que superan los 30 millones de pesos. Esto destaca la necesidad de que las organizaciones asignen recursos financieros adecuados para garantizar la protección de la información.

De acuerdo con esto podemos determinar que la implementación de la gestión de riesgos en seguridad informática genera beneficios a nivel empresarial en Colombia como lo es la protección de la información, concientización sobre los riesgos la negativa a ingresar a enlaces desconocidos en correos electrónicos y la implementación de políticas regulatorias en los sistemas de información indican que las organizaciones están tomando medidas para minimizar los riesgos cibernéticos. Esto demuestra una conciencia de los peligros potenciales y la importancia de mantener prácticas seguras, lo que puede prevenir ataques y sus costos asociados.

Si bien es importante reconocer que la implementación de la gestión de riesgos en seguridad informática conlleva inversiones y costos, los beneficios derivados de estas medidas superan a los posibles gastos. La protección de la información, la mitigación de riesgos, el cumplimiento normativo y la reducción del impacto financiero son aspectos clave que respaldan que la implementación de la gestión de riesgos en seguridad informática genera beneficios a nivel empresarial en Colombia.

REFERENCIAS

Ospina, M., y Sanabria, P. (2020). Desafíos nacionales frente a la ciberseguridad en el escenario global: un análisis para Colombia. Revista Criminalidad, 62(2), 201

Reyna, D., y Olivera, D.A. (2017). Las amenazas cibernéticas. (pp. 49-72).

Unión Internacional de Telecomunicaciones. (2010). Resolución 181: Definiciones y terminología relativas a la creación de confianza y seguridad en la utilización de las tecnologías de la información y la comunicación. Conferencia de Plenipotenciarios. Recuperado de: https://www.itu.int/en/council/Documents/basic-texts/RES-181-S.pdf

Abu, A., Massadeh, D., Bshayred.M, (2023). The impact of the COSO control components on the financial performance in the Jordanian banks and the moderating effect of board Independence. Scopus, 13 (1), 161-175, Recuperado de https://www-scopus-com.bdbiblioteca.universidadean.edu.co/record/display.uri?eid=2-s2.0-85131127461&origin=resultslist&sort=plf-f&src=s&st1=coso&sid=5ec8c132a217508195368ccaca35ab61&sot=b&sdt=b&sl=19&s=TITLE-ABS-KEY%28coso%29&relpos=10&citeCnt=1&searchTerm=

Buchtik, L. (2018). Secretos para dominar la Gestión de Riesgos en Proyectos. España: Buchtik Global

Business Of Marsh Mclennan. (2022). Riesgos de Personas 2022. Recuperado https://www.marsh.com/co/risks/people-risk/insights/the-five-pillars-of-people-risk.html

Calder, A., (2017). Nueve pasos para el éxito: Una visión de conjunto para la aplicación de la ISO 27001:2013. Recuperado de https://eds.s.ebscohost.com/eds/detail/detail?vid=5&sid=8b526229-5136-42f0-8868-ca27cd076391%40redis&bdata=Jmxhbmc9ZXMmc2l0ZT1lZHMtbGl2ZSZzY29wZT1zaXRl#AN=1593794&db=edsebk

Casares, I. 2021. Evolución de la gestión de riesgos en el mundo. Recuperado de https://www.iep.edu.es/evolucion-gestion-riesgos-mundo/#:~:text=En%20la%20d%C3%A9cada%20de%20los,la%20sostenibilidad%20de%20las%20empresas.

Conner, “Threat Intelligence, Industry Analysis and Cybersecurity Guidance for the Global Cyber Arms Race”, SonicWall Inc., Milpitas, California, Cyber threat report, 2018.

G. Rey Diario el Portafolio, 2023 “Porque ha crecido la importancia de la Ciberseguridad”, https://www.portafolio.co/economia/finanzas/ciberseguridad-aumenta-a-la-par-de-los-ataques-ciberneticos-579612.

Gómez, L., Duque, M., Cuervo, J., (2005). Gestión de riesgos en el costeo basado en actividades: una alternativa para su implantación exitosa. Contaduría, 47 (1), 61-85.

Hastings, N., (2015). ISO 55000 Series Standards. Recuperado de https://link-springer-com.bdbiblioteca.universidadean.edu.co/chapter/10.1007/978-3-319-14777-2_29#citeas

J. Cano, Diario el Portafolio, 2017 “El 59% de las empresas locales recortaría gastos en ciberseguridad”, http://www.portafolio.co/negocios/empresas/empresaslocales-recortaria-gastos-en-ciberseguridad-502771.

López Lemos, P. (2016). Novedades ISO 9001:2015. Madrid: Fundación Confemetal.

Ministerio de Tecnologías de la Información y las Comunicaciones. (2022). En el último mes y medio MinTIC ha recibido 36 reportes de ataques cibernéticos en Colombia. https://mintic.gov.co/portal/inicio/Sala-de-prensa/Noticias/273464:En-el-ultimo-mes-y-medio-MinTIC-ha-recibido-36-reportes-de-ataques-ciberneticos-en-Colombia.

Miranda-Calle, J., Vikranth, R. C., Dhawan, P., & Churi, P. (2021). Exploratory data analysis for cybersecurity. World Journal of Engineering, 18(5), 734-749. doi: https://doi.org/10.1108/WJE-11-2020-0560.

Ospina, M., y Sanabria, P. (2020). Desafíos nacionales frente a la ciberseguridad en el escenario global: un análisis para Colombia. Revista Criminalidad, 62(2), 201

Palko, D., Babenko, T., Bigdan, A., Kiktev, N., Hutsol, T., Kuboń, M., . . . Borusiewicz, A. (2023). Cyber security risk modeling in distributed information systems. Applied Sciences, 13(4), 2393. doi: https://doi.org/10.3390/app13042393.

Puche, N., Velásquez, M., Núñez, Y., Rangel, H. (2021). Sistema de Gestión de la Calidad: una visión general desde sus inicios hasta la actualidad. Tekhné, 24 (1), 12-23. Recuperado de https://revistasenlinea.saber.ucab.edu.ve/index.php/tekhne/article/view/4858

Ramírez, A., Ortiz, Z., (2011). Gestión de Riesgos tecnológicos basados en ISO 31000 e ISO 27005 y su aporte a la continuidad de negocios. Ingeniería, 16 (2), 56-66. Recuperado de https://dialnet.unirioja.es/servlet/articulo?codigo=4797252

Reyna, D., y Olivera, D.A. (2017). Las amenazas cibernéticas. (pp. 49-72).

Seguridad Aplicada al Fortalecimiento Empresarial. (2019). Informe Tendencias del Cibercrimen 2019 – 2020. Recuperado dehttps://www.ccit.org.co/wp-content/uploads/informetendencias-cibercrimen_compressed-3.pdf

Seguridad Aplicada al Fortalecimiento Empresarial. (2021). Informe Tendencias del Cibercrimen 2021 – 2021. Recuperado de https://www.ccit.org.co/wp-content/uploads/informesafe-tendencias-del-cibercrimen-2021-2022.pdf

Tamayo, S. y Gonzalez, D. (2020). La gestión de riesgos: herramienta estratégica de gestión empresarial. Recuperado de https://elibronet.bdbiblioteca.universidadean.edu.co/es/ereader/bibliotecaean/131885?page=14

Tonysé de la Rosa, M., (2021). Automation of an information security management system based on the iso / iec 27001 standard. Scopus 13 (1), 495-606, Recuperado de https://www-scopus-com.bdbiblioteca.universidadean.edu.co/record/display.uri?eid=2-s2.0-85116100308&origin=resultslist&sort=plf-f&src=s&st1=iso+27001&nlo=&nlr=&nls=&sid=281a5a538572ec405192501614144f22

&sot=b&sdt=b&sl=24&s=TITLE-ABS-KEY%28iso+27001%29&relpos=44&citeCnt=0&searchTerm=

Unión Internacional de Telecomunicaciones. (2010). Resolución 181: Definiciones y terminología relativas a la creación de confianza y seguridad en la utilización de las tecnologías de la información y la comunicación. Conferencia de Plenipotenciarios. Recuperado de: https://www.itu.int/en/council/Documents/basic-texts/RES-181-S.pdf

Urcuqui, C. C. y Navarro C. A. (2022). Ciberseguridad: los datos tienen la respuesta. (1a ed.). Universidad Icesi. Recuperado de https://elibro-net.bdbiblioteca.universidadean.edu.co/es/ereader/bibliotecaean/225844pg26.

Vargas, N. (25 de enero de 2023). Audifarma, Sanitas, Carvajal y hasta la Fiscalía son algunas de las organizaciones que han sufrido algún tipo de hackeo en los meses recientes. La República. Recuperado de https://www.larepublica.co/empresas/las-empresas-que-han-sidoblanco-de-ciberataques-en-colombia-en-el-ultimo-ano3529667#:~:text=Entre%20enero%20y%20octubre%20de,que%20fueron%20objeto%20de%20 hackeo

Ortiz, M. (2022). “Directorio Estadístico de Empresas 2019 – 2021”. Recuperado de https://www.dane.gov.co/files/investigaciones/boletines/registro-estadistico/boletin-directorio-estadistico-empresas-2019-2021.pdf

Cortés, M. E. C., Villar, N. M., León, M. I., & Iglesias, M. C. (2020). Algunas consideraciones para el cálculo del tamaño muestral en investigaciones de las Ciencias Médicas. MediSur, 18(5), 937-942

Ministerio de Defensa Nacional policía Nacional de Colombia. (2023). Ciber incidentes en tiempo real. Recuperado de: https://www.policia.gov.co/ciberseguridad

Salario medio para Analista Riesgo en Colombia 2023. 2023. Recuperado de: https://co.talent.com/salary?job=analista+riesgo#:~:text=Descubre%20cu%C3%A1l%20es%20el%20salario%20medio%20para%20Analista%20Riesgo&text=%C2%BFCu%C3%A1nto%20gana%20un%20Analista%20riesgo%20en%20Colombia%3F&text=El%20salario%20analista%20riesgo%20promedio,con%20un%20ingreso%20de%20%2425.539.

SERVICIOS DE INSPECCIÓN DIGITAL Y ANALÍTICA DE DATOS, 2023. Recuperado de: https://www.bureauveritas.com.co/es/needs/servicios-de-inspeccion-digital-y-analitica-de-datos

ANEXO 1

Milenio PC

24 de Mayo de 2023 **COTIZACIÓN No. BOG-80254**

Señores:
ONE CLICK SAS
Ing. JULIAN E. RAMIREZ RICO
Autopista NORTE NO 97-50
Bogotá

Relación de los elementos retirados

Cant	Descripción Serial	Costo
1	Computador Portatil HP Core i5-7200U	$220.000

OBSERVACIONES:

Sin observaciones

ANEXO 2

One-Click

Transformación digital, gobierno corporativo y automatización

ONE CLICK
SOLUTIONS S.A.S
NIT 900.483.274 – 8

COTIZACIÓN GESTIÓN DE RIESGOS EMPRESARIAL

Es grato para nosotros saber su interés por conocer nuestra propuesta de servicios de implementación de software para la Gestión de Riesgos Empresarial. Los costos relacionados en este documento están sujetos al estudio realizado previamente de la empresa, los requerimientos, las personalizaciones, la licencias y los servicios requeridos.

Antes de tomar la decisión se recomienda agendar una sesión de preventa donde se realizará una demostración con data real de la empresa o si se requiriere con data de prueba.

Servicio	Costo aproximado
Implementación de Software In-House con 3 escritorios, 1 licencia estática, levantamiento de requerimientos, documentación de requerimientos y garantía por 2 meses después de entregado el software. No incluye cargue de información, capacitaciones, soporte, manuales. La entidad adquiriente debe contar con una infraestructura tecnológica robusta.	$660.000
Implementación de Software Hopex V5.CP4, 4 licencias flotantes, levantamiento de requerimientos, documentación de requerimientos, garantía por 2 meses después de entregado el software, manuales, capacitación técnica y funcional de 20 horas, bolsa de horas para soporte de 200 horas, cargue de información. La entidad adquiriente debe contar con una infraestructura tecnológica robusta.	$870.000.000

Autopista Norte # 97-50 Oficina 804 Bogotá – Colombia

(+57 1) 743 76 28 – (+57 1) 743 76 29

Tarifas de referencia validas por 26 días hábiles a partir de hoy 1 de Junio 2023.

Cordialmente,

María del Pilar Gómez Trujillo
Consultor Comercial
maria.gomez@oneclick-sas.com
One-Click Solution S.A.S.