Institución Universitaria

Construcción de un modelo de ciberseguridad para empresas de servicios informáticos que fortalezca un adecuado manejo de incidentes de seguridad

Yenifer Zulay Giraldo Montes

Instituto Tecnológico Metropolitano

Facultad de Ingenierías

Medellín, Colombia

2020

Construcción de un modelo de ciberseguridad para empresas de servicios informáticos que fortalezca un adecuado manejo de incidentes de seguridad

Yenifer Zulay Giraldo Montes

Tesis o trabajo de investigación presentada(o) como requisito parcial para optar al título de:

Magister en Seguridad Informática

Director (a):

Magister Héctor Fernando Vargas Montoya

Línea de Investigación:

Ciencias computacionales

Instituto Tecnológico Metropolitano

Facultad de Ingenierías

Medellín, Colombia

2020

Al iniciar este proyecto, mi familia ha hecho parte de cada momento, durante este tiempo cada uno de ellos estuvieron acompañando mi alma, algunos me regalaron tiempo, otros amor, otros comprensión y otros felicidad.

Es por ello que dedico a cada integrante de mi familia esta tesis.

A mi esposo, quien fue parte fundamental como apoyo moral, su exigencia me lleno de fortaleza para comprender la importancia de cerrar ciclos.

A mi mascota Lola, quien durante todas las noches fue mi compañera de clase durante la pandemia y me regalo su presencia cada día para documentar cada hoja de este proyecto.

A mi hijo quien llegó sorpresivamente finalizando esta travesía, y aún así me permitió terminar este proyecto entregándome la fuerza necesaria aprender que una nueva vida no apaga sueños.

Agradecimientos

El inmenso esfuerzo que conlleva la realización de una tesis es igual al orgullo que se siente al finalizarla. Y detrás de la realización de una tesis, hay un conocimiento que se adquiere de varios seres que han dispuesto su vida a enseñar y entregar su conocimiento con el mero propósito de transformar el mundo.

Es por ello que agradezco a cada uno de los profesores de la maestría que con tanta dedicación acompañaron mi proceso académico, cada uno de ellos sembró semillas que serán cosechadas en cada paso que doy académica y laboralmente, resaltando la labor del Magister Héctor Vargas Montoya quien participo durante todo este proyecto de manera activa, con paciencia, dedicación, generosidad, solidaridad y lleno mi travesía de perseverancia.

A todos infinitas gracias, por ser el faro que ilumina el camino de todos los estudiantes.

Resumen

Este proyecto busca construir un modelo de ciberseguridad basado en el análisis de riesgos, con el objeto de fortalecer un adecuado manejo de incidentes de ciberseguridad para todas las operaciones que ofrecen servicios informáticos.
Para la consecución de este objetivo se inicia con la detección de los riesgos para empresas que ofrecen servicios informáticos, para ello se apoya de la norma ISO 27005:2018 que establece los procedimientos necesarios para el manejo y detección de riesgos de seguridad, iniciando por un proceso de identificación de activos para luego analizar sus escenarios de riegos y posterior definir los controles adecuados que permiten mitigar los impactos de la materialización de un riesgo; a fin de garantizar un adecuado manejo de incidentes de ciberseguridad se realiza la selección de las normas adecuadas que permitan fortalecer el proceso de incidentes basados en criterios selectivos y posterior a ello se construye el modelo de ciberseguridad, incluyendo dentro del manejo de incidentes los riesgos críticos y los controles adecuados para el cumplimiento del objetivo del proyecto.

Palabras clave: Controles de seguridad informática, Gestión de riesgos, Manejo de incidentes de seguridad, Modelo de seguridad.

Abstract

This project seeks to build a cybersecurity model based on risk analysis, in order to strengthen an adequate management of cybersecurity incidents for all operations that offer IT services.
In order to achieve this objective, it starts with the detection of risks for companies that offer IT services, for this purpose it is supported by the ISO 27005: 2018, which establishes the necessary procedures for the management and detection of security risks, starting with a process of identification of assets to then analyze their risk scenarios and subsequently define the appropriate controls that allow mitigating the impacts of the materialization of a risk; in order to ensure proper management of cybersecurity incidents, the selection of appropriate standards that allow strengthening the incident process based on selective criteria is performed and after that the cybersecurity model is built, including within the incident management the critical risks and appropriate controls for the fulfillment of the project's objective.

Keywords: IT security controls, Risk Management, Security Incident Management, Security Model.

Contenido

Contents

Lista de ilustraciones

Lista de Tablas

Lista de Símbolos y abreviaturas

A continuación, se presentan las abreviaturas utilizadas:

Abreviatura	Término
ISO	organización Internacional de estandarización
ITU	Unión Internacional de Telecomunicaciones
MINTIC	MiNISTerio de Tecnologías de la Información y Comunicaciones
NIST	Instituto Nacional de Estándares y Tecnología
AGESIC	Agencia de Gobierno electrónico y Sociedad de la Información y del Conocimiento
CMA	Evaluación de madurez cibernética
CSIRT	Equipo de Respuesta ante Emergencias Informáticas
PHVA	Planear, Hacer, Verificar Actuar
SAN	Red de área de almacenamiento
NAS	Network Attached Storage
NTP	Network Time Protocol
DHCP	Dynamic Host Configuration Protocol
RDP	Remote Desktop Protocol
SSH	Secure SHell
SBA	Survivable Branch Appliance
SIP	Session Initiation Protocol
PRTG	Software de monitorización de red,
XSS	Cross-Site Scripting

DoS/DDoS	Denial-of-service/ Denial-of-service Distributed
CSRF	Cross-Site Request Forgery
ETC	Etcétera
IP	Internet Protocol
PHVA	Planear, hacer, verificar y actuar
ARO	Análisis de riesgo operativo
SIEM	Gestión de eventos e información de seguridad
IT	Tecnologías de información

Introducción

El uso de las tecnologías de información y comunicaciones en las organizaciones, así como la cuarta revolución industrial, tiene un sello intrínseco en la tecnología, el know-how que ofrece permite la masificación, diversificación y transferencia de la información que hoy generan las compañías por medio del ciberespacio, es un fenómeno que apalanca la evolución tecnológica, sin embargo, trae consigo niveles de exposición que pueden causar daños sobre la información propia de cada organización, es por esto que los esfuerzos en implementar sistemas que permitan mitigar los riesgos de ciberseguridad deben realizarse de manera recurrente, es así que el objetivo principal de este trabajo está fundado en la "*construcción de un modelo de ciberseguridad para empresas que ofrecen servicios informáticos con base en referentes nacionales e internacionales, para establecer un adecuado manejo de incidentes de seguridad."*

Colombia ha crecido en inversiones de seguridad de manera progresiva, sin embargo, aún no es suficiente para el alto crecimiento en ataques cibernéticos que se presentan con la rápida convergencia tecnológica, para el 2019 solo un 70% según ACIS, "Ciberriesgos - Un riesgo sistémico," indicaron que cuentan con presupuestos asignado para la seguridad digital de sus organizaciones, una cifra que llama bastante la atención ya que para ese mismo año a un 54% de los encuestados se les presentaron incidentes de seguridad que terminaron interrumpiendo los servicios de las organizaciones [1], esto nos hace cuestionar entonces cómo hoy las organizaciones definen la postura de seguridad desde la administración del presupuesto asignado para contener los incidentes de seguridad informática.

Hoy las compañías deben contemplar la creación de estrategias que permitan estar alineados con los sucesos de seguridad que se vienen presentando; acorde a la empresa especializada en seguridad Kaspersky [2] , en Latinoamérica entre julio del 2018 y julio del 2019, los bloqueos más recurrentes que realizaron fue por consecuencia de una infección por algún tipo de malware en ese sentido, y como una reafirmación de la problemática de la región, la Asociación Colombiana de Ingenieros de sistemas[1] , informa que el 41% de las problemáticas de seguridad son asociadas a errores humanos, mientras que el 24% y el 22% corresponde al phishing e instalación de software no autorizado (respectivamente). Esto deja en evidencia que los ataques más comunes siguen siendo el frente que más usan los ciberdelincuentes para penetrar en las organizaciones, a continuación, se presentan los objetivos específicos de este proyecto cuya finalidad busca endurecer los controles asociados a la prevención de los eventos de seguridad por ataques recurrentes y en caso de que los controles no sean efectivos integra un sistema de gestión de incidentes que permite tener un modelo que cubre ambos frentes trabajando de manera sistemática.

Objetivo General

Construir un modelo de ciberseguridad para empresas que ofrecen servicios informáticos con base en referentes nacionales e internacionales, para establecer un adecuado manejo de incidentes de seguridad.

Objetivos específicos:

- ✓ Establecer los diferentes riesgos de ciberseguridad en empresas que ofrecen servicios informáticos.
- ✓ Caracterizar diferentes normas para manejo y respuesta de los incidentes de seguridad, acorde a los riesgos detectados y la aplicabilidad en empresas de servicios informáticos.
- ✓ Evaluar el modelo de ciberseguridad para el manejo de incidentes a través de un caso de estudio.

Al desarrollar estos objetivos se aborda la problemática actual, trabajando desde la perspectiva de fortalecer el manejo de incidentes iniciando por la identificación de los riesgos y definiendo controles adecuados que permiten mitigar los impactos y establecer cómo se deben abordar adecuadamente los incidentes de ciberseguridad que se materializan debido a la falta de eficiencia de los controles que se establecieron bajo el procedimiento de los riesgos críticos detectados para empresas del sector.

El informe se presenta de manera secuencial de acuerdo a el cumplimiento del primer objetivo, iniciando por la caracterización de los riesgos que presentan las empresas del sector informático para desarrollar la estrategia que permite fortalecer el adecuado manejo de incidentes de seguridad a fin de garantizar la construcción y evaluación del modelo de ciberseguridad

1. Marco Teórico y Estado del Arte

1.1 Marco teórico

La Ciberseguridad es un concepto que nace alrededor de las interconexiones que se realizan para la transferencia de contenido, tiene como finalidad proteger todo lo que viaja a través de los sistemas informáticos, es definida por la Unión Internacional de telecomunicaciones - ITU [3] como el conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el entorno cibernético, un concepto que se usa en el proyecto para iniciar el proceso de la gestión de riesgos con el objeto de articularlo con la gestión de incidentes de seguridad como parte de aseguramiento tecnológico abarcando en gran medida de la definición dada por la ITU.

El objetivo de la gestión de riesgos dentro del proyecto es crear estrategias que permitan la mitigación de los escenarios que causan las vulnerabilidades; las cuales son debilidades que tienen todos los sistemas, y comúnmente suelen presentarse por diversos factores entre ellos técnicos e incluso en algunos casos son nativas de los activos, además suelen ser explotadas por las amenazas, ya que son agentes que por diversas causas se aprovechan de las vulnerabilidades existentes para causar daños. Las amenazas suelen ser clasificadas de acuerdo a la categoría y se pueden presentar como naturales o humanas, voluntarias e involuntarias. [17]

Teniendo en cuenta que el ciberespacio como parte de sus componentes contempla los activos de las organizaciones nace el concepto ciber-riesgo o riesgo cibernético el cual se define [4] como la probabilidad de que ocurra un evento sobre los recursos informáticos por consecuencia de la materialización de un incidente de seguridad, es así como dentro del sistema de ciberseguridad que se construyó en este proyecto se debe calcular el ciber-riesgo y reconocer como parte de un sistema para gestionar e integrar de manera transversal en los procesos intrínsecos de la ciberseguridad.

Una de las estrategias que plantea el proyecto para abordar el ciber-riesgo es la implementación de controles, los controles suelen ser todas las inversiones estratégicas o técnicas que se implementan en una organización para mitigar los escenarios de riesgo

que surgen a partir de las vulnerabilidades y las posibilidades de ser explotadas por la diversidad de amenazas. Los controles de acuerdo al mismo, acarrean esfuerzos en costos, tiempo y algunos suelen ser más fácil de implementar que otros, sin embargo, la implementación de controles por sí solo no son una garantía para la mitigación de un riesgo, un sistema de riesgos para ser eficiente además de la implementación de controles debe contener estrategias que permitan monitorear la efectividad y a partir de allí crear actividades relacionadas con la mejora continua.

Debió al crecimiento de los riesgos cibernéticos las organizaciones se encuentran adaptando modelos de seguridad que incluyan buenas prácticas, para lo cual, según MINTIC [5] en su modelo de seguridad permite que las entidades puedan gestionar adecuadamente la seguridad y privacidad de sus activos de información, lo que conlleva a garantizar privacidad en los datos que se procesan dentro de los sistemas.

Así mismo las organizaciones deben incorporar en sus procesos la gestión de riesgo, ya que es un mecanismo que permite valorar la posición actual en seguridad de las compañías. [6] MINTIC define la gestión de riesgos como un proceso sistémico que se realiza para detectar los riesgos a los cuales están sometidos los activos de una organización con el fin de evitar vulnerabilidades, amenazas, eventos o incidentes de seguridad, su objetivo es conocer cuál es la probabilidad que una amenaza se concrete y mitigar ese riesgo con la implementación de políticas de seguridad.

En la actualidad se presentan una serie de normas internacionales como la ISO 31000 [7] que es definida como una norma que permite proporcionar principios y directivas eficaces para el tratamiento y la gestión de riesgos. ISO31000 ayuda a las organizaciones a identificar, analizar, evaluar y tratar sus riesgos con el fin de mejorar las técnicas de gestión de riesgos y garantizar así la seguridad en el lugar de trabajo en todo momento, permite realizar la identificación riesgos a nivel general, por su parte la ISO27005:2018 es un conjunto de lineamientos con un enfoque en seguridad informática usada para el desarrollo de este proyecto como un conjunto de directrices orientados en la gestión de riesgos de seguridad de la información basada en un ciclo PHVA que permite la identificación del alcance del sistema y a partir de allí se reconocen los activos con sus respectivos escenarios de riesgos a los cuales se les realiza una evaluación del impacto de acuerdo a las probabilidades que se puedan presentar, con el objeto de identificar los riegos que son

inadmisibles para las organizaciones a fin de iniciar procesos de priorización que permiten la implementación de controles enmarcados dentro de un plan de tratamiento que debe ser medible, monitoreado y comunicado a toda la organización dentro de ciclos iterativos que permitan la implementación de estrategias enfocadas a la mejora continua.

La gestión de riesgo dentro de un modelo de seguridad aporta a la reducción de los niveles de riesgo y expone los riesgos que deben ser aceptados, transferidos o tratados por las organizaciones; este tipo de variables contemplan soluciones proactivas ante diversas situaciones, sin embargo, dentro de un modelo de seguridad se deben contemplar varios parámetros para que el modelo sea escalable, adaptable y sostenible en el tiempo, conceptos como el manejo de incidentes de seguridad dentro del modelo permite ser predecible ante ciertas situaciones de riesgo.

Según MINTIC [5] El objetivo principal del modelo de gestión de incidentes de seguridad de la información es tener un enfoque estructurado y bien planificado que permita manejar adecuadamente los incidentes de seguridad de la información, pero el documento hace una descripción general del modelo y muy asociado a las empresas de telecomunicaciones, por otro lado, [8] R. Delvasto Ramírez la describe la gestión de incidentes como la capacidad para gestionar de manera efectiva eventos inesperados que pueden perjudicar la operación de las organizaciones y tienen como fin minimizar su impacto y mantener o restaurar las operaciones dentro de los tiempos establecidos.

Por otro lado, ISO Publica la norma ISO / IEC 27035-1: 2016 como un apartado especializado para la gestión de incidentes de seguridad de la información, dicha norma consta de 2 principios, gestión de incidentes y las pautas para planificar y prepararse para la respuesta a incidentes, el apartado no es una guía completa, sino una referencia para ciertos principios fundamentales que tienen la intención de garantizar que las herramientas, técnicas y métodos se puedan seleccionar de manera adecuada y se demuestre que son óptimos para el propósito en caso de necesidad.

Por su parte NIST SP 800-61 [9] define la respuesta a incidentes de seguridad como un componente importante de la tecnología de la información, ya que los ataques relacionados con ciberseguridad no solo se han vuelto más numerosos y diversos sino dañinos y cada vez más perjudiciales, para los sistemas de información. La referencia en mención entrega

una guía con una serie de pasos a seguir para manejar los incidentes de seguridad, los cuales tienen bajo su responsabilidad preparar, detectar, analizar, contener, erradicar, recuperar y realizar actividades que prevengan un incidente de seguridad similar.

La implementación de todas estas estrategias dentro del desarrollo del proyecto se orienta en organizaciones que prestan servicios informáticos; los cuales son aquellos procesos de apoyo para el desarrollo de los actividades core de cualquier organización; en la actualidad con la acelerada transformación tecnológica que se presenta en el entorno digital todas las organizaciones se han migrado a sistemas digitales para aprovechar el beneficio del Big-data, para que una organización pueda incluirse dentro de estos ecosistemas independiente de su conocimiento requiere el uso de servicios especializados con el del manejo de sistemas como la mensajería electrónica (Outlook, teams), el desarrollo de programas incluyendo las capas de traducción que permiten la comunicación y la administración de datos en aplicaciones distribuidas (sistemas middleware) [22], además requieren personal especializado que preste soporte a sus usuarios finales para hacer uso y sacar provecho de sus sistemas digitales, servicios referentes a la administración y soporte de sistemas como las bases de datos, servicios de despliegues que permiten la distribución masiva de actualizaciones, el manejo y uso de comunicaciones unificadas enfocadas en los servicios de video conferencias y todo lo relacionado al ciclo de vida de productos como el almacenamiento (storage), virtualización, y sistemas en cloud. [23]

1.2 Estado del arte

Entender el contexto actual y conocer los antecedentes con relación a la seguridad informática permite tomar las acciones correctas para enfrentar la transformación digital y los riesgos que existen en ella.

Un modelo de ciberseguridad [19] implica la prevención, detección, reacción o respuesta, y debe incluir un elemento de aprendizaje para la mejora continua del propio proceso. Este trabajo contiene una selección de exhaustiva de 201 estudios relevantes en modelos de madurez de ciberseguridad el cual expone la usabilidad de los modelos existentes en relación con el tema, lo cual provee material para la investigación propuesta ya que a partir de los modelos de ciberseguridad más usuales y otras variables expuestas en el artículo se puede determinar un modelo que se adapte a las necesidades de una empresa de servicios informáticos.

[11] ISACA expone un modelo de ciberseguridad de AGESIC basado en el NIST y contextualizado a los organismos pertenecientes a la administración central, para su implementación define un modelo de madurez llamado Cyber Maturity Assessmentde (CMA) que permite por medio de una visión periférica de personas, procesos y tecnología entender la ciberseguridad desde un punto de vista holístico. Este tipo de modelos supone un punto de partida para la solución del planteamiento del problema, su implementación aumenta la creación de modelos de ciberseguridad a partir de los frentes bajo los cuales se estructuran las organizaciones, personas, procesos y tecnologías permitiendo ordenar los temas y facilitar la planificación o los planes de acción de ciberseguridad.

La literatura encontrada no solo indica que la mitigación de los riesgos se enfrenta por medio de modelos cibernéticos de seguridad, también expone el manejo de incidentes de seguridad como un mecanismo para abordar la problemática del tema central de investigación.

Para Sabillon [12] establecer un modelo de auditorías en los temas de ciberseguridad es fundamental y con ello la posibilidad de poder validar, medir y verificar el estado de los riesgos y el nivel de madures de la seguridad en sí. Los autores plantean un modelo que permite abordar las amenazas, los riesgos y los ataques cibernéticos en entidades privadas o públicas, haciendo una revisión de metodologías de auditoría a aplicar, pero dichos procesos se deben hacer en consideración de un modelo ya establecido o la proyección de poder tener un modelo de ciberseguridad empresarial, los autores no establecen la forma como debería implementarse el modelo, pero si el proceso de auditoría sobre uno ya existente.

Un informe de los hallazgos iniciales y una propuesta de solución conceptual es entregado por los autores Rathod and T. Hämäläinen [12] en el documento plantean los retos de la ciberseguridad y como se encuentra el estado actual, se establece una serie de prácticas segmentadas para tratar diferentes problemáticas, las reducciones de los eventos de ciberseguridad también son fragmentados en su solución. Parte de la solución conceptual está basada en el costo-beneficio y modelo financiero que se debe afrontar desde las organizaciones, sin embargo, no establecen modelos ni estrategias de ciberseguridad técnicas o funcionales que ayude a la reducción de los riesgos o que puedan ser aplicados a una organización que ofrezca servicios.

[14] R. Paredes, mediante el diseño y dimensionamiento de un equipo de respuesta ante incidentes de seguridad informática (CSIRT), realiza la implementación y valoración de los equipos de respuesta a incidentes de seguridad para un caso de estudio, es una propuesta que le apuesta al desarrollo de los grupos de respuesta ante incidentes informáticos, allí exponen la estructura organizacional del CSIRT lo que sirve como entendimiento para la formación de los aspectos claves del modelamiento adecuado para el manejo de incidentes de seguridad

[15] Chicano, describe una guía que entrega conceptos generales acerca de los tipos de incidentes, como prevenirlos , como gestionarlos así como medidas de incidentes, controles, respuesta a incidentes procesos de notificación, etc., a pesar de su época de publicación es una guía importante dentro del trabajo ya que permite entender la taxonomía de los ataques que aunque hoy en día se presentan ataques más sofisticados en la referencia mencionada se puede observar que muchos de los ataques de hoy son mutaciones de los ataques mencionados en la referencia, además expone la arquitectura de los sistemas de prevención que hoy en día aún suelen usarse para lidiar con las incidencias actuales.

R. Delvasto ramírez [8] Diseña un modelo para la gestión de incidentes de seguridad de la información para empresas PyMEs con el fin de mejorar la atención de incidentes de seguridad, su objetivo principal es permitir a las entidades detectar, reportar, contener y recuperarse de un evento no controlado, es un proyecto que entrega el paso a paso para la construcción de un modelo de gestión de incidentes; sin embargo es un modelo basado en las mejores prácticas, lo cual podría no ser suficiente en medio de la rápida transformación digital que presenta la nueva era, la ambición del proyecto en asunto es fundamentar el manejo de incidentes de seguridad desde un modelo de ciberseguridad que este adaptado a los activos de un sector específico y así evitar que este proceso presente obsolescencia en el tiempo.

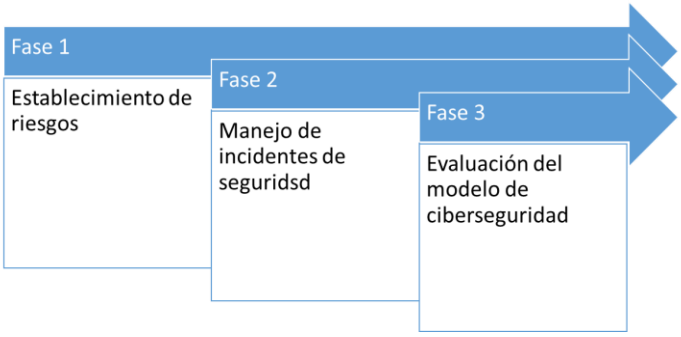
[16] la guía de gestión de incidentes de seguridad de la información para la oficina de tecnología de la información y la comunicación tiene un acercamiento con el trabajo en asunto ya que genera una guía completa de gestión de incidentes de seguridad de la información para un caso de estudio, el documento articula la gestión del riesgo con el manejo de incidentes de seguridad y diseña una propuesta para la gestión de incidencias de seguridad con el fin de dar una respuesta efectiva y reducir los tiempos de atención, en su contenido establece de forma muy clara los procesos de incidentes adaptados a la necesidad propia de la organización en estudio y entrega una guía para el tratamiento de incidentes catastróficos, es un trabajo que brinda un norte al autor de este proyecto para la construcción del modelo de incidentes de seguridad, sin embargo al no correlacionar ciberseguridad en su ciclo de vida integral podría presentar falencias de tipo estructural al momento de su misma ejecución.

Las citas mencionadas en el estado del arte dejan en evidencia como el crecimiento en el tema surge de manera exponencial y muestran la importancia de plantear soluciones apropiadas para la diversidad de situaciones que se presentan hoy día con la evolución tecnológica, las organizaciones para solventar esta situación ponen en práctica modelos de seguridad estandarizados, ya que muchas de las soluciones que incluyen en sus procesos no se ajustan a sus necesidades propias de un mercado.

2. Metodología

Para el desarrollo del proyecto se definieron tres fases (en coherencia con los objetivos establecidos), correspondientes a cada uno de los objetivos específicos y cada fase tiene unas actividades puntuales que se desarrollaron para dar cumplimiento a dicha fase (Figura 2-1).

Ilustración 2-1: Metodología usada para desarrollar los objetivos

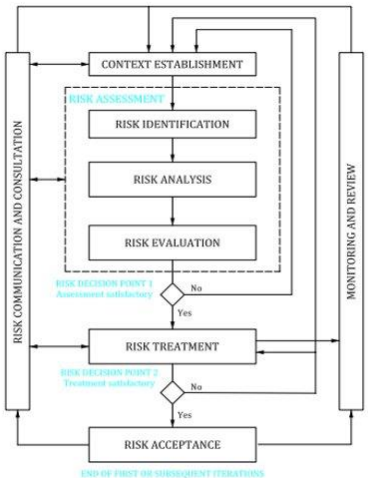


2.1 Fase 1 Establecer los diferentes riesgos de ciberseguridad en empresas que ofrecen servicios informáticos.

2.1.1 Obtener los diferentes riesgos de ciberseguridad en empresas que ofrecen servicios informáticos, con base en el uso de la norma ISO 27005:2018 y su proceso de gestión

Para establecer los diferentes riesgos de ciberseguridad en empresas que ofrecen servicios informáticos, estos se obtuvieron con base en el uso de la norma ISO 27005:2018 y su proceso de gestión, se establecieron los procedimientos dados por la norma descrita, los cuales se encuentran definidos en la siguiente imagen:

Ilustración 2-2: Proceso gestión de riesgos de seguridad de la información. [17]



Dado lo anterior, el procedimiento general ejecutado para la obtención de los riesgos fue:

a) Definición del contexto y alcance.
b) Caracterización de servicios tecnológicos y los activos de información sobre dichos servicios.
c) Clasificación de los activos, vulnerabilidades y controles actuales (con la respectiva medición de efectividad).
d) Obtención de amenazas y cruce de escenarios de riesgos.
e) Definición de las tablas de probabilidad e impacto.
f) Calificación de los escenarios de riesgos y obtención del mapa de aceptabilidad.
g) Finalmente, definición del plan de tratamiento sobre los riesgos encontrados.

En la primera etapa, el contexto establecido es el que se indicó en el objetivo general, esto es, las empresas de servicios informáticos, y dentro de este contexto se define un alcance basado en los servicios más relevantes ofrecidos (tabla 2-1) por una empresa del sector, para lo cual se determinó evaluar los servicios que presta una organización del sector versus los servicios consumidos por sus clientes, con esto se pretende encontrar cuales son los servicios más recurrentes y enfocar el análisis en lo que demanda el mercado actual.

Tabla 2 1 Caracterización de los productos de una empresa de servicios informáticos

PLATAFORMASADMINISTRADAS	Cliente A	Cliente B	Cliente C	Cliente D	Cliente E	Cliente F	Cliente G	Cliente H	Cliente I	Cliente J	Total
MESA DE SOPORTE											
OFFICE 365											
MIDDLEWARE											
STORAGE											
SO Y VIRTUALIZACIÓN											
COMUNICACIONES UNIFICADAS											
OPERACIÓN DE AS 400											
SERVICIO DE MONITOREO											
SERVICIOS DE NUBE											
DESPLIEGUES											
BASES DE DATOS											

Se realiza un estudio de mercado de los proveedores a nivel Colombia como lo es INTERGRUPO, ARUS e INTERNEXA, que tienen como misión a través de la innovación y la tecnología, gestionar servicios de tecnologías de información. Por medio de su portafolio virtual se pueden identificar la prestación de servicios enfocados en la administración de servicios IT, así mismo, se logró identificar los posibles clientes (cantidad) que puede consumir un servicio (fijando el valor de 1 de acuerdo a los clientes), al final, se hace una sumatoria de la cantidad de clientes por servicio y se tomaran los 4 servicios más demandados o adquiridos como alcance para el análisis de riesgos.

Los servicios de IT son todas las actividades necesarias que se realizan para operar el funcionamiento digital de las organizaciones a través de modelos que permiten manipular infraestructuras digitales; los 3 proveedores dentro de su portafolio virtual cuentan con la operación de mesas de soporte que incluye la gestión y administración de plataformas como office 365, servicios de virtualización, almacenamiento, monitoreo de los componentes de IT, bases de datos y despliegues a fin de garantizar un adecuado mantenimiento y evolución de los servicios de IT.

Cada uno de los servicios que se prestan en una empresa del sector informático fue mapeado con los clientes (cliente A, Cliente B, etc) que consumen sus productos y para ello se inició un proceso de investigación donde se identificó de acuerdo a los servicios ofrecidos la cantidad de bienes consumidos, para cada cliente que consume un producto se identificó con el número 1, posteriormente se realizó un conteo de la cantidad de servicios por cada cliente y los productos que contaran con consumos por encima de 7 puntos fueron identificados como los servicios más recurrentes.

Definido el contexto y el alcance, se determinó cuáles son los activos de información o componentes necesarios para prestar el servicio en dicho contexto y para ello se modelaron los productos y sus respectivos componentes, así se determinan además de los componentes cuales son de su mismo tipo y tendrían un mismo tratamiento con la finalidad de modelar los activos referentes al contexto.

Tabla 2 2 Componentes de los servicios

Servicio A	Servicio B	Servicio C	Servicio D
Activo de información 1 asociados al servicio			
Activo de información 2 asociados al servicio			
Activo de información 3 asociados al servicio			

La norma indica que al encontrar los activos es necesario iniciar un plan de análisis que determine como se clasifican los activos según su contenido, con toda finalidad de conocer cuál es el impacto sobre la organización en caso de que un activo sea vulnerado y así tomar acciones determinantes sobre los activos críticos. Para ello se establece la tabla de valoración de activos de la referencia en mención (tabla 2-3).

Tabla 2 3 Clasificación de los activos vs los impactos empresariales [18]

Activo	Afectación sobre los planes de negocio (finanzas).	Afectación en un proceso Interno	Afecta legalmente a la empresa	Afecta las ventas o una ventaja competitiva.	Tiene afectación la IMAGEN o reputación	Nivel de criticidad	
						0	Sin clasificar

Tener un nivel de clasificación es fundamental para conocer los posibles impactos, de acuerdo al nivel de criticidad, que un activo puede llegar a tener, así mismo, la clasificación da otro punto de vista en la medida que, por ese nivel de criticidad, la valoración de controles actuales o futuros, se hace más relevantes.

El proceso de obtener una clasificación de los activos se hace de forma semi-automática, valorando la importancia (de pérdida, alteración o modificación) que pueda tener cada activo en diferentes factores, esto daría como resultado un nivel de clasificación de 3 niveles: Confidencial, privada o pública.

Conociendo la criticidad de cada activo y los impactos sobre el negocio, se deben establecer las vulnerabilidades asociadas, así como los controles actuales con la finalidad de realizar una evaluación básica sobre la efectividad de los controles existentes y tomar acciones de mejora de acuerdo con los resultados de la gestión de riesgos (tabla 2-4).

Tabla 2 4 Clasificación de los activos vs los impactos empresariales [18]

Activos	Vulnerabilidades	Controles actuales implementados en el activo.	Clasificación del activo	Efectividad de los controles = Eficiencia + Eficacia	0% = No se cuenta con controles 25% = Algunos controles están implementados, pero no funcionan adecuadamente o son limitados (no cubren todo el riesgo) 50% = todos los controles propuestos están implementados, pero no se valida su efectividad. 75%= Todos los controles están implementados, se verifican su efectividad, pero no se monitorea ni se hacen planes de mejora continua. 100%= La totalidad de controles están implementados, se miden, monitorean y se generan planes de acción para su mantenimiento (líneas bases periódicas y auditorias).

Posterior al conocimiento obtenido sobre la situación actual es necesario listar las amenazas que eventualmente podrían ocasionar daños el activo, con la explotación de las vulnerabilidades existentes (tabla 2-5), para luego llegar el cruce de escenarios de riesgos.

Tabla 2 5 Amenazas Vs Activos [18]

ACTIVOS AMENAZAS			

Con este entendimiento se rastrean los posibles escenarios de riesgos, con el objetivo de evaluar su impacto [17], los criterios de impacto deben desarrollarse y especificarse en términos del grado de daño o costos a la organización causado por un evento de seguridad de información. Un concepto de impacto en el negocio se utiliza para medir consecuencias.

Con el objeto de identificar los escenarios de riesgos se realizó un análisis sobre cómo estos impactarían a la organización; su medición se debe fijar de acuerdo con el tipo de compañía y sus valores corporativos, teniendo en cuenta cuáles son esos factores que afectan más sus procesos misionales en caso de ser impactados. Con la convergencia tecnológica los pilares de la seguridad de la información hacen parte de los valores corporativos de muchas organizaciones, y esto podría suponer un punto de partida para conocer los impactos.

El presente trabajo desarrolla la técnica de evaluación de impacto teniendo en cuenta la probabilidad de ocurrencia (tabla 2-6) vs. el impacto en la información desde la mirada de la confidencialidad (tabla 2-7), se realiza desde esta perspectiva debido a que las organizaciones que presentan servicios informáticos tiene como core del negocio manejar los sistemas de un tercero, creando acuerdos de confidencialidad (dada la información local o en tránsito que se pueda tener) y estos acuerdos son determinantes para generar relaciones comerciales entre ambos, crear crecimiento y evolución tanto en procesos misionales como estratégicos.

Para calcular el nivel de impacto, se define la matriz de criticidad de 5x5 la cual significa que, para ubicar el nivel de riesgo se cuenta con 5 niveles en probabilidad y 5 niveles en impacto (tabla 2-9).

Tabla 2 6 Probabilidad o Frecuencia [19]

Nivel	Rangos	Ejemplo detallado de la descripción
1	**Raro**	Puede ocurrir solo bajo circunstancias excepcionales
2	**Improbable**	Podría ocurrir algunas veces
3	**Posible**	Puede ocurrir en algún momento
4	**Probable**	Probabilidad de ocurrencia en la mayoría de las circunstancias
5	**Casi seguro**	La expectativa de ocurrencia se da en la mayoría de circunstancias

Tabla 2 7 Impacto en la información pilar confidencialidad [19]

Nivel	Rangos	Confidencialidad que un individuo, entidad o proceso no autorizado acceda al activo de información
1	**Insignificante**	Genera pérdida de confidencialidad o fuga de activos de información que no es de utilidad para la competencia o individuos o grupos internos o externos
2	**Menor**	Genera pérdida de confidencialidad o fuga del activo de información que puede ser de utilidad para la competencia o individuos o grupos internos o externos con efectos mitigables o recuperables en el corto plazo
3	**Intermedio**	Genera pérdida de confidencialidad o fuga del activo de información que puede ser de utilidad para la competencia o individuos o grupos internos o externos con efectos mitigables o recuperables en el mediano plazo
4	**Mayor**	Genera pérdida de confidencialidad o fuga del activo de información que puede ser de utilidad para la competencia o individuos o grupos internos o externos con efectos mitigables o recuperables en el largo plazo
5	**Superior**	Genera pérdida de confidencialidad o fuga del activo de información que puede ser de utilidad para la competencia o individuos o grupos internos o externos, con efectos no recuperables para la Empresa o el grupo

Con el conocimiento que se alcanza identificando las variables anteriores, se inicia un proceso de evaluación que entregará un reporte donde se podrá evidenciar la situación actual y cuales podrían ser las consecuencias en una organización (considerando los controles actuales) así mismo, cuál es el nivel de impacto en términos del conocimiento al ser vulnerado el activo. Para la evaluación se define los parámetros de la siguiente tabla 2-8:

Tabla 2 8 Impacto en la información pilar confidencialidad [19]

Escenario de riesgos	PROBABILIDAD		IMPACTO INFORMACIÓN CONFIDENCIALIDAD		Riesgo P*Impacto Cliente Mercado	Clasificación del activo

Los resultados de cada escenario evaluado se exponen en la matriz 5*5 de criticidad que refleja una mirada holística del riesgo en la organización (tabla 2-7).

Tabla 2 9 Matriz de Riesgos [18]

Probabilidad		Consecuencia				
	valor	Insignificante	Menor	Intermedio	Mayor	Superior
Casi seguro	5					
Probable	4					
Posible	3					
Improbable	2					
Raro	1					

Las zonas del mapa de riesgos son:

- Verde: Zona aceptable
- Amarilla: Zona Tolerable
- Naranja: Zona inadmisible
- Roja: Zona inaceptable

Los riesgos de mayor probabilidad y alto impacto requieren más atención (Zona naranja y roja), y, por lo tanto, serán los riesgos que tendrán un plan de tratamiento. Los riesgos en las zonas bajas (verde y amarillo) son los que se aceptan.

2.1.2 Lo siguiente realizado, fue proponer un plan de tratamiento para los riesgos identificados, considerando aquellos riesgos altos y estableciendo mecanismos de reducción, tomando como referencia los controles de la norma ISO 27001:2013 y/o la NIST 800-53.

[17] Los criterios de aceptación del riesgo deben ser desarrollados y especificados a menudo dependen de las políticas de la organización, las metas, los objetivos y los intereses de las partes interesadas.

El objetivo principal se basa en un sistema integral de ciberseguridad, es por esto por lo que ningún riesgo debe ser transferido para cumplir el objetivo del presente trabajo, El plan de tratamiento se enmarcó en ciclo PHVA, para ello se considera el siguiente plan de tratamiento donde se contemplan además de los controles, los resultados (tabla 2-10).

Tabla 2 10 Plan tratamiento de riesgos [18]

RIESGOS ALTOS Considerando los controles actuales	TRATAMIENTO			Descripción del plan: * Controlar o evitar: ¿cómo? * Transferir: ¿A quién? * Aceptar: ¿Por qué?	Plan de monitoreo		
	Aceptarlo	Evitarlo	Controlarlo			Responsable (basados en el caso de estudio y la cantidad de empleados de la compañía Tecnología para todos S.A.S)	Resultado Esperado

2.2 Fase 2: Caracterizar diferentes normas para el manejo y respuesta de los incidentes de seguridad, acorde a los riesgos detectados y la aplicabilidad en empresas de servicios informáticos.

Para lograr esta fase que corresponde al objetivo2, se definieron las siguientes actividades (2.2.1 y 2.2.2) como la hoja de ruta necesaria, para cumplir con el desarrollo del objetivo.

2.2.1 Caracterizar las normas para la creación de la estrategia para el manejo de incidentes, considerando la norma NIST SP800-61 (Computer Security Incident Handling Guide), ISO 27035, el proyecto amparado de LACNIC (CSIRT) y/o los manuales del MiNISTerio TIC.

Identificar los puntos clave de cada norma nos permite entender la fortaleza de cada una, para ello este proyecto se construyó la tabla 2-11 donde se realizó un pareto de las normas seleccionadas a través del numeral 2.2.1, contra unos conceptos base que permitirán el

entendimiento de cada norma, con ello, logar encontrar las principales características (ventajas, procesos y enfoque).

En la tabla 2-11 las ventajas harán referencia a las características que sobre salen en cada una de las normas, son esas actividades o procesos que prevalecen en la documentación. Para el contexto actual las ventajas estarán conectadas con los procesos de cada norma y los procesos hacen referencia a la descripción de los pasos y/o procesos que se describen en la documentación para implementar dicho marco, el ultimo concepto genérico se relaciona con el foco de la norma, donde se podrían dar conceptos como normas genéricas que le apuntan a la seguridad de la información o normas un poco más centradas en el concepto de ciberseguridad.

Tabla 2 11 Normas y definición criterios

	Ventajas	Procesos	Enfocada en: seguridad de la información, ciberseguridad
NIST			
ISO27035			
Proyecto amparo lacnic			
Guia para la gestión de incidentes, Mintic			
Marco NIST Ciberseguridad			

Una vez definidas las normas y sus principales características se proceden a validar la siguiente actividad, enmarcada en la estrategia para la selección de la norma.

2.2.2 Establecer la estrategia para el manejo de incidentes a partir de la norma seleccionada y los riesgos altos detectados.

Esta metodología buscó establecer la estrategia para el manejo de incidentes a partir del objetivo general, el cual está enmarcado en la construcción de un modelo de ciberseguridad para empresas que ofrecen servicios informáticos con base en referentes nacionales e internacionales.

Para la selección, definición o agrupación de metodologías se tuvieron en cuenta los siguientes criterios, esto, en consideración que se trata de una propuesta hacia empresas que ofrecen servicios informáticos y es necesario conceptualizar o buscar en las normas elementos fundamentales como son:

1. **Procesos definidos**

Para éste primer criterio es fundamental que la norma establezca o dé una guía de cómo desarrollar o potencializar el manejo de incidentes de seguridad a través de los procesos. Dentro de este criterio se valoraron los siguientes elementos:

- ✓ Recomendación de herramientas y técnicas: para precisar una estrategia es necesario conocer las recomendaciones que tiene el mercado acerca del software o hardware para el soporte del proceso en cada una de las fases por las cuales se debe tratar un incidente de seguridad. Es importante que la norma a evaluar genere dichas recomendaciones, el no usar herramientas adecuadas para la atención de eventos de seguridad puede generar lentitud en los procesos; si se cuenta con herramientas es más probable que cualquier respuesta sea tratada más eficaz.
- ✓ Recomendación de cómo documentar y hacer el informe final: La definición de la documentación es clave dentro de la generación de un proceso, estructurar el Informe final y generar las plantillas a seguir a partir de una norma permite formar técnicas de madurez dentro del ciclo de vida de la seguridad informática. [21] la documentación permite seguir procesos en momentos de crisis y restablecer los servicios de manera adecuada y segura
- ✓ Recomendaciones sobre cómo debe ser un equipo de respuesta a incidentes de seguridad: son fundamentales para una adecuada atención, la norma o metodología debe recomendar al menos que roles, funcionalidades, organigrama, actividades y tipo de personal debe conformar el equipo. Esto es determinante para la creación de un método que permita tener un adecuado manejo de incidentes de seguridad. Que cada persona conozca su rol dentro del equipo es concluyente al momento de actuar en una crisis y estos pueden ser capaz de operar eficazmente por sí mismos y en estrecha colaboración con sus integrantes.

2. **Ciclos evolutivos**

El segundo criterio tiene como objeto definir un proceso que sea sostenibles en el tiempo como los ciclos PHVA, donde no solo se definen estrategias para la inicio y desarrollo, si no en procesos cíclicos que permiten evaluaciones continuas y sostenibles en el tiempo. Es por ello por lo que para enmarcar la estrategia que se construyo fue necesario valorar:

- ✓ Normas que contemplen tácticas de desarrollo sostenible en el tiempo, que permitan autoevaluarse recurrentemente [24] la autoevaluación y la medición deberían mejorar la toma de decisiones sobre las prioridades de inversión. Por ejemplo, medir, o al menos caracterizar robustamente, los aspectos del estado de seguridad cibernética de una organización y las tendencias a lo largo del tiempo puede permitirle a esa organización comprender y transmitir información de riesgo significativa a dependientes, proveedores, compradores y otras partes.
- ✓ Procesos que determinen un nivel actual de seguridad y un punto objetivo, las organizaciones deben examinar constantemente en qué medida están logrando los resultados descritos en los objetivos empresariales, y en caso de no encontrarse alineados su estrategia deben permitir implementar planes de acción tempranos para evitar sobre costos en sus ejecuciones además deben buscar fortalecer las prácticas existentes de seguridad cibernética y reducir el respectivo riesgo informático. Con estas evaluaciones podría determinarse que sus inversiones no son eficaces pero debido a la rapidez en la cual se fijó esto, se puede priorizar y volver iniciar.
- ✓ En las lecturas el marco debe referenciar al menos un caso de éxito documentado, implementar un marco desde el desconocimiento produce reprocesos y retrasos en la implementación si no se tienen claros los métodos a seguir, en cambio conocer las estrategias que otras organizaciones utilizaron y sus lecciones aprendidas permite tener una base de conocimiento para priorizar las actividades y ganar tiempo en las implementaciones.

3. Una estrategia enfocada a la reducción de riesgos

El ultimo criterio busca definir una norma que le apunte a la reducción de los riesgos favoreciendo las inversiones de los presupuestos. Para ello se revisarán normas que le apunten a:

- ✓ El marco debe orientar las lecciones aprendidas a el proceso de gestión de riesgos. Si los mapas de riesgos se alimentan de las lecciones aprendidas, las inversiones siempre estarán alineadas con las necesidades del negocio, lo cual genera rentabilidad para las organizaciones y un retorno en la inversión sostenible y no basado en probabilidades.

- ✓ Fortalecer el enfoque en la prevención. Definir una estrategia con base a las actividades de reacción no es rentable en el tiempo, la necesidad misma de solventar las situaciones de manera rápida podría costar incluso a una organización mala reputación y daños irreparables, la norma seleccionada debe entregar tácticas que se enfoquen en actividades que permitan anticiparse e incluso evitar situaciones complejas.
- ✓ Contribuir a la justificación del presupuesto y los recursos. El manejo de riesgos debe considerarse de acuerdo a una estrategia global en las organizaciones, cada área debe apuntarles a los mismos objetivos empresariales, donde debe primar el cuidado por el bien común. La norma debe apuntarle a optimizar los recursos y las inversiones para que sus aportes sean considerados dentro de los presupuestos organizacionales.

Una vez definidos los criterios de aceptación para la selección de la norma es preciso determinar cuáles serán las calificaciones que se darán a los criterios. La siguiente tabla 2-12 describe un rango de 0 a 2 que califica el cumplimiento del criterio en la norma.

Tabla 2 12 Calificaciones posibles

Calificaciones posibles
0 - No posee la característica
1- Posee una característica parcial de acuerdo con la lectura
2- Da un cumplimiento de la característica valorada

Para realizar la calificación se define la tabla 2-11, la cual enfrenta las normas a cada criterio, y la calificación estará basada en el cumplimiento o no del criterio. Para ello se usará la tabla de calificaciones posibles y será totalizadas.

Tabla 2 13 Normas y calificación criterios

Criterios Norma	Procesos definidos	Ciclos evolutivos	estrategia enfocada a la reducción de riesgos	Calificación total
NIST				
ISO27035				
Proyecto amparo lacnic				
Guia para la gestión de incidentes, Mintic				
Marco NIST Ciberseguridad				

La norma seleccionada será la que sume una calificación mayor, en caso de presentarse una igualdad al momento de totalizar las calificaciones, será necesario analizar si esa igualdad hace referencia a complementariedad en las normas.

2.3 Fase 3: Evaluar el modelo de ciberseguridad para el manejo de incidentes a través de un caso de estudio

Para el cumplimiento de esta fase que corresponde al objetivo 3 se desarrollaron 2 actividades enunciadas en los puntos (2.3.1 y 2.3.2) como la hoja de ruta.

2.3.1 Actividad 1: Creación del modelo de ciberseguridad que integre el manejo de incidentes de seguridad, esto se realizará con base en las normas de riesgos, ISO 27001, NIST y las de gestión de incidentes. El modelo debe permitir la reducción y tratamiento de los incidentes identificados para las empresas tercerizadoras de servicios informáticos.

La creación del modelo se inicia a partir de los resultados obtenidos en el objetivo 1, donde se establecieron los riesgos para empresas del sector informático y se determinaron los planes de tratamiento para los riesgos identificados como los potencialmente causantes de mayor impacto dentro de las organizaciones del sector, para cumplir con el objetivo principal del proyecto se realiza un modelamiento que permita relacionar el objetivo 2 que tiene como propósito la selección de una norma adecuada para el manejo de incidentes

de seguridad informática, allí de acuerdo a los criterios de selección determinados en el objetivo se selección la norma ISO27035 y el framework de ciberseguridad NIST, la dualidad de ambas normas permite un correcto encadenamiento de los resultados obtenidos en el objetivo 1 y 2 para la construcción del modelo de ciberseguridad.

Se inicia entonces con el proceso de construcción partiendo del framework de ciberseguridad NIST donde se identifican los procesos macro dentro del modelo como el establecimiento de las estrategias de seguridad y la identificación de las políticas que se deben desarrollar de manera alineada a los riesgos detectados en el objetivo 1.

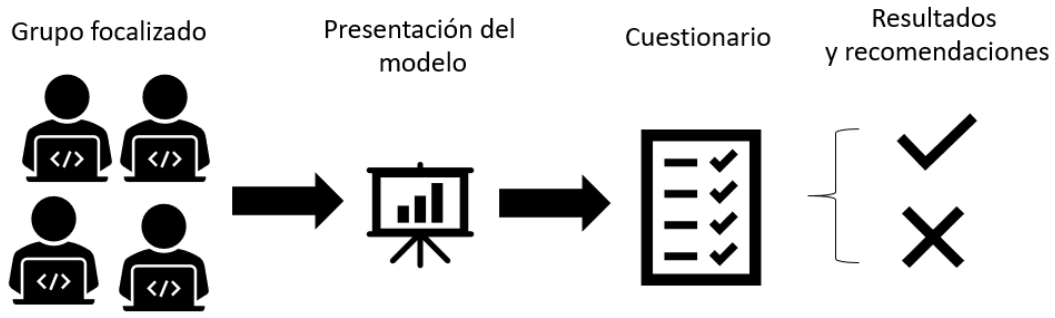
Dentro de los procesos macro se deben definir cada uno de los subprocesos que el framework de ciberseguridad NIST precisa para el adecuado manejo de incidentes de seguridad identificados dentro del marco como las funciones; cada función se mapea con los procesos identificados por la norma ISO27035 donde se emplean los pasos, procesos, procedimientos, lineamientos y ejemplos para el manejo de un incidente de seguridad.

Con los resultados de los objetivos 1 y 2, es viable el inicio de la creación del modelo de ciberseguridad enfocado en la búsqueda de alternativas que permitan la construcción de una estrategia orientada a un adecuado manejo de incidentes de seguridad para empresas del sector.

2.3.2 Actividad 2: Determinar y ejecutar una estrategia que permita la evaluación del objetivo, considerando un caso de estudio en una empresa que ofrece servicios tercerizados de TI, esto se hará a través de entrevistas, encuestas y/o check-list de validación de cumplimiento con el personal de la empresa seleccionada.

Para establecer la estrategia que permitiera la evaluación del modelo de ciberseguridad se definieron de manera metódica 4 pasos como se describe en la ilustración 3, estrategia para la evaluación del modelo de ciberseguridad.

Ilustración 3 Estrategia para la evaluación del modelo de ciberseguridad. Fuente construcción propia



La evaluación del modelo se realizó a través de la descripción de un caso de estudio, el cual fue evaluado por un grupo focalizado de expertos en los servicios de seguridad para empresas del sector, el grupo focalizado se conformó con personas que laboran en una organización que ofrece servicios informáticos, además el rol de cada uno de los participantes debería estar relacionado con servicios de seguridad informática en una empresa del sector; con el objeto de contar con personal competente para la evaluación del modelo se incluyeron personas que contaran con amplia experiencia y competencia relacionada con el manejo de incidentes de seguridad.

Conformado el grupo expertos se procede a realizar una presentación que incluyera de manera sistemática el modelo de ciberseguridad para empresas del sector informático que fortalezca un adecuado manejo de incidentes de seguridad, incluyendo la problemática que aborda el modelo, los riesgos inadmisibles e inaceptables detectado en el caso de estudio y una descripción del estudio que conllevo a la creación del modelo

Caso de estudio

El caso de estudio se orientó en una organización que presta servicios informáticos (no se indica el nombre de la organización por temas de confidencialidad); los servicios informáticos son aquellos procesos de apoyo para el desarrollo de los procesos core de cualquier organización; en la actualidad con la acelerada transformación tecnológica que se presenta en el entorno digital todas las organizaciones se han migrado a sistemas digitales para aprovechar el beneficio de la digitalización, para que una organización pueda incluirse dentro de estos ecosistemas independiente de su conocimiento, requiere el uso de servicios especializados como el del manejo de sistemas como la mensajería electrónica (Outlook, teams), el desarrollo de programas, incluyendo las capas de traducción que permiten la comunicación y la administración de datos en aplicaciones distribuidas (sistemas middleware), además, requieren personal especializado que preste

soporte a sus usuarios finales para hacer uso y sacar provecho de sus sistemas digitales, servicios referentes a la administración y soporte de sistemas como las bases de datos, servicios de despliegues que permiten la distribución masiva de actualizaciones, el manejo y uso de comunicaciones unificadas enfocadas en los servicios de vídeo conferencias y todo lo relacionado al ciclo de vida de productos como el almacenamiento (storage), virtualización, y sistemas en Cloud.

Al prestar estos servicios las organizaciones están en el deber de manejar adecuadamente la información que procesan para cada uno de sus clientes, además se deben establecer mecanismos que permitan la verificación de los procesos que se establecen bajo las políticas, con el objeto de garantizar un adecuado manejo de los activos buscando con ello que se cubren la mayoría de los riesgos que se puedan presentar, a esta situación se le debe sumar una cobertura en el sistema que se enfoque en estar preparados adecuadamente para el manejo de cualquier incidente que se pueda presentar. De acuerdo a la empresa especializada en auditoria y seguridad, Deloitte [20], indica que 1 de cada 3 empresas se consideran que están poco o nada preparadas para hacer frente a un incidente de seguridad. Y estar preparados para el manejo de un incidente de seguridad no solo es establecer los procesos y formatos, además se debe garantizar una adecuada segregación de roles, cumplimiento de las políticas de acuerdo a las metodologías establecidas y un correcto entendimiento de todos los actores del proceso.

La estrategia para evaluar el modelo incluyó, además, un cuestionario con dos componentes, en la primera sección se incluyeron cinco preguntas que permitieran describir el perfil de referenciación de las personas que conformaron el grupo focalizado, para ello se definieron las siguientes preguntas.

1. ¿En qué sector trabaja actualmente?
2. ¿Labora usted en una empresa que ofrece servicios informáticos?
3. ¿Su cargo actual está relacionado con servicios de seguridad informática?
4. ¿Cuántos años de experiencia tiene usted trabajando en servicios de seguridad informática?
5. ¿Dentro de su experiencia ha tenido relación con la solución de un incidente de seguridad? ¿Dentro de su experiencia ha desarrollado algún rol para manejar un incidente de seguridad relacionado con Ransomware?

El objetivo de la segunda sección se construyó orientado en la evaluación del modelo de ciberseguridad, para ello se plantearon 9 preguntas.

1. De acuerdo al modelo de ciberseguridad si éste fuese implementado, ¿considera que al materializarse los escenarios de riesgos inadmisibles es posible reducir los niveles de exposición?

2. ¿De acuerdo al modelo de ciberseguridad planteado considera que se implementaron estrategias que permiten anticiparnos a la materialización de un evento de seguridad?
3. ¿De acuerdo al modelo de ciberseguridad planteado considera que con las funciones proteger y detectar es posible reducir los niveles de exposición de los riesgos?
4. ¿De acuerdo al modelo de ciberseguridad planteado considera que se implementaron estrategias adecuadas en la función Recuperar para reducir los tiempos de indisponibilidad de los activos en los que se materializan los escenarios de riesgos?
5. ¿De acuerdo al modelo de ciberseguridad planteado considera que las políticas definidas en el modelo crean valor enfocado en reducir los niveles de exposición de los escenarios de riesgos identificados?
6. ¿De acuerdo al modelo de ciberseguridad planteado y teniendo en cuenta los riesgos identificados como altos es posible con las acciones descritas en la función proteger reducir los niveles de exposición de los riesgos?
7. ¿De acuerdo al modelo de ciberseguridad planteado considera que se definió una estrategia adecuada en la función acciones de mejora enfocada en el aprendizaje y por ende implementación de actividades que permitan no repetir los escenarios que se pueden materializar?
8. ¿De acuerdo al modelo de ciberseguridad plenteado específicamente para el escenario de riesgo Posibilidad que la amenaza: crakeo de contraseñas, afecte el activo como correo/medios de almacenamiento, teléfonos móviles es posible reducir el nivel de exposición?
9. ¿Considera usted que el modelo de ciberseguridad planteado se puede mejorar en algún aspecto?

Finalmente, se realizó un análisis con los resultados de la encuesta que permitiera determinar si la aplicación del modelo de ciberseguridad si permite fortalecer un adecuado manejo de incidentes de seguridad basado en referentes nacionales e internacionales.

3. Resultados

3.1 Fase 1: Establecer los diferentes riesgos de ciberseguridad en empresas que ofrecen servicios informáticos.

3.1.1 Obtener los diferentes riesgos de ciberseguridad en empresas que ofrecen servicios informáticos, con base en el uso de la norma ISO 27005:2018 y su proceso de gestión

Como se indicó en la metodología, se evaluaron los servicios que presta una organización del sector vs. los servicios consumidos por sus clientes, cuyos resultados se establecen en la tabla 3-1.

Tabla 3 1 Caracterización de los productos de una empresa de servicios informático

PLATAFORMASADMINISTRADAS	Cliente A	Cliente B	Cliente C	Cliente D	Cliente E	Cliente F	Cliente G	Cliente H	Cliente I	Cliente J	Total, servicios por cliente
MESA DE SOPORTE	1					1	1				3
OFFICE 365	1	1	1	1	1				1	1	7
MIDDLEWARE									1		1
STORAGE	1		1						1	1	4
SO Y VIRTUALIZACIÓN	1	1	1	1	1				1	1	7
COMUNICACIONES UNIFICADAS	1	1	1	1	1				1	1	7
OPERACIÓN DE AS 400									1	1	2
SERVICIO DE MONITOREO	1	1	1	1	1	1	1	1	1	1	10
SERVICIOS DE NUBE	1	1	1	1	1				1		6
DESPLIEGUES		1	1			1	1		1	1	6
BASES DE DATOS				1				1			2

De acuerdo con la recurrencia de los servicios y de acuerdo con los totales obtenidos, se define el contexto sobre la **infraestructura basada en la prestación de servicios office 365, Virtualización, Comunicaciones unificadas (Skype for bussines), Monitoreo (monitoreo de servidores y componentes asociados a estos).**

A partir de esta información, se caracterizaron los componentes necesarios para prestar el servicio en dicho contexto, y para ello se modelaron los productos y sus respectivos activos de información (tabla 3-2), así se determinan además de los componentes cuales son del mismo tipo y suponen un mismo tratamiento.

Tabla 3 2 Componentes de los servicios

Office 365	Virtualización	Comunicaciones unificadas	Servicio de monitoreo
tenat	Server 2008 Estándar	SBA	Server 2016 Estándar
Licencias E1	Server 2008 R2	Gateway de voz	PRTG
Licencias E3	Server 2016 Estándar	teléfono polycom	Publicador apache
Licencias E5	Server 2012	Service Skype for bussines	Certificados digitales
Desktop Windows 10	Server 20016 R2	Teams	VPN
Usuarios	SAN	Troncales SIP	Server 2016 Estándar
One Drive	NAS	Certificados Digitales	Service desk
Share Point	Agentes de antivirus		teléfono Móviles Android
Power BI	Agentes de PRTG		
Outlook	Agentes de lansweeper		
	NTP		
	DHCP		
	VPN		
	RDP		
	SSH		

De acuerdo a la metodología, se establece el contexto para el cual se realizó la evaluación de riesgos y los activos pertenecientes al contexto (tabla 3-3), esto es, para los diferentes servicios ofrecidos se reagruparon los diferentes activos, dejando una lista representativa de ellos, así, para una empresa que ofrece servicio informáticos a clientes, el alcance de los riesgos se suscribe a la "*Infraestructura basada en la prestación de servicios office 365, Virtualización, Comunicaciones unificadas y Monitoreo*"

Tabla 3 3 Contexto y Activos

Infraestructura basada en la prestación de servicios office 365, Virtualización, Comunicaciones unificadas y Monitoreo
Correo (Outlook)
Licencias
Windows 10
Windows Server 2008 (estándar, R2)
Server 20016 (Estándar y R2)
Windows Server 2012
Almacenamiento local/remota (OneDrive, SharePoint, SAN, NAS)
VoIP/ToIP
Usuarios/Clientes
Personal de soporte/administradores
Servicio Web (apache)

VPN
Criptografía: Certificados, SSH
Monitoreo PRTG
Servicio DHCP
Servicio NTP
teléfono Móviles Android
Documentos y manuales

Para conocer el nivel de clasificación de la información se utilizan las escalas de clasificación determinadas para una organización del sector (como ya se indicó en la metodología: confidencial, privada o pública), las cuales se describen a continuación.

Nivel de clasificación Privada: Es toda la información financiera, técnica e información utilizada por empleados, terceros o practicantes de la organización que no puede ser conocida por terceros, sin autorización especial del responsable de la dependencia o proyecto que genera y utiliza dicha información. En caso de ser conocida, utilizada o modificada por personas sin la debida autorización, impactaría de forma importante a terceros o a los sistemas y/o procesos de la Compañía.

Nivel de clasificación Confidencial: Es toda la información financiera, técnica e información utilizada por empleados, terceros o practicantes de la organización, que no puede ser conocida por terceros sin autorización especial del presidente de la empresa, Gerente General o Director de Área, que genera y utiliza dicha información. En caso de ser divulgada, utilizada o modificada por personas sin la debida autorización, impactaría de forma grave a los convenios o a los sistemas y/o procesos de la compañía.

Nivel de clasificación Pública: Esta es información general de la organización como técnica y es utilizada por los empleados, terceros o practicantes de la compañía, la cual no puede ser conocida por externos sin la autorización del responsable de la información. En caso de ser divulgada, utilizada o modificada por personas, sin la debida autorización no impactaría de manera significativa los clientes, sistemas o procesos de la empresa.

Seguidamente, el proceso de valorar el nivel de clasificación de los activos es el siguiente (tabla 3-4):

1. Se definieron 5 posibles factores de impacto que puede tener un activo si este se modifica, elimina o daña:

2. Cada factor de afectación debe ser valorado en una escala de 1 a 5, en dónde 1 es el menor valor de afectación y 5 es el mayor valor en afectación.
3. Si un activo tiene todos os mayores valores, el puntaje total será 25.
4. Dependiendo de los puntajes totales, se da una valoración a los niveles de clasificación de la siguiente manera:
    a. Público: Si el valor total de los factores afectados está por debajo de 8, o que significa que no representa gran riesgo.
    b. Privada: Si el valor total de los factores esta entre 8 y 15, lo que indica un valor medio.
    c. Confidencial: Si el valor total de los factores está por encima de 15.
5. El sistema calcula el valor total y la clasificación dado a cada activo de información, con lo cual, se prosigue con el siguiente paso en la metodología de riesgos.

Como resultado de la valoración de los activos, se puede ver en la tabla 3-4.

Tabla 3 4 Clasificación de los activos vs los impactos empresariales. Fuente: tomada y ajustada de [18]

Activo	Afectación sobre los planes de negocio (finanzas).	Afectación en un proceso Interno	Afecta legalmente a la empresa	Afecta las ventas o una ventaja competitiva.	Tiene afectación la IMAGEN o reputación	Nivel de criticidad	
Correo (Outlook)	2	3	2	3	3	13	Privada
Licencias	1	3	2	1	2	9	Privada
Windows 10	3	3	3	2	2	13	Privada
Windows Server 2008 (estándar, R2)	3	3	3	2	2	13	Privada
Server 20016 (Estándar y R2)	3	3	3	2	2	13	Privada
Windows Server 2012	3	3	3	2	2	13	Privada
Almacenamiento local/remota (OneDrive, SharePoint, SAN, NAS)	3	3	3	3	3	15	confidencial
VoIP/ToIP	2	3	2	3	2	12	Privada
Usuarios/Clientes	3	2	1	2	2	10	Privada
Personal de soporte/administradores	2	3	1	3	2	11	Privada
Servicio Web (apache)	1	3	2	1	1	8	Publica
VPN	1	2	1	2	3	9	Privada
Criptografía: Certificados, SSH	1	3	1	3	3	11	Privada
Monitoreo PRTG	3	3	3	2	1	12	Privada
Servicio DHCP	1	3	1	3	2	10	Privada
Servicio NTP	1	3	1	1	2	8	Publica
teléfono Móviles Android	2	2	2	3	3	12	Privada
Documentos y manuales	3	3	3	3	3	15	confidencial

La clasificación de los activos se ejecuta de acuerdo a la definición de tres conceptos, la información podría determinarse como pública, privada o confidencial. Las compañías se deberían considerar en dicho margen para realizar acciones desde estas perspectivas; para el caso de estudio los prestadores de servicios Informáticos siempre deberán considerarlos para el manejo del servicio dentro de 2 de ellos, y la información que es propia de su negocio podría clasificarse dentro de los 3 conceptos según su nivel de criticidad, sin embargo al realizar el análisis de los servicios se detecta que los activos si bien son un bien público de todos los integrantes de las organizaciones cada uno debe ser resguardado de tal forma que los externos no tengan acceso a la información que se encuentra en ellos, es por esto que la clasificación evidencia que el 89% de los activos terminan siendo un bien privado, pues cada uno de ellos cuenta con información propia de las organizaciones a las cuales se les prestan los servicios mencionados en el alcance, nada contenido en los activos debería estar expuesto a manipulaciones o lecturas por partes externas, todo esto se realiza con el fin de generar ecuanimidad a los convenios, la información que contienen estos puede ser usada para explotar vulnerabilidades causando daños o perdidas con consecuencias graves para ambas organizaciones.

La presencia de una vulnerabilidad no causa daño en sí mismo, ya que es necesario que haya una amenaza actual para explotarla. Una vulnerabilidad que no tiene peligro puede no requerir la implementación de un control, sino que debe ser reconocido y supervisado para los cambios [17].

Para supervisar estos cambios es necesario definir cuáles son las vulnerabilidades actuales de cada activo y conocer la eficacia y eficiencia de los controles iniciales, para ello se definen los siguientes porcentajes, enmarcados de acuerdo a los controles actuales vs las vulnerabilidades existentes [18]:

- ✓ 0% = No se cuenta con controles
- ✓ 25% = Algunos controles están implementados, pero no funcionan adecuadamente o son limitados (no cubren todo el riesgo)
- ✓ 50% = todos los controles propuestos están implementados, pero no se valida su efectividad.

- ✓ 75%= Todos los controles están implementados, se verifican su efectividad, pero no se monitorea ni se hacen planes de mejora continua.

  100%= La totalidad de controles están implementados, se miden, monitorean y se generan planes de acción para su mantenimiento (líneas bases periódicas y auditorias).

Tabla 3 5 Clasificación de los activos vs los impactos empresariales [18]

Activos	Vulnerabilidades	Controles actuales implementados en el activo.	Clasificación del activo	Efectividad de los controles = Eficiencia + Eficacia
Correo (Outlook)	Fuga de información	ATP firewall CASB Control de acceso	privada	50%
Licencias	Desactualización de versiones	Revisión mensual	privada	25%
Windows 10	Desactualización de versiones	Parchado trimestral Antivirus	privada	80%
Windows Server 2008 (estándar, R2)	Desactualización de versiones	Parchado a ultima liberación Antivirus	privada	25%
Server 20016 (Estándar y R2)	Desactualización de versiones	Parchado trimestral Antivirus	privada	80%
Windows Server 2012	Desactualización de versiones	Parchado trimestral	privada	80%

Para más detalle del proceso, se puede ver en el anexo A (mapa de riesgos) la tabla completa.

En la medición de los controles actuales promedia un 43% lo que indica la escala es que algunos están implementados, pero no funcionan adecuadamente o son limitados (no cubren todo el riesgo), y es allí donde cobra relevancia la actualización de nuevas medidas de manera recurrente, y genera importancia en la creación de modelos de ciberseguridad adecuados a los activos que cada organización contiene.

Es determinante conocer con la nueva tecnología como los activos se pueden involucrar con el paso del tiempo en amenazas que no se había contemplado, en la siguiente tabla se realiza un listado de amenazas vs activos para iniciar un proceso de reconocimiento y crear una actualización de escenarios. El cruce de estos asocia la posibilidad de que una amenaza pueda actuar en un activo o grupo de activos determinado.

Tabla 3 6 Amenazas Vs Activos [18]

ACTIVOS **AMENAZAS**	Correo (Outlook)	Licencias	Windows 10	Windows Server 2008 (estándar, R2)	Server 20016 (Estándar y R2)	Windows Server 2012	Almacenamiento local/remota (OneDrive, SharePoint, SAN, NAS)	VoIP/ToIP	Usuarios/Clientes	Personal de soporte/	Servicio Web (apache)	VPN	Criptografía: Certificados, SSH	Monitoreo PRTG	Servicio DHCP	Servicio NTP	teléfono Móviles Android	Documentos y manuales
Man in the middle	x						x	x						x		x	x	
DoS/DDoS	x		x	x	x	x	x	x			x	x		x	x	x		
XSS											x							
SQL INJECTION											x							
MALWARE	x		x	x	x	x	x										x	
ARP SPOOFING								x							x	x		
NTP reflexion			x	x	x	x	x	x						x		x		
Phishing	x							x			x						x	
Fallas eléctricas	x		x	x	x	x	x	x				x		x				
Defacement								x			x			x				
Ingeniería Social									x	x								
Ransomware			x	x	x	x	x										x	
CSRF											x							
Ataque de fijación de sesiones								x			x		x					
crakeo de contraseñas	x		x	x	x	x	x	x			x	x	x	x			x	
Desastres naturales									x	x				x				x
Robo		x					x		x	x							x	x
Daño o error humano	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
Violación de derechos de autor o propiedad intelectual		x							x	x								x
Brecha en la legislación		x	x	x	x	x			x	x								x
Ataques DHCP							x	x							x			
Acceso físico no autorizado							x		x	x							x	x
Instalación no autorizada de software			x	x	x	x	x											
Mal funcionamiento del equipo			x	x	x	x	x	x				x					x	
Fuga de información									x	x				x			x	x

Acceso a la red o al sistema de información por personas no autorizadas.							x	x										x
Incumplimiento de relaciones contractuales									x	x								x

Al determinar los posibles escenarios se inicia la fase de valoración de acuerdo a las tablas de impacto definidas en la metodología, aquí se puede evidenciar la situación actual como puede ser impactada en términos de los controles actuales y cuál es el nivel de impacto en términos del conocimiento al ser vulnerado el activo (Ver anexo A mapa de Riesgos).

Al realizar el cruce de escenarios se obtuvieron 144 riesgos, los cuales posterior a su identificación se llevan a las tablas que permiten además de calificados determinar su probabilidad e impacto.

El proceso de calificación de los escenarios de riesgos, establece seleccionar que tan probable es que ocurra con el objetivo de determinar cuál es el impacto que genera. La calificación toma las tablas ya definidas de probabilidad e impacto y se ha considerado los controles actuales y la clasificación de la información.

Tabla 3 7 Impacto en la información pilar confidencialidad [18]

No.	Escenario de riesgos	PROBABILIDAD		IMPACTO INFORMACIÓN CONFIDENCIALIDAD		Riesgo P*Impacto Cliente Mercado	Clasificación del activo
(1)	Posibilidad que la amenaza: Man in the middle, afecte el activo: Correo (Outlook)	Posible	3	Mayor	4	12	Privada
(2)	Posibilidad que la amenaza: Man in the middle, afecte el activo: Almacenamiento local/remota (OneDrive, SharePoint, SAN, NAS)	Improbable	2	Superior	5	10	confidencial
(3)	Posibilidad que la amenaza: Man in the middle, afecte el activo: VoIP/ToIP	Posible	3	Mayor	4	12	Privada
(4)	Posibilidad que la amenaza: Man in the middle, afecte el activo: Monitoreo PRTG	Improbable	2	Intermedio	3	6	Privada

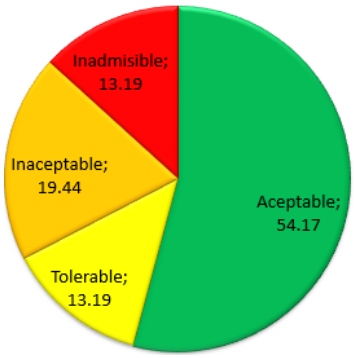
Los resultados de cada escenario se tabulan en la matriz 5*5 de criticidad que refleja una mirada holística del riesgo en la organización. **Ver anexo A mapa de Riesgos.**

Como resultado final, se obtiene una distribución porcentual (tabla 3-8, ilustración 3-1), la cual indica que los riesgos que deben ser tratados son considerablemente pocos (32% de los riesgos son altos-naranjas y rojos) a pesar de que la efectividad de los controles actuales estaba dada en un 43%, esto significa que realmente se debe trabajar en la efectividad de los controles más que en la implementación de nuevos controles, una situación que se puede presentar debido a la evolución tecnológica.

Tabla 3 8 Matriz de Riesgos [18]

ZONA	%	Total, riesgos
Aceptable	54,17	78
Tolerable	13,19	19
Inaceptable	19,44	28
Inadmisible	13,19	19

Ilustración 3-1 Distribución porcentual de riesgos



3.1.2 Proponer un plan de tratamiento para los riesgos identificados, considerando aquellos riesgos altos y estableciendo mecanismos de reducción con el fin de apoyar un proceso para el manejo de incidentes, tomando como referencia los controles de la norma ISO 27001:2013 y/o la NIST 800-53.

Como se determinó en la metodología, a continuación, se realiza un plan de controles para los riesgos que por su impacto deben ser tratados de manera inmediata (naranjas y rojos), para más detalle ver anexo A mapa de Riesgos.

Es importante precisar que muchos de los controles propuestos (tabla 3-9) también apoyan a que los riesgos bajos (amarillos y verdes) no suban su nivel.

Tabla 3 9 Plan de tratamiento [18]

RIESGOS ALTOS Considerando los controles actuales	TRATAMIENTO			Mapeo de controles con la norma	Descripción del plan: * Controlar o evitar: ¿cómo? * Transferir: ¿A quién? * Aceptar: ¿Por qué?	Plan de monitoreo	Responsable (basados en el caso de estudio y la cantidad de empleados de la compañía Tecnología para todos S.A.S)	Resultado Esperado
	Aceptarlo	Evitarlo	Controlarlo					
(1) -Posibilidad que la amenaza: Man in the middle, afecte el activo: Correo (outlook)			x	**A.13 Seguridad de las comunicaciones** A.13.1.2 Seguridad de los servicios de red **A.12.4 Registro y seguimiento** A.12.4.3 Registro del admiNISTrador y del operador	Implementación IDS	Configuración de reglas con notificaciones de comportamientos anómalos, como envió de notificaciones repetitivas, etc	Equipo de ciberseguridad	Detectar los intrusos de manera temprana
(2) -Posibilidad que la amenaza: Man in the middle, afecte el activo: Almacenamiento local/remota (OneDrive, SharePoint, SAN, NAS)			x	**A.9.1 Control de acceso** A.9.1.2 Acceso a redes y a servicios en la red A.9.2.2 SumiNISTro de acceso a usuarios	Implementación de sistema PAM	mantienen un monitoreo constante sobre los usuarios regulares	Equipo de ciberseguridad	Detectar los intrusos de manera temprana
(3) -Posibilidad que la amenaza: Man in the middle, afecte el activo: VoIP/ToIP			x	**A.13 Seguridad de las comunicaciones** A.13.1.2 Seguridad de los servicios de red **A.12.4 Registro y seguimiento** A.12.4.3 Registro del admiNISTrador y del operador	Implementación IDS	Configuración de reglas con notificaciones de comportamientos anómalos, como envío de notificaciones repetitivas, etc	Equipo de ciberseguridad	Detectar los intrusos de manera temprana
(22) -Posibilidad que la amenaza: MALWARE, afecte el activo: Windows 10			x	**A.13 Seguridad de las comunicaciones** A.13.1.3 Separación en las redes **A.12 Seguridad de las operaciones** A.12.2 Protección contra código malicioso A.12.3 Copias de respaldo	Directivas a los grupos por DA para que ningún usuario tenga acceso admiNISTrador de los dispositivos. Programación de escaneos automáticos al finalizar las jornadas laborales. Implementación de Itune	Revisión de los objetos que son enviados a cuarentena al momento del escaneo. Control y gestión del alertamiento generado en Itune	Equipo de ciberseguridad	Se espera que a través de la restricción de ejecución de programas, no se pueda ejecutar ningún macro o .exe
(23) -Posibilidad que la amenaza: MALWARE, afecte el activo: Windows Server 2008 (estándar, R2)			x	**A.13 Seguridad de las comunicaciones** A.13.1.3 Separación en las redes **A.12 Seguridad de las operaciones** A.12.2 Protección contra código malicioso A.12.3 Copias de respaldo	Migración -Creación de un ARO para responsabilizar e informar las consecuencias que tiene no migrar este sistema operativo -Implementación ATP	Los aros son revisados por el personal de calidad de manera semestral y se revisan que se estén ejecutando controles como aplicación de antivirus, etc Revisar el alertamiento que se presenta para	Equipo de Calidad Equipo de ciberseguridad	Se espera que el sistema debido al alto riesgo que tenga este protegido con los controles mininos de seguridad (Hardening, antivirus, etc)

				A.12.6 Gestión de la Vulnerabilidad Técnica A.14.1 Adquisición, desarrollo y mantenimiento de los sistemas		determinar acciones de mejora		

En la Tabla 3 9 Plan de tratamiento [18] se determinan además de los riesgos críticos, la estrategia determinada para el plan de tratamiento de cada uno donde se observa que el 100% de los riesgos críticos serán controlados y no se contemplan las estrategias asociadas a evitar o aceptarlos, debido a los impactos que podrían generar para una organización. Así mismo se establecen 85 controles de la norma ISO27001 que permiten determinar cómo se van a controlar estos riesgos críticos y se definen además como se va garantizar un plan de monitoreo que permita el cumplimiento adecuado de los controles definidos para cada uno de ellos, indicando por consiguiente quienes son los responsables del manejo del riesgo y cuál es el resultado esperando luego de la aplicación de los controles. Con el objeto de cerrar las brechas que se dejan al momento de establecer los ciclos para una adecuada gestión del riesgo.

3.2 Fase 2: Caracterizar diferentes normas para el manejo y respuesta de los incidentes de seguridad, acorde a los riesgos detectados y la aplicabilidad en empresas de servicios informáticos

De acuerdo con la hoja de ruta definida para el cumplimiento del objetivo, a continuación, se presentan los resultados obtenidos.

3.2.1 Caracterizar las normas para la creación de la estrategia para el manejo de incidentes, considerando la norma NIST SP800-61 (Computer Security Incident Handling Guide), ISO 27035, el proyecto amparado de LACNIC (CSIRT) y/o los manuales del Ministerio de las TIC.

Tal como se indicó en la metodología, a continuación, la tabla 3-10 describe de manera genérica las normas seleccionadas, allí se realiza una descripción y caracterización de cada una. Bajo tres conceptos genéricos que se utilizaron para describirlas.

Tabla 3 10 Normas versus criterios

	VENTAJAS	Proceso	Enfocada en: seguridad de la información, ciberseguridad
NIST	NIST SP 800-61 enfatiza el análisis de los incidentes junto con la detección	Define las siguientes fases en el proceso de gestión de incidentes. ✓ Preparación ✓ Detección y análisis ✓ Contener, erradicar y recuperar ✓ Lecciones aprendidas Es una descripción general de las actividades que se deben tener en cuenta en cada una de las fases	Ciberseguridad
ISO27035	El término "gestión de incidentes de seguridad de la información" se utiliza en esta Norma Internacional para abarcar la gestión no solo de los incidentes de seguridad de la información, sino también de las vulnerabilidades de seguridad de la información. Se alinea con la gestión de crisis Integral las lecciones aprendidas con el sistema de gestión de riesgos Entrega plantilla para la notificación de vulnerabilidades	Define las siguientes fases en el proceso de gestión de incidentes. **Planee y prepare** **Detecte y reporte** **Evaluación y decisión** **Fase de Respuestas** **Lecciones aprendidas** La norma realiza una descripción detallada de cada una de las fases, es clara sobre las actividades puntuales a realizar en cada una de ellas, caracteriza los determinados procesos en plantillas como base.	Seguridad de la información
Proyecto amparo lacnic	Describe un proceso completo para la construcción de un csirt en las organizaciones. Es un modelo para la zona donde se quiere implementar el proyecto (america latina). Se integra con el estandar ISO estándar ISO 27002:2013 para la implementación de los controles de seguridad en una organización. Incluye Políticas de Gestión de Riesgos en un Centro de Respuesta	Su eje principal se encuentra en la construcción de un CSIRT. Este proyecto define cada una de las actividades que debe cumplir un CSIRT, como es su construcción como es el modelo de trabajo. Define las actividades, roles a realizar dentro de una organización. Define aspectos a tener en cuenta dentro de la creación de políticas para la gestión de riesgos e incidentes	Seguridad de la información
Guía para la gestión de incidentes , Mintic	Alineada con la gestión de la continuidad	Define las actividades del CSIRT grosso modo. ✓ Incluye las siguientes actividades macro, basadas en la norma NIST. ✓ Preparación ✓ Recursos de comunicación ✓ Detección evaluación y análisis	Seguridad de la información

		✓ contención erradicación y recuperación. ✓ actividades posts-incidentes ✓ lecciones aprendidas define los roles y perfiles necesarios para la atención de incidentes	
Marco NIST Ciberseguridad	NIST observa y monitorea los recursos y referencias relevantes, incluso define una hoja de ruta para la actualización del modelo. Es decir, este marco actúa bajo un ciclo PHVA. Las funciones se alinean con las metodologías existentes para la gestión de incidentes y ayudan a mostrar el impacto de las inversiones en ciberseguridad. Es posible implementar por niveles. lo que permite visionar hacia donde se quiere llegar. Además, permite perfilar el nivel actual y fortalecer las prácticas de ciberseguridad	El marco de ciberseguridad consta de tres componentes principales: Framework Core: Identificar, Proteger, detectar, responder, recuperar Niveles de implementación Perfiles En cada parte del proceso se realiza una descripción clara de cómo realizar una implementación, para ello se apoya de otras normas las fases.	ciberseguridad

Una vez se ha realizado una descripción de cada una de las normas se procede a enmarcar el objetivo general dentro de tres criterios que tienen como objetivo definir la estrategia adecuada para el manejo de incidentes, procesos definidos, ciclos evolutivos y definición de estrategias enfocadas en reducción de riesgos. Todo ello con el fin de cumplir con el desarrollo de la siguiente actividad.

La tabla 3-10 normas versus criterios, detalla cada una de las ventajas, describe el Marco NIST Ciberseguridad y la ISO27035 como los procesos que entregan mayor valor dentro de cada una de los lineamientos al momento de tratar un incidente de ciberseguridad, la NIST por su parte deja claramente cómo se debe realizar los procesos de observación y monitoreo de los recursos y referencias relevantes, incluso define una hoja de ruta para la actualización del modelo, así mismo la ISO establece formatos base para cada uno de los procesos críticos sobre los incidentes de seguridad, lo que permite determinar cuáles son las actividades puntuales en cada fase, cuáles son los roles y las funciones esenciales al momento de implementar la norma sobre el manejo de un incidente.

Al combinar el marco NIST de ciberseguridad con la norma ISO27035 es posible encontrar un balance sobre el proceso macro con cada uno de los componentes que entrega la norma ISO27035, estableciendo la completitud de los lineamientos y haciendo uso de los formatos ya definidos en la norma.

3.2.2 Establecer la estrategia para el manejo de incidentes a partir de la norma seleccionada y los riesgos altos detectados. Dicha estrategia estará enfocada a la reducción de riesgos y el procedimiento de cómo actuar frente un evento de ciberseguridad que afecte la información.

Para establecer la metodología es necesario seleccionar la norma que dará los lineamientos para actuar frente a un incidente de seguridad. A continuación, en la tabla Tabla 3-11 “Normas y calificación criterios” se presenta la metodología para la selección de la norma, dicha estrategia estuvo basada bajo un proceso documental apoyado en la selección de tres criterios que enmarcan el objetivo general.

A cada norma, según la definición de los criterios y la documentación, se le dio una calificación basada en la definición de la Tabla 3 11 Normas y calificación criterios

Tabla 3 11 Normas y calificación criterios

	Procesos definidos	un ciclo que permita evolucionar en el tiempo	estrategia enfocada en la reducción de riesgos	Calificación total
NIST	1	1	1	3
ISO27035	2	1	2	5
Proyecto amparo lacnic	2	1	1	4
Guia para la gestión de incidentes, Mintic	1	1	1	3
Marco NIST Ciberseguridad	1	2	2	5

De acuerdo con la metodología definida la norma seleccionada fue aquella con mayor calificación posible, sin embargo, al realizar la calificación de cada una de las se observa que la norma ISO27035 y el Marco NIST Ciberseguridad quedaron en paralelismo al momento de los resultados, por lo cual se procede a analizar las particularidades de cada una.

Se detecta que ambas normas cuentan con una estrategia dinámica enfocada en la reducción de riesgos, la norma ISO27065 define actividades claras y puntuales para

revisar, identificar y realizar mejoras a la evaluación de riesgos de seguridad de la información existente de las organizaciones, así como los resultados de la revisión de la gestión, el resultado de las lecciones aprendidas es incluidas dentro de la gestión de riesgos. Por su parte el marco NIST [9] permite implementaciones basadas en riesgos que se adaptan a las necesidades de la organización favoreciendo los retornos en la inversión de cada organización. Es decir, tanto el marco NIST como la norma ISO27035 orientan las lecciones aprendidas a el proceso de gestión de riesgos, lo que permite fortalecer el enfoque en la prevención y así contribuir a la justificación de los presupuestos y los recursos de las organizaciones.

Al revisar la valoración del criterio “procesos definidos” en cada una de las normas que igualaron su calificación final, se detecta que la norma [21] ISO27035 dentro de sus fases definidas para la gestión de incidentes entrega actividades claves para realizar dentro del proceso de preparación, la norma incluye la creación de una política para la creación de incidentes (informa quienes son las partes involucradas y cuál es el contenido de una norma), la cual se integra con las demás políticas organizaciones, describe los procesos y tareas del equipo de respuesta a incidentes entrega las pautas para un programa de concientización a usuario y define verificaciones de los procesos; en la fase de detección y reporte establece cuales son los posibles artefactos para detectar el origen de un incidente, entrega posibles herramientas y en su ejercicio, describe un formulario del sistema de seguimiento de incidentes; en la fase de evaluación y decisión precisa las actividades para saber si es un incidente de seguridad o un evento, entrega una guía los requerimientos necesarios y objetos relevantes a documentar en los incidentes de seguridad, en la fase de responsabilidades define pasos a seguir de los involucrados de acuerdo a lo sucedido, define las actividades para la adquisición de la evidencia y define un plan de comunicación de eventos de incidentes de seguridad en su fase de lecciones aprendidas indica actividades para revisar, identificar y realizar mejoras dentro de todo el proceso evolutivo.

El marco NIST posee una característica parcial del criterio proceso definido, en este marco se precisan cuáles son las técnicas dentro de la norma, define tres componentes dentro del proceso macro, los cuales según se pueden evidenciar en la siguiente Ilustración 3-2 Técnicas del marco NIST están referenciados en otras normas. Dichas normas describen el proceso que se debe realizar, pero no hay una definición clara del como ejecutarlo.

Ilustración 3-2 Técnicas del marco NIST [9]

Function	Category	Subcategory	Informative References
IDENTIFY (ID)	**Asset Management (ID.AM):** The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.	**ID.AM-1:** Physical devices and systems within the organization are inventoried	**CIS CSC** 1 **COBIT 5** BAI09.01, BAI09.02 **ISA 62443-2-1:2009** 4.2.3.4 **ISA 62443-3-3:2013** SR 7.8 **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2 **NIST SP 800-53 Rev. 4** CM-8, PM-5
		ID.AM-2: Software platforms and applications within the organization are inventoried	**CIS CSC** 2 **COBIT 5** BAI09.01, BAI09.02, BAI09.05 **ISA 62443-2-1:2009** 4.2.3.4 **ISA 62443-3-3:2013** SR 7.8 **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2, A.12.5.1 **NIST SP 800-53 Rev. 4** CM-8, PM-5
		ID.AM-3: Organizational communication and data flows are mapped	**CIS CSC** 12 **COBIT 5** DSS05.02 **ISA 62443-2-1:2009** 4.2.3.4 **ISO/IEC 27001:2013** A.13.2.1, A.13.2.2 **NIST SP 800-53 Rev. 4** AC-4, CA-3, CA-9, PL-8
		ID.AM-4: External information systems are catalogued	**CIS CSC** 12 **COBIT 5** APO02.02, APO10.04, DSS01.02 **ISO/IEC 27001:2013** A.11.2.6 **NIST SP 800-53 Rev. 4** AC-20, SA-9
		ID.AM-5: Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value	**CIS CSC** 13, 14 **COBIT 5** APO03.03, APO03.04, APO12.01, BAI04.02, BAI09.02 **ISA 62443-2-1:2009** 4.2.3.6 **ISO/IEC 27001:2013** A.8.2.1 **NIST SP 800-53 Rev. 4** CP-2, RA-2, SA-14, SC-6
		ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and	**CIS CSC** 17, 19 **COBIT 5** APO01.02, APO07.06, APO13.01, DSS06.03

El marco NIST se complementa en el criterio "proceso definido" de la norma ISO27035, la cual documenta no solo la definición de la cada fase si no el cómo podría usarlo basado en ejemplos, herramientas y plantillas.

Sin embargo, la norma ISO27035 define dentro de las practicas documentadas para la gestión de incidentes, las actividades post incidentes que apoyan los procesos cíclicos para fortalecer las tácticas de desarrollo sostenible en el tiempo, pero los métodos evolutivos requieren además técnicas que determinen un nivel actual de seguridad y un punto objetivo lo cual permite un entendimiento adecuado de la postura inicial y trazar un objetivo evolutivo en el tiempo. La norma NIST de ciberseguridad [9] dentro de las componentes del marco define un numeral específico para el entendimiento del perfil actual, donde el objetivo se basa en que de las organizaciones pueden utilizar este punto para identificar oportunidades que permitan mejorar la postura de seguridad cibernética comparando un Perfil "actual" (el estado "tal como está") con un Perfil "objetivo" (el estado "por ser").

Los Perfiles se pueden utilizar para realizar autoevaluaciones y comunicarse dentro de una organización o entre organizaciones, además el marco NIST referencia cuatro niveles de implementación que tienen como objeto proporcionar un contexto sobre cómo una organización considera el riesgo de seguridad cibernética y los procesos establecidos para gestionar dicho riesgo. Los Niveles Parcial (Nivel 1) a Adaptable (Nivel 4) describen un grado cada vez mayor de rigor y sofisticación en las prácticas de gestión de riesgos de seguridad cibernética. Ayudan a determinar en qué medida la gestión del riesgo de seguridad cibernética se basa en las necesidades empresariales y se integra a las prácticas generales de gestión del riesgo de una organización.

Dentro de la documentación del marco se destacan casos de éxito en su aplicación, [25] ISACA, por ejemplo, indica que el framework de ciberseguridad ha ayudado a ISACA a transmitir la importancia de la ciberseguridad a sus 140.000 componentes en todo el mundo. Además, refuerza la relevancia del campo y solidifica la comprensión de la importancia de la ciberseguridad para las misiones de las organizaciones. Según la referencia en mención se detecta que a través de una encuesta a numerosos CISO y a quienes poseen la certificación Certified in Information Security Management® (CISM®), ISACA descubrió que de los casi 800 encuestados, más del 75% conocía el Marco y creía que ayuda a elevar la importancia general de la seguridad cibernética.

Esto permite sintetizar que los resultados de la evaluación de la Tabla 3-11 Normas y calificación criterios describen una igualdad en las normas ISO27035 y el marco NIST de ciberseguridad, porque cada una de ellas posee características relevantes en los lineamientos definidos, la norma ISO27035 establece todos los pasos para una apropiada definición de los procesos que se deben definir en una estrategia para el manejo de incidentes de ciberseguridad además es fuerte en la definición de técnicas enfocadas en la reducción de riesgos, sin embargo es una norma que se debe complementar con prácticas que fortalezcan el proceso de evolución continua y para ello el marco de ciberseguridad de NIST cuenta con los componentes perfiles y niveles de todo el ciclo que establecen técnicas dentro de un proceso que le apuntan a la evolución continua.

Por lo cual este proyecto define las normas ISO27035 y el Marco de ciberseguridad de NIST como la estrategia adecuada para el manejo de incidentes de ciberseguridad, haciendo una integración funcional entre ellas.

3.3 Fase 3: Evaluar el modelo de ciberseguridad para el manejo de incidentes a través de un caso de estudio.

De acuerdo con la hoja de ruta definida para el cumplimiento del objetivo, a continuación, se presentan los resultados obtenidos.

3.3.1 Actividad 1: Creación del modelo de ciberseguridad que integre el manejo de incidentes de seguridad, esto se realizará con base en las normas de riesgos, ISO 27001, NIST y las de gestión de incidentes. El modelo debe permitir la reducción y tratamiento de los incidentes identificados para las empresas tercerizadoras de servicios informáticos.

Como resultado de esta actividad, el Modelo de Ciberseguridad que logra cubrir los diferentes riesgos encontrados en las organizaciones que ofrecen servicios informáticos, establece varias partes:

- ✓ Introducción.
- ✓ Objetivo del modelo de ciberseguridad
- ✓ Estructura y descripción
- ✓ Estrategia de seguridad
- ✓ Políticas
- ✓ Procedimiento paras el Manejo de incidentes de seguridad

A continuación, se hace una descripción de cada uno de los componentes:

Introducción

La seguridad de la información hace parte de la sostenibilidad de las organizaciones, una falla en esta área dentro de los procesos irrumpe actividades esenciales con consecuencias irremediables en algunos casos.

Este documento tiene como objetivo desarrollar una serie de actividades como parte de la estrategia para realizar un manejo de incidentes de seguridad de la información desde la prevención de los mismos, se busca entregar un modelo que sea evolutivo en el tiempo y que indique los lineamientos a realizar desde la gestión del riesgo como prevención de los incidentes y una serie de acciones para operar en los casos donde el riesgo se materializa.

Objetivo

Este modelo de ciberseguridad tiene como objeto hacer uso de las buenas prácticas que se presentan en normas internaciones para el manejo de incidentes como el framework de ciberseguridad de la NIST y la norma ISO27035 usando un insumo de riesgos basando en los activos que tienen empresas que ofrecen servicios informáticos con el objeto de crear un modelo desde la prevención para establecer un adecuado manejo de incidentes de seguridad, las normas usadas incluyen procedimientos claros en cada una de sus fases lo que permite fortalecer el manejo de incidentes.

ISACA en el modelo de negocio para la seguridad de la información manifiesta que los profesionales de la seguridad han estado reaccionando ante amenazas, riesgos, legislación, infracciones, tecnologías emergentes de manera reactiva debido a que se exige un alto cumplimiento con estándares que no son claros en el desarrollo del cómo aplicarlos lo que trae como consecuencia la inversión de poco tiempo para la creación, innovación y estrategias de valor en el área de seguridad de la información [1].

Por lo cual se entrega un modelo con lineamientos específicos para actuar frente a la materialización de un riesgo en empresas que prestan servicios informáticos contribuyendo con el desarrollo de modelos que aporten a una respuesta adecuada ante un incidente de ciberseguridad

El alcance de este modelo se centra en las organizaciones que prestan servicios informáticos, donde su eje principal es velar por los pilares de la seguridad de la información disponibilidad, integridad y confidencialidad de cada uno de los clientes que confía el activo información.

Modelo de ciberseguridad para empresas de servicios informáticos para fortalecer un manejo de incidente de seguridad

El modelo de ciberseguridad para empresas de servicios informáticos que permite fortalecer el proceso para el manejo de incidentes de seguridad contempla un proceso que consta de cinco funciones basadas en el core del framework de ciberseguridad de NIST.

En el modelo se contemplan 4 niveles (parcial, riesgo informado, repetible, adaptable) de implementación del framework de ciberseguridad de NIST, [2] estos brindan un lineamiento a las organizaciones para suponer un nivel apropiado en su esquema de ciberseguridad su objetivo es definir el apetito por el riesgo, prioridad de la misión y el presupuesto.

Las actividades correctivas como punto final en el modelo definen cuales son las acciones a implementar dentro de la estrategia, sustentadas bajo las lecciones aprendidas esto para los casos donde los controles son insuficientes y sea necesario desplegar la actividad propia para el manejo de incidentes.

Un modelo basado en el manejo de riesgos permite a las organizaciones determinar estrategias fundamentadas en la prevención, lo cual es clave dentro de las actividades propias que le apuntan a la ciberseguridad porque permite la reducción de incidentes, si se disminuyen los incidentes de seguridad hay mejores posibilidades de maniobra ante la aparición de alguno.

Para la construcción del modelo de ciberseguridad es necesario crear un proceso que permita encontrar los riesgos y a partir de allí priorizar los planes de remediación, para ello se estableció un procedimiento de detección de riesgos basado en la norma ISO27005:2018, donde se inició por establecer el contexto y alcance, luego se procede a realizar el respectivo análisis de los activos y los riesgo de acuerdo a los resultados de allí se realiza una evaluación de riesgos y finalmente se define los planes de tratamiento.

La creación del proceso de riesgos para empresas que ofrecen servicios informáticos entrego como resultados la matriz de riesgos obtenida en el objetivo 1 **Tabla 3-8** matriz de Riesgos [18]

Para crear un modelo que permita establecer un adecuado manejo de incidentes de seguridad se parte de los riesgos detectados como inadmisibles e inaceptables los cuales, aunque son considerados en promedio el 16% se deben establecer procedimientos, nuevos controles o incluso actualizaciones a políticas o directrices, no ser tratados podría generar incidentes de seguridad con graves consecuencias.

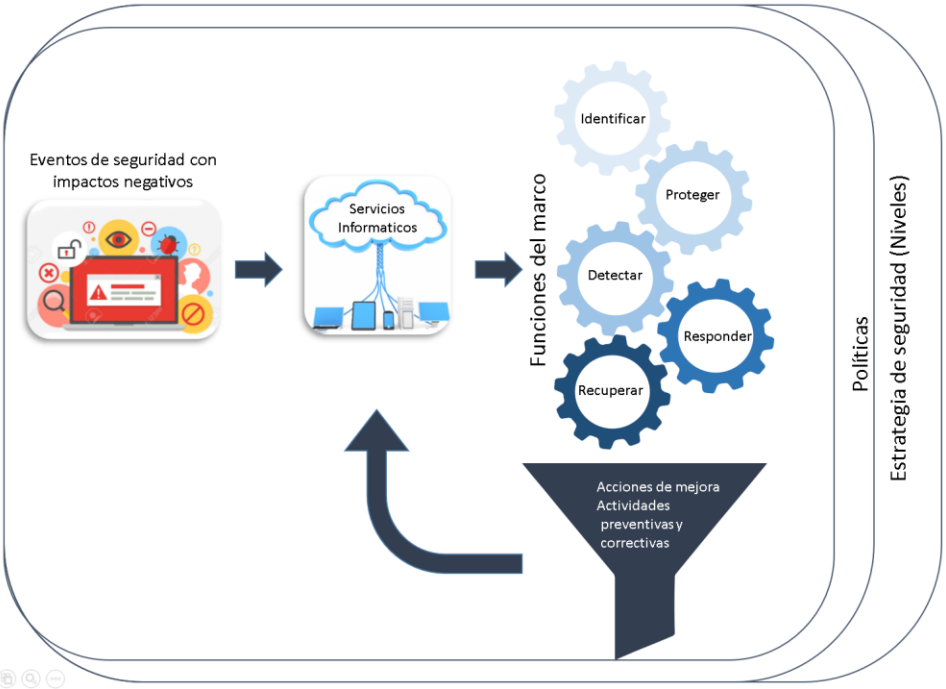
Cada uno de los pasos que establece el framework NIST fue mapeado durante el proceso de riesgos con el objeto de garantizar un cubrimiento total a cada una de las categorías y crear un modelo para la gestión de incidentes que esté basado en un adecuado manejo de incidentes.

Cada uno de los controles y acciones que genere este modelo debe estar enmarcado dentro de políticas, las cuales entregan lineamientos claros sobre lo que deben realizar cada uno de los actores del modelo y deben ir aliénanos a una estrategia corporativa que fortalezca un adecuado manejo de incidentes de seguridad desde la prevención.

Descripción del modelo de operación

A continuación, se diagrama el funcionamiento del modelo de ciberseguridad (ilustración 3-3) que le apunta a fortalecer un adecuado manejo de incidentes de seguridad, el cual se estructura bajo cinco funciones que se integran para guiar a las empresas que prestan servicios informáticos en la reducción de riesgos y manejo de incidentes como parte de una estrategia de ciberseguridad.

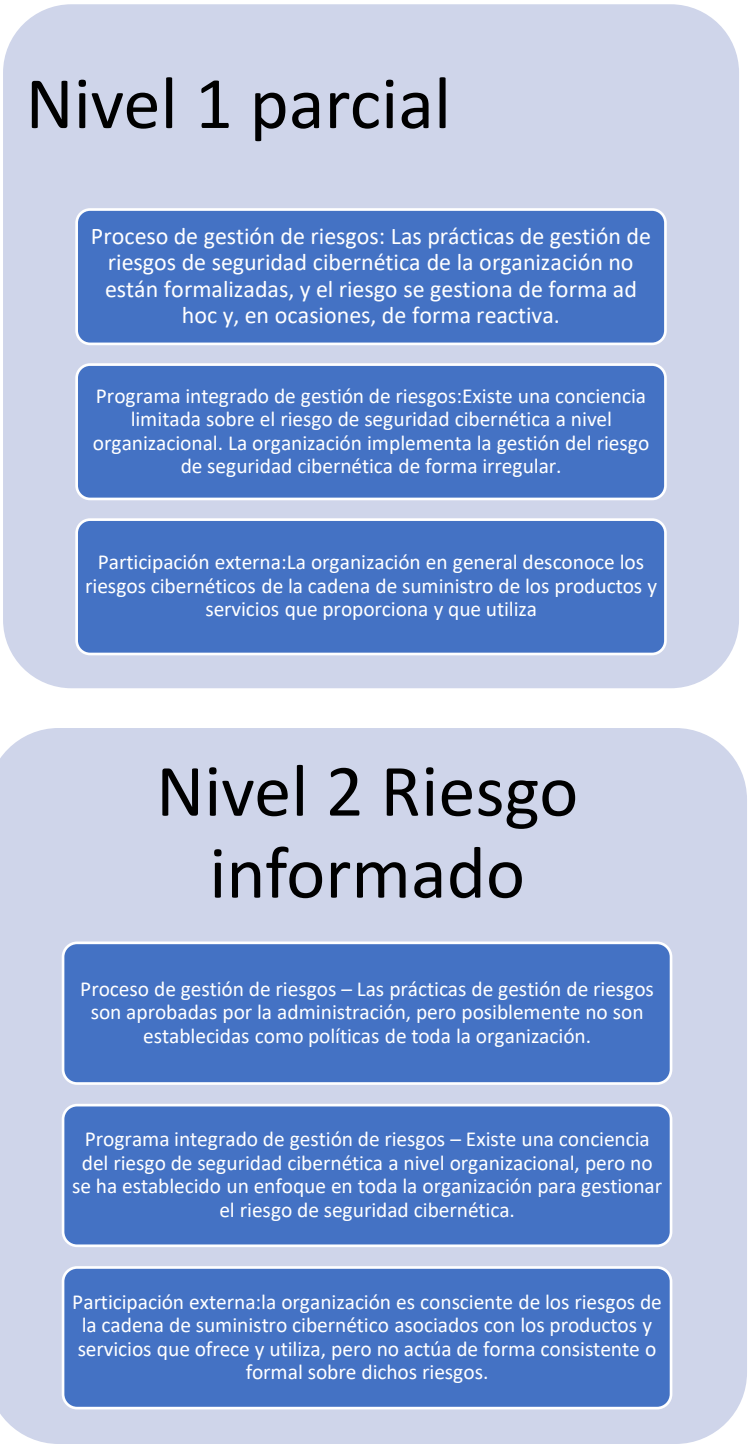
Ilustración 3-3 Modelo de ciberseguridad. Fuente construcción propia



De acuerdo a la definición de las normas ISO27035 y el marco Marco NIST de Ciberseguridad desarrollado bajo el objetivo número 2 se inició el proceso de construcción del modelo de ciberseguridad teniendo en cuenta los siguientes pasos:

La estrategia de seguridad se basa en la identificación por niveles que entrega el marco NIST de la implementación del sistema, aquí básicamente se define de acuerdo a las actividades realizadas el nivel de madurez actual y objetivo, para ello el marco NIST precisa los siguientes niveles.

Ilustración 3-4 Niveles Marco NIST



Nivel 3 Repetible

Proceso de gestión de riesgos – Las prácticas para la gestión de riesgos de la organización se aprueban formalmente y se expresan como políticas.

Programa integrado de gestión de riesgos – Existe un enfoque de toda la organización para gestionar el riesgo de seguridad cibernética. Las políticas, procesos y procedimientos informados sobre riesgos se definen e implementan según lo previsto, y se revisan.

Participación externa:Colabora y recibe regularmente información de otras entidades que complementan la información generada internamente, y comparte información con otras entidades.

Nivel 4 Adaptable

Proceso de gestión de riesgos – La organización adapta sus prácticas de seguridad cibernética basándose en actividades previas y actuales de ciberseguridad, el cual incluye las lecciones aprendidas y los indicadores predictivos

Programa integrado de gestión de riesgos – Existe un enfoque en toda la organización para gestionar el riesgo de seguridad cibernética que utiliza las políticas, los procesos y los procedimientos informados sobre riesgos para abordar posibles eventos de seguridad cibernética. Se entiende claramente la relación entre el riesgo de seguridad cibernética y los objetivos de la organización, y se tienen en cuenta al tomar decisiones

Participación externa – La organización entiende su rol, sus dependencias y sus dependientes en el ecosistema más amplio y contribuye a una mayor comprensión de los riesgos por parte de la comunidad. Recibe, genera y revisa información priorizada que informa el análisis continuo de sus riesgos a medidaque evolucionan los paisajes de amenazas y tecnología.

Las políticas dentro del modelo se definen acorde a los riesgos detectados para empresas del sector informático, lo que permite un aseguramiento estratégico en la implementación de controles técnicos, básicamente son las directrices y estándares que se deben seguir en una organización.

Para la definición de las políticas que se entregan en el modelo se realizó una relación de los riesgos contra los controles, por ejemplo, se detectó que de los 38 riesgos un 38% se resuelven con el establecimiento de directrices y controles técnicos definidos en políticas de uso aceptable de activos, a continuación (ilustración 3-5), se detalla el % de políticas asociadas a los riesgos encontradas para empresas del sector.

Ilustración 3-5 Distribución de políticas por riesgos

Las funciones del marco detallan el ciclo end to end de todo el modelo de acuerdo con lo establecido por el marco NIST, el marco se usa dentro del modelo como la referencia de

los pasos a seguir para la construcción del modelo y por su parte cada paso se establece bajo los procedimientos, parámetros, ejemplos, directrices que entrega la norma ISO27035.

La identificación del objetivo es la descripción de las acciones hacia las cuales se direccionan cada uno de los pasos que se siguen dentro del modelo enfocados todos a la creación de un modelo desde la prevención que permite establecer un adecuado manejo de incidentes de seguridad.

La descripción del modelo entrega de manera genérica las actividades que se deben seguir en cada una de las etapas, pero además realiza una integración con el proceso de gestión de riesgos que se debe crear para llegar al desarrollo de las funciones del marco.

Las funciones del marco mapean los riesgos de acuerdo con su objetivo, el marco entrega seis funciones detalladas a continuación.

1) Identificación: Es el desarrollo de una comprensión organizacional para administrar el riesgo de seguridad cibernética para sistemas, personas, activos, datos y capacidades, aquí se identifican todos los riesgos inadmisibles e inaceptables detectados para una organización que presta servicios informáticos.
2) Protección: Es el desarrollo e implementación de medidas de seguridad adecuadas para garantizar la entrega de servicios críticos. En este punto se identifican nuevos controles para los riesgos detectados para una organización que presta servicios informáticos.
3) Detección: Es la fase que permite desarrollar e implementar actividades apropiadas para identificar la ocurrencia de un evento de seguridad cibernética; básicamente son las actividades que se deben establecer dentro de un plan de monitoreo que permitan realizar una medición de la eficiencia de cada uno de los controles.
4) Responder: Son todas las actividades enfocadas en ejecutar las acciones necesarias para resolver un incidente de seguridad cibernética; aunque el modelo de ciberseguridad está basado en la prevención de un incidente de seguridad su objetivo principal es construir un modelo que permita una gestión adecuada de incidentes de seguridad, en ese sentido es importante definir si un control es ineficiente cuales son los pasos que se deben seguir para responder ante dicha situación, aquí se identifican las actividades referentes a la caracterización de la situación, clasificación del incidente y escalamientos.

5) Recuperar: aquí se definen cuáles son las actividades que se deben realizar para conservar los planes de resiliencia y reestablecer cualquier capacidad o servicio que se haya visto afectado debido a un incidente de seguridad cibernética, se definen los momentos adecuados para la activación de un plan de continuidad, la activación de las mesas de crisis e incluso los procedimientos para la recuperación de servicios.
6) Actividades de mejora: en esta fase se contemplan estas actividades para incluir un proceso que asegure un aprendizaje de los incidentes que se hayan materializado, esto incluye el manejo de los pasos para la solución del incidente y como fueron tratados.

A continuación, se hace la descripción de los resultados obtenidos por cada uno de los pasos que se definen en el modelo (ilustración 3-3)

Estrategia de seguridad

La estrategia de seguridad debe estar alineada con la planeación corporativa y se define como la hoja de ruta de inicio allí se deben definir aspectos como el apetito del riesgo bajo el cual la organización trabajara la adecuada gestión del riesgo, además debe ir acorde a los objetivos empresariales.

Al implementar el modelo la organización define un nivel 3 del marco NIST debido a que las prácticas de gestión de riesgo se basan en la predicción de incidentes de seguridad manejado bajo la ISO 27005:2018 con un enfoque orientado en el uso de políticas para abordar los eventos de seguridad de la información sin embargo la participación externa se realiza en un solo sentido recibiendo regularmente información de otras entidades que complementan la información generada internamente compartiendo información con otras entidades pero no contribuye de manera activa en el ecosistema externo.

Políticas del marco

La creación de las políticas del marco está enfocada en la detección de los riesgos para empresas del sector, dichas políticas le apuntan a disminuir el riesgo desde lineamientos entregados a los usuarios finales hasta la creación de controles técnicos, acorde a la definición de las políticas requeridas se definen las siguientes políticas.

- Política de uso aceptable de los activos

- ✓ Mensajería electrónica
- ✓ Uso de repositorios
- ✓ Uso de internet

- Política de antivirus
- Política de contraseñas
- Política de comunicaciones seguras
- Política de criptografía
- Política asignación de privilegios
- Procedimiento asociado al análisis de riesgo operativo (ARO)

La documentación referente a la definición de cada política y procedimiento se encuentra en el anexo B Políticas

Funciones del marco

Las funciones del marco se toman del framework de ciberseguridad NIST y se integran para proporcionar un conjunto de actividades enfocadas en manejar los riesgos de ciberseguridad de una empresa del sector informático, es una guía que permite a las organizaciones visualizar el manejo que se le debe dar a los mismos, implementando controles desde la prevención, sin embargo, también se establecen controles re activos para dar un lineamiento sobre cómo actuar en los casos donde los escenarios se convierten en incidencias de seguridad por diversas situaciones.

Las funciones describen actividades primordiales de seguridad cibernética a nivel macro las cuales se enfrentan a cada uno de los riesgos identificados para empresas del sector. Como en el marco de ciberseguridad NIST, estas funciones no conducen un estado estático, las funciones se deben realizar continuamente para construir una cultura operativa que aborde el riesgo dinámico de seguridad cibernética [1] a continuación se detalla la función de cada actividad, en donde primero se da una definición acerca del significado de cada función y posterior se anexa la tabla con el detalle:

- ✓ **Identificar** es desarrollar una comprensión organizacional para administrar el riesgo de seguridad cibernética para sistemas, personas, activos, datos y capacidades. Para empresas que prestan servicios informáticos se mapea dentro de la función identificar los riesgos altos y medios detectados en el ejercicio realizado bajo la norma ISO27005:2018, son las situaciones con una probabilidad o impacto alto que eventualmente pueden afectar negativamente la organización en caso de masterizarse dicho riesgo.

Para la identificación de los riesgos se determinan los elementos denominados como los activos para empresas del sector informático, así como sus vulnerabilidades relacionadas también las posibles amenazas, con ello los escenarios de riesgos son evaluados bajo la probabilidad y el impacto que podrían causar para una organización.

A continuación (tabla 3-12), se presentan los escenarios de riesgos y cómo es cubierta por las diferentes actividades del marco.

Tabla 3-12 Función Identificar

Identificar	Posibilidad que la amenaza: Man in the middle, afecte el activo: Correo (outlook)
	Posibilidad que la amenaza: Man in the middle, afecte el activo: Almacenamiento local/remota (OneDrive, SharePoint, SAN, NAS)
	Posibilidad que la amenaza: Man in the middle, afecte el activo: VoIP/ToIP
	Posibilidad que la amenaza: MALWARE, afecte el activo: Windows 10
	Posibilidad que la amenaza: MALWARE, afecte el activo: Windows Server 2008 (estándar, R2)
	Posibilidad que la amenaza: MALWARE, afecte el activo: Server 20016 (Estándar y R2)
	Posibilidad que la amenaza: MALWARE, afecte el activo: Windows Server 2012
	Posibilidad que la amenaza: MALWARE, afecte el activo: Almacenamiento local/remota (OneDrive, SharePoint, SAN, NAS)
	Posibilidad que la amenaza: MALWARE, afecte el activo: Teléfonos Móviles Android
	Posibilidad que la amenaza: Phishing, afecte el activo: Correo (Outlook)
	Posibilidad que la amenaza: Phishing, afecte el activo: teléfonos Móviles Android
	Posibilidad que la amenaza: Defacement, afecte el activo: VoIP/ToIP
	Posibilidad que la amenaza: Ingeniería Social, afecte el activo: Usuarios/Clientes
	Posibilidad que la amenaza: Ingeniería Social, afecte el activo: Personal de soporte/administradores
	Posibilidad que la amenaza: Ransomware, afecte el activo: Windows 10

	Posibilidad que la amenaza: Ransomware, afecte el activo: Windows Server 2008 (estándar, R2)
	Posibilidad que la amenaza: Ransomware, afecte el activo: Server 20016 (Estándar y R2)
	Posibilidad que la amenaza: Ransomware, afecte el activo: Windows Server 2012
	Posibilidad que la amenaza: Ransomware, afecte el activo: Almacenamiento local/remota (OneDrive, SharePoint, SAN, NAS)
	Posibilidad que la amenaza: Ransomware, afecte el activo: Teléfonos Móviles Android
	Posibilidad que la amenaza: crakeo de contraseñas, afecte el activo: Correo (outlook)
	Posibilidad que la amenaza: crakeo de contraseñas, afecte el activo: Almacenamiento local/remota (OneDrive, SharePoint, SAN, NAS)
	Posibilidad que la amenaza: crakeo de contraseñas, afecte el activo: Teléfonos Móviles Android
	Posibilidad que la amenaza: Robo, afecte el activo: Usuarios/Clientes
	Posibilidad que la amenaza: Robo, afecte el activo: Personal de soporte/administradores
	Posibilidad que la amenaza: Robo, afecte el activo: Teléfonos Móviles Android
	Posibilidad que la amenaza: Daño o error humano, afecte el activo: Teléfonos Móviles Android
	Posibilidad que la amenaza: Daño o error humano, afecte el activo: Documentos y manuales
	Posibilidad que la amenaza: Acceso físico no autorizado, afecte el activo: Teléfonos Móviles Android
	Posibilidad que la amenaza: Instalación no autorizada de software, afecte el activo: Windows 10
	Posibilidad que la amenaza: Instalación no autorizada de software, afecte el activo: Windows Server 2008 (estándar, R2)
	Posibilidad que la amenaza: Instalación no autorizada de software, afecte el activo: Server 20016 (Estándar y R2)
	Posibilidad que la amenaza: Instalación no autorizada de software, afecte el activo: Windows Server 2012
	Posibilidad que la amenaza: Instalación no autorizada de software, afecte el activo: Almacenamiento local/remota (OneDrive, SharePoint, SAN, NAS)
	Posibilidad que la amenaza: Fuga de información, afecte el activo: Usuarios/Clientes
	Posibilidad que la amenaza: Fuga de información, afecte el activo: Personal de soporte/administradores
	Posibilidad que la amenaza: Fuga de información, afecte el activo: Teléfonos Móviles Android
	Posibilidad que la amenaza: Fuga de información, afecte el activo: Documentos y manuales

- ✓ **Proteger** – Desarrollar e implementar medidas de seguridad adecuadas para garantizar la entrega de servicios críticos. Los riesgos detectados para empresas que ofrecen servicios informáticos parten de la definición de unos controles iniciales, sin embargo, se detecta que estos son insuficientes y se adiciona los siguientes controles con el objetivo de proteger los riesgos y evitar su materialización.

Tabla 3 13 Función proteger

Proteger	Implementación IDS
	Implementación de sistema PAM
	Implementación IDS
	Microsegmentación que permita aislar las máquinas y no exponer los servicios hacia internet Implementación de PAM Implementación ATP Implementación de un ARO
	Microsegmentación que permita aislar las máquinas y no exponer los servicios hacia internet Implementación de PAM Implementación ATP Implementación de un ARO
	Microsegmentación que permita aislar las máquinas y no exponer los servicios hacia internet Implementación de PAM Implementación ATP Implementación de un ARO
	Microsegmentación que permita aislar las máquinas y no exponer los servicios hacia internet Implementación de PAM Implementación ATP Implementación de un ARO
	ON PREMISE Segmentación de Roles, restringiendo la ejecución de archivos. ONLINE Implementación de Cloud app security center
	Instalación de antivirus Implementación Intune
	Implementación Cloudgard
	Instalación de antivirus Implementación Intune Socialización acerca de las políticas de privacidad y confidencialidad
	Política de control de acceso Realizar segregación de roles para evitar abusos sobre la información contenida
	Socialización de la política de etiquetado de la información
	Socialización de la política de etiquetado de la información
	Micro Segmentación que permita aislar las máquinas Directivas desde el DA que no permitan ejecución de archivos a todos los usuarios Creación de un ARO para responsabilizar e informar las consecuencias que tiene no migrar este sistema operativo

	Micro Segmentación que permita aislar las máquinas Directivas desde el DA que no permitan ejecución de archivos a todos los usuarios Creación de un ARO para responsabilizar e informar las consecuencias que tiene no migrar este sistema operativo
	Microsegmentación que permita aislar las máquinas y no exponer los servicios hacia internet Implementación de PAM Implementación ATP Implementación de un ARO
	Microsegmentación que permita aislar las máquinas y no exponer los servicios hacia internet Implementación de PAM Implementación ATP Implementación de un ARO
	Para los productos Microsoft realizar bloqueo de ejecutables en las plataformas, para el almacenamiento on premise segregación de roles Actualización del firewall
	Implementación de antivirus Implementación de Intune
	Implementación de MFA para los productos Microsoft Implementación SSO para los productos que se puedan registrar contra directorio activo
	Implementación de MFA para los productos Microsoft Implementación SSO para los productos que se puedan registrar contra directorio activo
	Socialización masiva de la política de gestión de contraseñas Implementación MFA
	La información de los clientes reposara en repositorios internos de la organización y se implementara control de acceso
	Generar clausulas ligadas a los planes de desarrollo profesional que ofrece la organización.
	Socialización a través de campañas de sensibilización acerca del manejo de uso aceptable de dispositivos
	Socialización a través de campañas de sensibilización acerca del manejo de uso aceptable de dispositivos
	Segregación de roles e implementando un repositorio único en sharepoint con controles de acceso. Cada documento tendrá su control de versiones y modificaciones sobre el mismo, el área de calidad será el encargado de cargar cualquier cambio en las versiones
	Socialización de la política de la gestión de contraseñas
	Socialización a través de campañas de sensibilización la política de gestión de activos
	Implementación de PAM Implementación de un ARO Procesos disciplinarios

	Implementación de PAM Implementación de un ARO Procesos disciplinarios
	Implementación de PAM Implementación de un ARO Procesos disciplinarios
	Implementación de ARO´s Procesos disciplinarios
	Cláusulas de confidencialidad campañas de concientización Implementación de procesos disciplinarios
	Cláusulas de confidencialidad campañas de concientización
	Cláusulas de confidencialidad campañas de concientización
	Los documentos y manuales son almacenados en un repositorio interno, en una cuenta en sharepoint con acceso restringido. Se definirán cláusulas de confidencialidad para los retiros que se realicen en la organización.

- ✓ **Detectar** – Desarrollar e implementar actividades apropiadas para identificar la ocurrencia de un evento de seguridad cibernética. Se definen las siguientes actividades para el monitoreo de los riesgos las cuales permitirán detectar la materialización de un escenario, estas actividades permiten monitorear la efectividad y eficiencia de un control.

Tabla 3 14 Función detectar

DETECTAR	Configuración de reglas con notificaciones de comportamientos anómalos, como envío de notificaciones repetitivas, etc
	mantienen un monitoreo constante sobre los usuarios regulares
	Configuración de reglas con notificaciones de comportamientos anómalos, como envío de notificaciones repetitivas, etc
	Depuración alertamiento Análisis anual de los ARO´s que permita determinar si aún es necesario el componente
	Depuración alertamiento Análisis anual de los ARO´s que permita determinar si aún es necesario el componente
	Depuración alertamiento Análisis anual de los ARO´s que permita determinar si aún es necesario el componente
	Depuración alertamiento Análisis anual de los ARO´s que permita determinar si aún es necesario el componente
	Depuración semestral de objetos del DA. Administración y gestión de alertamiento
	Revisión anual de licenciamiento Revisión del alertamiento

	Gestión y administración de alertamiento Revisión anual del licenciamiento
	Revisión anual de licenciamiento Revisión del alertamiento
	Identificar por medio de los logs las ip´s que realizan modificaciones abusivas y aplicar bloqueos sobre estas. Auditoría de los roles y los usuarios nuevos y antiguos mensualmente
	Encuestas que midan el conocimiento de la política
	Encuestas que midan el conocimiento de la política
	Los aros son revisados por el personal de seguridad de manera semestral y se revisan que se estén ejecutando controles como aplicación de antivirus, etc Revisar el alertamiento que se presenta para determinar acciones de mejora
	Depuración alertamiento Análisis anual de los ARO´s que permita determinar si aún es necesario el componente
	Depuración alertamiento Análisis anual de los ARO´s que permita determinar si aún es necesario el componente
	Depuración alertamiento Análisis anual de los ARO´s que permita determinar si aún es necesario el componente
	Realizar monitoreo de cuentas mensual y depurar objetos. De manera semestral se debe revisar actualizaciones de los fabricantes Depuración de alertamiento
	Renovación del licenciamiento Monitoreo del alertamiento
	Realizar monitoreo al ADSYNC Realizar monitoreo de cuentas mensual y depurar objetos
	Realizar monitoreo al ADSYNC Realizar monitoreo de cuentas mensual y depurar objetos
	Encuestas de verificación del conocimiento de la política
	De manera anual se realizará una revisión de las personas que acceden a los repositorios y los permisos de acceso de cada repositorio
	Auditoria semestral de los planes de desarrollo profesional.
	Encuestas de verificación del conocimiento de la política
	Encuestas de verificación del conocimiento de la política
	Revisión semestral de la documentación del repositorio
	Encuestas que midan el conocimiento de la política
	Realizar encuestas acerca de la socialización de la política

	Por medio de herramientas como lansweeper se realizará un monitoreo de los usuarios que ingresan y los movimientos que realizan allí. Análisis de los logs de la herramienta PAM
	Por medio de herramientas como lansweeper se realizará un monitoreo de los usuarios que ingresan y los movimientos que realizan allí. Análisis de los logs de la herramienta PAM
	Por medio de herramientas como lansweeper se realizará un monitoreo de los usuarios que ingresan y los movimientos que realizan allí. Análisis de los logs de la herramienta PAM
	Por medio de herramientas como lansweeper se realizará un monitoreo de los usuarios que ingresan y los movimientos que realizan allí
	Pruebas que midan el nivel de madurez de las campañas de sensibilización.
	Renovación de relaciones laborales
	Pruebas que midan el nivel de madurez de las campañas de sensibilización.
	Realizar segregación de roles de manera semestral para realizar depuración de elementos

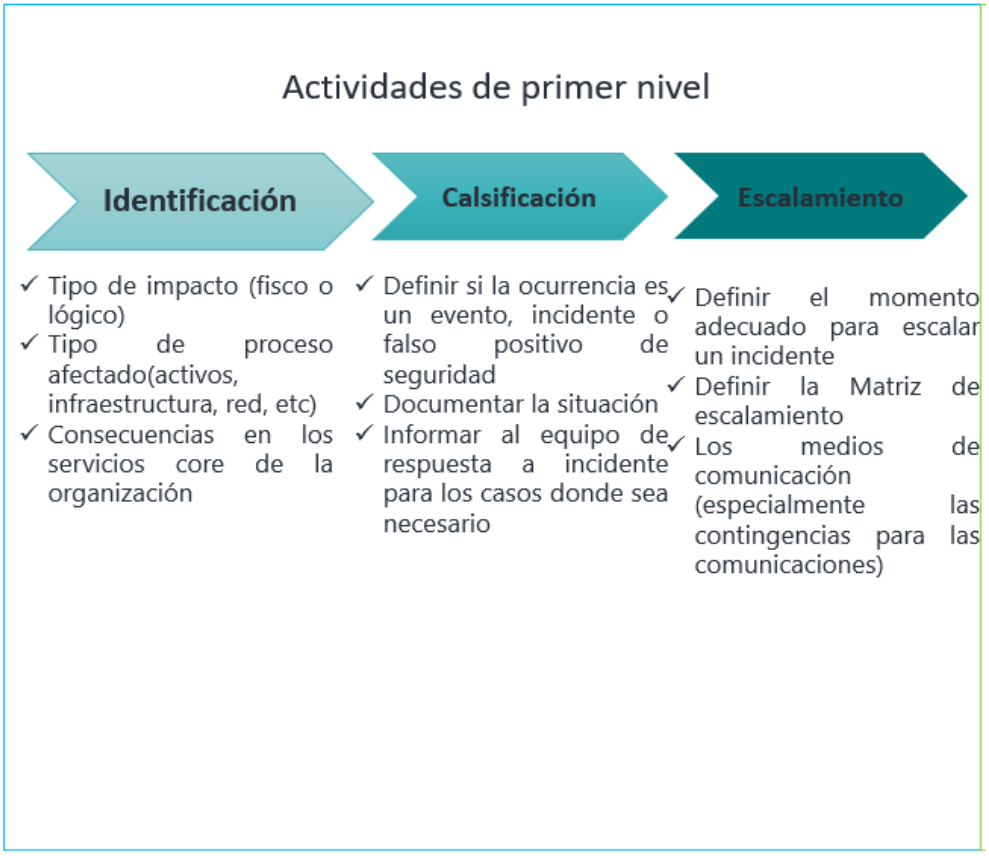
- ✓ **Responder** – Realizar actividades enfocadas en ejecutar las acciones necesarias para resolver un incidente de seguridad cibernética, esta función se vincula con el numeral 7 fase de evaluación y decisión de la norma ISO27035 la cual tiene como objeto definir si la situación hace parte de un incidente de seguridad, realizar la clasificación y los escalamientos necesarios

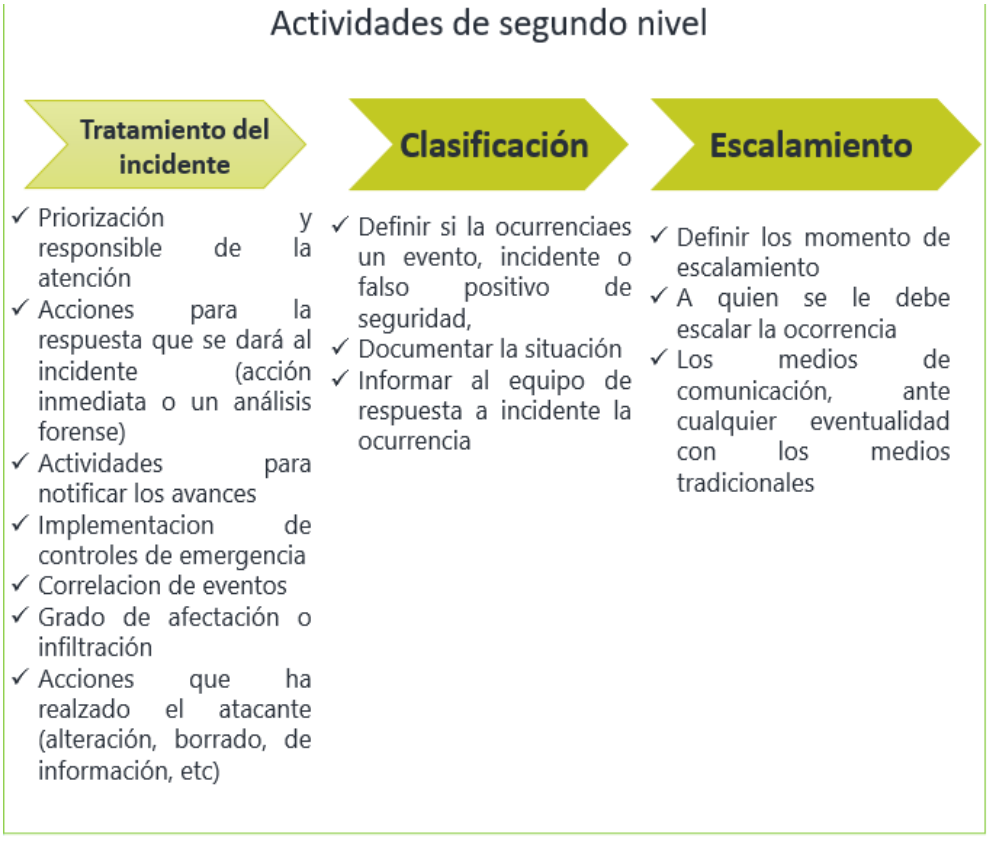
  Previamente la organización debe definir los siguientes componentes, los cuales son necesarios para ejecutar la función ***responder***, al momento de manejar un incidente de ciberseguridad.

  - Punto único de contacto
  - Escala de clasificación de eventos/ incidentes de la seguridad de la información anexo C
  - Escala de gravedad de eventos/ incidentes de la seguridad de la información
  - ISIRT (Information Security Incident Response Team) o equipo de respuesta a incidentes de seguridad de la información
  - Mesa de crisis

  De acuerdo a los lineamientos de la norma ISO27035 se definen 2 niveles para realizar el tratamiento de la situación (ilustración 3-9).

Ilustración 3-6 Niveles por Actividad





El primer nivel de escalamiento se encarga de valorar y determinar si el evento es un incidente de seguridad que se encuentra en curso o ya fue materializado, además debe establecer si se trata de una falsa alarma o fijar de acuerdo a los niveles de clasificación de eventos/incidentes el posible impacto.

Con el procedimiento de la escala de gravedad del incidente se toman las acciones para determinar en qué momento se trasladan las situaciones y a que personas se deben informar, es necesario instaurar prioridades para ordenar las respuestas que se van a dar a los incidentes de seguridad de la información (para más detalle ver los Anexos C y D).

El segundo nivel se encarga de tomar las acciones que sean necesarias para determinar y tratar el incidente de seguridad.

Además, se debe precisar una estrategia para la documentación del incidente, todas las actividades deben quedar documentadas para cualquier análisis posterior que se requiera. La estrategia debe incluir la definición de procesos asociados a:

1) Control de cambios debido al incidente.
2) know-how de errores conocidos o actualización de las bases de datos de vulnerabilidades.
3) Para el rastreo de incidentes, definir las actividades que permitan la recolección de la evidencia y el almacenamiento de la misma, es necesario precisar las actividades que permitan una preservación segura de la evidencia para las acciones posteriores de un incidente de seguridad. Es importante indicar como se archivó la evidencia y los detalles del almacenamiento/custodia segura del material y del acceso posterior a él.
4) Definir procedimientos que deben seguir los equipos, estos incluyen la revisión y recolección del reporte, evaluación de los daños, correlación de los daños, además incluyen la notificación al personal encargado del activo. En cada procedimiento se debe indicar en relación a la gravedad del incidente
5) La documentación debe incluir qué se observó y qué se hizo (incluyendo las herramientas usadas) y por qué; la ubicación de la evidencia potencial; cómo se llevó a cabo la verificación de la evidencia (si es aplicable), en qué consiste el incidente de seguridad de la información, cómo fue causado, y qué o quién lo causó, a qué afecta o podría afectar, el impacto real o potencial del incidente de seguridad de la información en el negocio de la organización, una indicación en cuanto si el incidente de seguridad de la información se considera significativo o no (usando la escala de clasificación predeterminada de la organización), y cómo

se ha tratado hasta el momento, como se ha tratado el incidente en cada momento y por quien.

6) Lecciones aprendidas (por ejemplo, los controles que se van a adoptar para impedir nuevas ocurrencias u ocurrencias similares)

Es necesario además incluir la identificación de las posibles consecuencias que tendrá el incidente de seguridad sobre la organización y que pilares fueron impactados por el incidente, ejemplo disponibilidad, confidencial, no repudio, o integridad, de acuerdo a ellos considerara las verdaderas consecuencias sobre el negocio

1) Gastos financieros
2) complicación en las operaciones
3) utilidades económicas
4) información personal
5) implicaciones legales
6) implicaciones reputacionales

- ✓ **Recuperar** – realizar actividades enfocadas en conservar los planes de resiliencia y reestablecer cualquier capacidad o servicio que se haya visto afectado debido a un incidente de seguridad cibernética.

Previamente la organización debe definir los siguientes componentes

Plan de continuidad o planes de contingencia en su defecto.

Plan de gestión de crisis

El objetivo principal de esta función es desarrollar las actividades necesarias para devolver las operaciones, aplicaciones o procesos a su estado habitual, además se deben ejecutar acciones que permitan la trazabilidad del incidente, determinar cómo se va comunicar a las partes interesadas la situación que se pueda estar presentando y establecer los métodos para disparar un plan de continuidad o crisis según sea la situación.

Se debe establecer un paso de valoración por parte del equipo de respuesta a incidente, para definir el estado del incidente (ilustración 3-10)

Ilustración 3-7 Pasos para la valoración

Así mismo, es necesario definir las responsabilidades de los miembros del equipo de acuerdo al incidente de seguridad, esto contiene los procedimientos documentados incluida la revisión y corrección de reportes, la reevaluación de daños y la notificación al personal pertinente, se deben determinar las actividad para dar inicio al análisis forense de seguridad de la información las actividad para informar a los responsables de las comunicaciones internas y externas acerca de los hechos y propuestas que se deberían comunicar, en qué forma y a quién.

En la función ***recuperar*** se requiere tener en cuenta las siguientes consideraciones

a) En los casos donde la situación se sale de control es necesario promover a una mesa de crisis o identificar la activación de los planes de continuidad, aquí se debe definir cuándo es necesario escalar los asuntos, y a quién llevarlos.
   Los planes de crisis definen las prioridades de las unidades de negocio y los tiempos de recuperación teniendo en cuenta los tiempos mínimos aceptables de las interrupciones de los servicios. Estas tácticas se enfocan en las medidas requeridas de gestión de crisis, resiliencia y acciones preventivas, la definición de responsabilidades para la respuesta ante una situación de esta dimensión y el contenido con los pasos que se deben

seguir ante la gestión de crisis, los controles que apoyan el inicio de los planes.

b) En las situaciones que se encuentre fuera de control y existan riesgos con impactos inadmisibles para el negocio, es necesario activar los planes de continuidad de negocio.
c) Definir las actividades para realizar los análisis forenses que sean necesarios, asegurar que se recolecta evidencia electrónica y se almacena en forma segura, de manera comprobable, y que se hace seguimiento continuo de su preservación segura. todos los datos volátiles se deberían recolectar antes de apagar el sistema, La información por recolectar incluye los contenidos de memoria, cache y registros, y detalle de cualquier acción que se esté realizando, se debería elaborar un duplicado forense completo de seguridad de la información del sistema afectado, o un archivo de respaldo de bajo nivel de registros y archivos importantes, dependiendo de la naturaleza del incidente de seguridad de la información, se deben recolectar y revisar los registros de los sistemas, servicios y redes vecinas, toda la información recolectada se debería almacenar en forma segura en modo de lectura solamente, mientras se lleva a cabo la duplicación forense de seguridad de la información es conveniente que haya al menos dos personas que afirmen y certifiquen que todas las actividades se han llevado a cabo, de acuerdo con la legislación y la reglamentación pertinente, las especificaciones y descripciones de las herramientas y comandos usados para llevar a cabo la duplicación forense de seguridad de la información se deberían documentar y almacenar junto con los medios originales.
d) Se debe identificar si la situación puede ser resuelta con personal interno o es necesario convocar personal externo
e) Definir los procesos de documentación del incidente incluyendo la documentación de la base de datos de errores conocidos, esta contiene, en qué consiste el incidente de seguridad de la información, cómo fue causado, y qué o quién lo causó, que afecta o podría afectar, el impacto real o potencial del incidente en el negocio de la organización, cambios en la indicación de si el incidente de seguridad de la información se considera significativo o no (usando la escala predeterminada de clasificación de severidad de la organización), y cómo se ha tratado hasta el momento. Aquí se deben definir las actividades necesarias que garanticen la retención, confidencialidad, disponibilidad e integridad de las pruebas detectadas. La información sé que documente debe tener los registros de cada proceso.
f) Definir los procesos necesarios para la implementación de cambios en los sistemas. Esto podría incluir apagar el sistema, o aislar la parte afectada, apagarla mientras se implementan los controles adecuados. Sin embargo, para los casos donde el incidente se genera por una vulnerabilidad que es necesaria el diseño del sistema, es necesario evaluar los impactos antes de realizar los cambios y analizar alternativas para restablecer los sistemas.

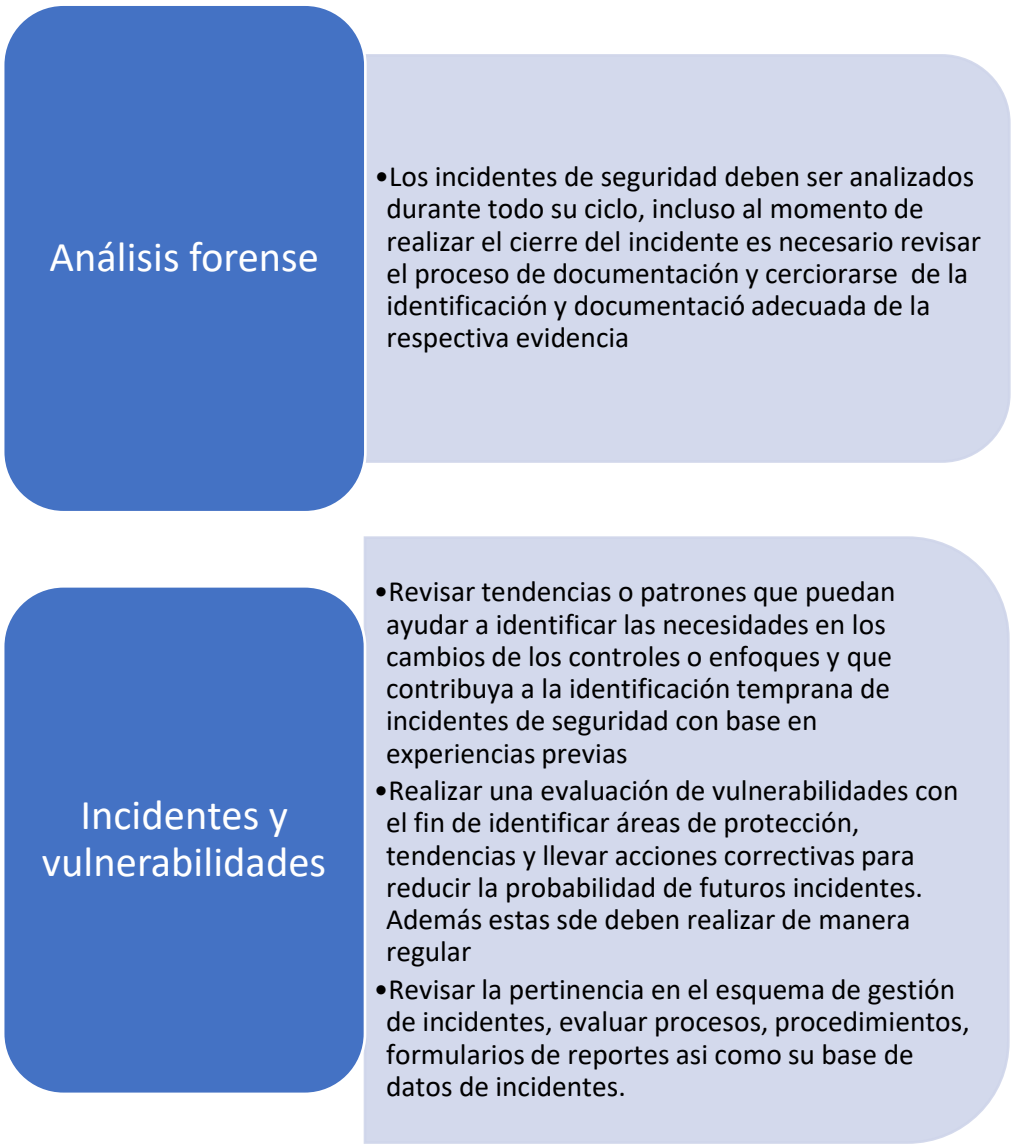
g) Definir el proceso para realizar la comunicación a las partes (lideres, medios, etc.) que sea necesario, según el nivel de criticidad del incidente. Este proceso debe definir los momentos en que se realizan comunicaciones, cuando un incidente tiene impactos catastróficos se pueden dar varios puntos de comunicación (informar el inicio del incidente, cuando se encuentre bajo control, momentos de escalamiento y los respectivos cierres incluyendo las consecuencias), esto debe ir alienado de acuerdo a las partes a comunicar que se va informar. La comunicación se podrá segmentar según el público (tipo de incidente impacto) y antes de ser comunicada debe ser revisada por la alta dirección, coordinadores de relaciones públicas y seguridad de la información

El desarrollo de estas actividades permite responder a los incidentes de seguridad para restringir los impactos que se presentan. Sin embargo, es necesario considerar que mientras estas actividades se despliegan, el atacante puede tomar acciones que causen más daños o realizar movimientos que complican la evidencia del rastro de su intrusión.

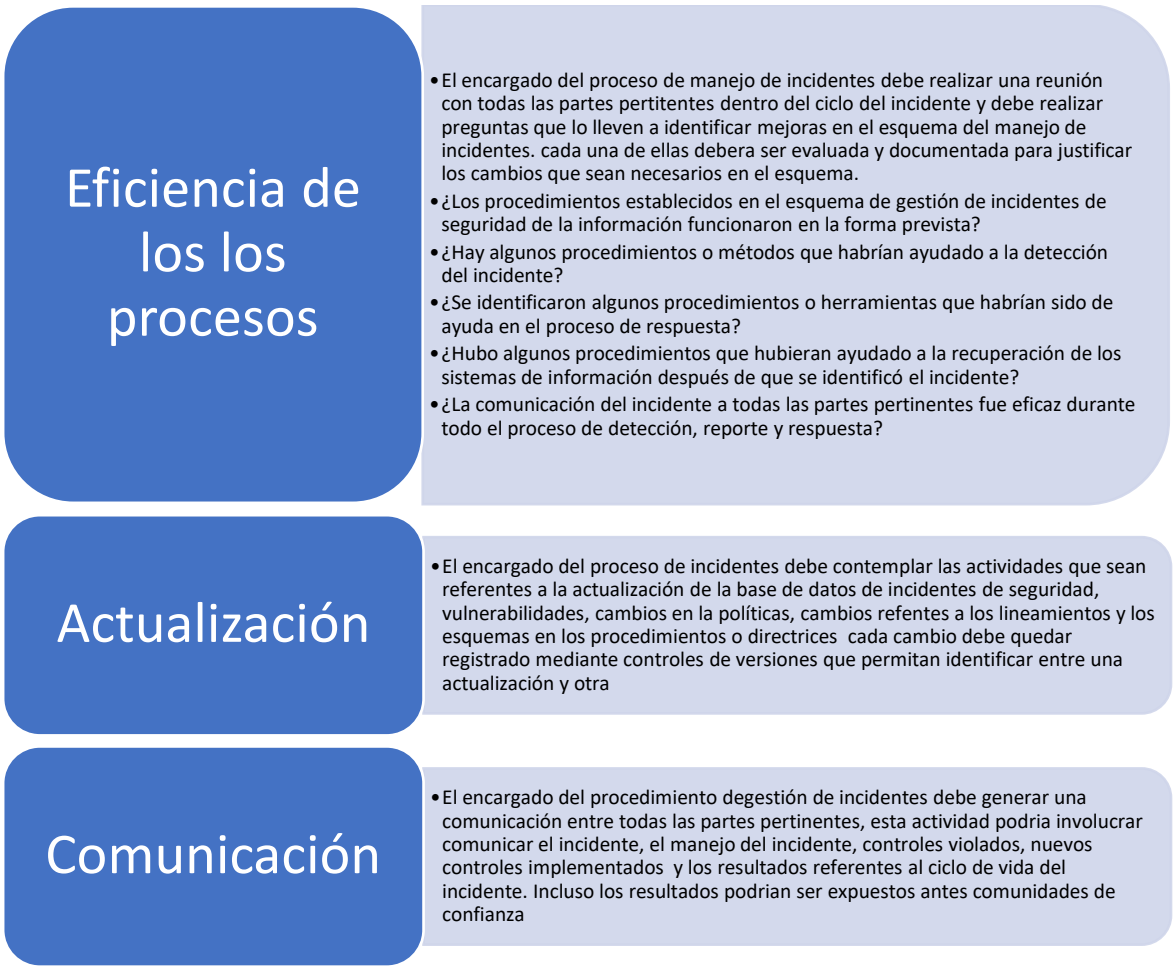
- ✓ **Actividades de mejora**, se contemplan estas actividades para incluir un proceso que asegure un aprendizaje de los incidentes que se hayan materializado, esto incluye el manejo de los pasos para la solución del incidente y como fueron tratados.

  A continuación, se listan cada una de las actividades que se deben analizar dentro del proceso de mejora continua que están en la fase de lecciones aprendidas (ilustración 3-11).

Ilustración 3-8 Actividades lecciones aprendidas



Identificación y mejoras en la implementación de controles	•identificar controles nuevos o modificaciones a éstos, según se requieran en caso que no sea viable financiera ni operativamente implementarlos de inmediato, se deberían incluir en los objetivos de la organización a un plazo más largo. •la implementación de controles pueden ser actualizaciones o nuevos controles y podrian varias entre controles técnicos, actualizciones rápidas de los materiales, la entrega de nuevas instrucciones de toma de conciencia sobre seguridad, publicaciones de directrices y/o normas
Identificación y mejoras a los resultados de la revisión por la Dirección y de la evaluación de riesgos de seguridad de la Información.	•De acuerdo al impacto y severidad del incidente es necesario realizar una nueva evaluación de riesgos de seguridad que permita tener en cuenta nuevas amenazas y vulnerabilidades, incluso determinar en equipo con la alta dirección la inversión de nuevos controles o simplemente cambios sobre los controles actuales, esto en línea con la actividad del punto anterior



3.3.2 Actividad 2: Determinar y ejecutar una estrategia que permita la evaluación del objetivo, considerando un caso de estudio en una empresa que ofrece servicios tercerizados de TI, esto se hará a través de entrevistas, encuestas y/o check-list de validación de cumplimiento con el personal de la empresa seleccionada.

De acuerdo a la estrategia definida tal como se indicó en la Ilustración 3 Estrategia para la evaluación del modelo de ciberseguridad, se presentan los siguientes resultados para cada uno de los pasos definidos.

a) Grupo focalizado:

A continuación, se presenta el perfil demográfico de las personas que conformaron el grupo focalizado.

El 100% de los encuestados indicaron que su experiencia laboral ha estado enfocada en el sector privado, además cada uno indicó que actualmente labora en empresas de servicios informáticos donde sus roles han estado relacionados con servicios de

seguridad informática, en promedio el 100% informó que cuentan con más de tres años de experiencia desarrollando actividades relacionadas con seguridad asociada a la solución de un incidentes y eventos de seguridad.

A la pregunta ¿Dentro de su experiencia ha desarrollado algún rol para manejar un incidente de seguridad relacionado con Ransomware? El 100% de los encuestados informó que ha participado activamente en la resolución y recuperación de los eventos de seguridad asociados a este tipo de situaciones.

Lo que nos permite determinar que el grupo focalizado se encuentra con la competencia necesaria para la evaluación del modelo de ciberseguridad desarrollado, lo cual permite una estimación eficiente del desde el punto de vista competente; su conocimiento ha sido adquirido basándose en vivencias dentro del área de seguridad y debido a que se encuentran con más de tres años de experiencia, se puede determinar que las decisiones que toman al momento de enfrentar las diversas situaciones en el sector son abordadas desde las lecciones aprendidas, experiencias e incluso documentación que han recolecta a través de la experiencia de las personas que hacen parte del grupo focalizado. El nivel de preparación del equipo experto permite entonces determinar si verdaderamente el modelo es aplicable y como valor agregado están en la facultad de informar qué debe desarrollarse adicional para mejorar el modelo y cumplir con una correcta preparación, que permita la prevención de los incidentes de ciberseguridad para empresas del sector informático.

b) Evaluación del modelo:

De acuerdo a la metodología planteada, el 100% de las personas que hicieron parte del grupo focalizado consideraron que al materializarse los escenarios de riesgos inadmisibles descritos en el Anexo A (Mapa de Riesgos), era posible reducir los niveles de exposición, además indicaron que el modelo de ciberseguridad planteado considera que se implementaron estrategias que permiten anticiparnos a la materialización de un evento; así mismo, el grupo focalizado calificó el modelo de ciberseguridad en las funciones proteger y detectar (ver Ilustración 3-3 Modelo de ciberseguridad) como estrategias viables que permiten la reducción de los niveles de exposición de los riesgos informados bajo el desarrollo de los resultados del objetivo 1, (ver Anexo A: Mapa de Riesgos), al mismo tiempo consideraron que en el modelo se implementaron estrategias adecuadas en la función recuperar (ver Ilustración 3-3 Modelo de ciberseguridad) para reducir los tiempos de indisponibilidad de los activos en los que se materializaran los escenarios de riesgos, en ese mismo sentido, el 100% de los encuestados considero que las políticas definidas dentro del modelo crearon valor al momento de reducir los niveles de exposición de los escenarios de riesgos identificados y descritos bajo los resultados del objetivo 1; conjuntamente informaron que se definió una estrategia adecuada en la función acciones de mejora orientada en el aprendizaje y por ende la implementación de actividades que permitieran no repetir los escenarios de riesgo que se pueden materializar y generar inconvenientes dentro de las organizaciones del sector.

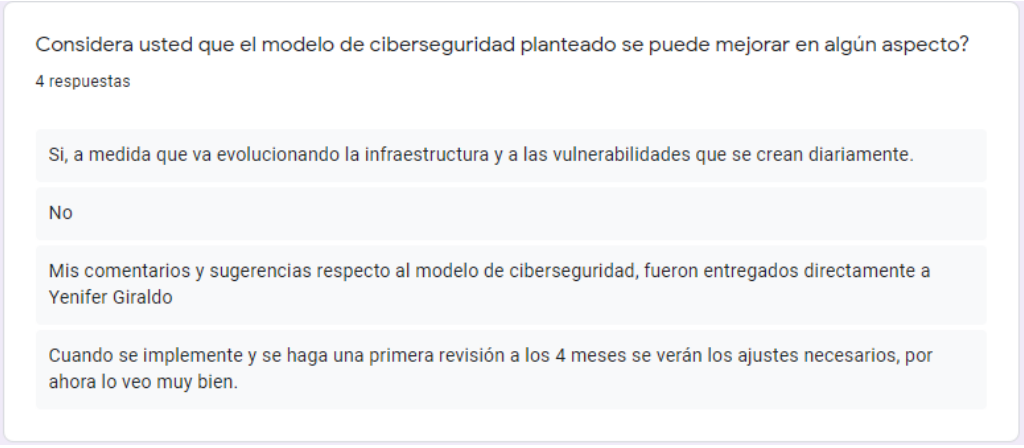
Al analizar específicamente uno de los riesgos detectados como inaceptables (Posibilidad que la amenaza: crakeo de contraseñas, afecte activos como correo/medios de almacenamiento, teléfonos móviles), el grupo focalizado indico que al aplicar el plan de remediación definido dentro del Anexo A (Mapa de Riesgos) es posible reducir el nivel de exposición.

De la misma forma el grupo focalizado al evaluar el modelo de ciberseguridad consideró que este se puede mejorar en aspectos como:

- ✓ La creación de estrategias que permitan una evaluación de riesgos recurrente, es decir, incluir en el modelo una metodología que permita evaluar periódicamente e identificar vulnerabilidades que se crean regularmente debido a la evolución de la infraestructura.
- ✓ Dentro de las funciones referenciadas en el modelo, específicamente en la función DETECTAR se recomienda incluir la integración con herramientas tipo SIEM para la correlación de eventos.
- ✓ Dentro de las funciones referenciadas en el modelo, específicamente en la función RESPONDER del framework, se propone tener en cuenta soluciones o configuración de soluciones tipo SOAR, para llevar a cabo la ejecución de respuestas automáticas que puedan ser configuradas.
- ✓ El modelo debe incluir un paso que permita evaluar y percibir en retrospectiva ajustes, por lo cual, se recomienda incluir actividades definidas dentro de los marcos agiles.

Mejoras que fueron descritas en la encuesta a la pregunta, ¿Considera usted que el modelo de ciberseguridad planteado se puede mejorar en algún aspecto?, tal como se muestra en la ilustración 3 12 Grupo focalizado

Ilustración 3-9 Encuesta Grupo Focalizado



Dado lo anterior, se puede concluir que el modelo de ciberseguridad construido para empresas específicamente de servicios informáticos, si se da la ejecución y despliegue permite fortalecer un adecuado manejo de incidentes de seguridad, esto según las respuestas informadas en la evaluación del modelo que estuvo enfocado en valorar cada

una de las acciones construidas y es aplicable a organizaciones que ofrecen servicios como mensajería electrónica (Outlook, Teams), sistemas middleware, soporte de sistemas como bases de datos, servicios de despliegues, manejo y uso de comunicaciones unificadas enfocadas en los servicios de video conferencias y todo lo relacionado al ciclo de vida de productos como el almacenamiento, virtualización, y sistemas en cloud, dado que fue evaluado en un caso de estudio donde se incluyeron los activos que se requieren para prestar los servicios descritos anteriormente.

4. Conclusiones y recomendaciones

4.1 Conclusiones

Un modelo de ciberseguridad basado en la gestión de riesgos y en un plan para el manejo de incidentes de seguridad es fundamental en las organizaciones que ofrecen servicios informáticos, esto, por un lado, le permite dar mejores características de seguridad en el producto y servicio, además establece una ruta de gestión sobre los activos críticos a proteger ante eventos de ciberseguridad.

A través de la ejecución de este proyecto, se ha logrado el objetivo específico de establecer los diferentes riesgos de ciberseguridad en empresas que ofrecen servicios informáticos, en consecuencia se contribuye en la construcción del modelo de ciberseguridad para empresas del sector, esto favorece positivamente ya que las evaluaciones de los riesgos tienen más sentido de acuerdo a la recurrencia con la que se realicen; los ataques de día cero evolucionan constantemente y contar con modelos de riesgos que implementen nuevas tecnologías converge a un sistema de riesgos actualizado y con una alta mitigación de riesgos, creando sistemas eficaces, eficientes y efectivos.

La identificación de los riesgos caracterizados se logró a través del modelamiento de los servicios que se prestan en estas empresas partiendo de los activos, además fue posible determinar cuál era el nivel de impacto en caso de afectación de un activo clasificado como privado en el numeral 3.1 se puede observar el detalle, lo cual supone un conocimiento transversal de las organizaciones que permite tomar decisiones acertadas acerca del tratamiento de este.

Fue posible caracterizar los escenarios de riesgos detallando los agentes generadores y cuáles serían esas consecuencias ver anexo A, con esta información las organizaciones podrían crear políticas que supongan estar un paso adelante del atacante y mitigar riesgos desde esta perspectiva cubriendo más frentes de ataques, finalmente se calificaron los escenarios de riesgo en términos de impactos los cuales permitieron determinar una matriz de riesgos con menos riesgos altos que bajos.

Así mismo se determinó el procedimiento para un adecuado manejo de incidentes de seguridad basado en normas internacionales alineando la norma para el manejo de incidentes ISO27035 y el marco NIST de ciberseguridad, ambas poseen características relevantes que permiten asociarse a los riesgos detectados y la aplicabilidad en empresas de servicios informáticos.

En consecuencia, se construye un modelo de ciberseguridad que parte de los riegos detectados e integra las definiciones de cada una de las normas seleccionadas para el manejo de incidentes de ciberseguridad, así mismo, la validación del modelo con un grupo objetivo que hace parte del sector de los servicios informáticos fue muy positiva y con ello, se da por cumplido el objetivo general.

4.2 Trabajo futuro

El éxito de una gestión de riesgos parte de un buen manejo de la identificación de los activos, para ello se recomienda entender la norma que se seguirá y acoplar los procesos de manera secuencial y congruente, sin embargo, es conveniente que cada organización realice su proceso de gestión de riesgos modelado a los activos propios de su organización y a sus capacidades, esto evitara sobre costos en la implementación de controles para la mitigación de los riesgos.

Como trabajo futuro se debe analizar la creación de estrategias que permitan una evaluación de riesgos recurrente, es decir, construir una metodología que permita evaluar periódicamente e identificar vulnerabilidades que se crean regularmente debido a la evolución de la infraestructura, y contemplar dentro del proceso de riesgos la identificación asociados a los ataques de día cero sobre las infraestructuras alojadas en la nube, articulando controles enfocados en la protección de datos personales, donde podrían contemplarse la aplicación de normas como la ISO27701; esto debido a que hoy con la hiper conectividad de los datos que han logrado las organizaciones se ha visto potencialmente afectada la protección de la privacidad de la información debido al tratamiento que se realiza por todas las partes que la procesan (titular, responsable, encargado y tercero); su creación debería estar articulada con los procedimientos asociados que permitan la implementación de la misma, alineada con normas como la ISO 27032:2012 "Tecnologías de la información - Técnicas de seguridad - Directrices para la Ciberseguridad" orientada a intentar garantizar un entorno seguro a través de directrices de seguridad.

Por otro lado, se propone que este modelo de ciberseguridad pueda ser validado e implementado si es del caso, en otro tipo de organizaciones o establecer un mecanismo para que sea homologado a servicios en la nube (o nube híbrida), con ello, poder explotar mejor las bondades en diferentes organizaciones.

Finalmente, se podría ampliar el alcance del modelo no solo a servicios de clientes, también hacia los servicios internos de la compañía, con ello, se podría fortalecer la cadena de valor, logrando una mejora en los resultados en los temas de ciberseguridad.

5. Anexos

5.1 Anexo A: Mapa de Riesgos

5.2 Anexo B: Anexo Políticas

5.3 Anexo C: ISO/IEC 27035:2011- Annex C

5.4 Anexo D: ISO/IEC 27035:2011(E)- Annex D

6. Bibliografía

[1] ACIS, “Ciberriesgos - Un riesgo sistémico,” Sistemas, no. 148, pp. 12–41, 2019.

[2] KASPERSKY, (2019, Ago. 28) ¨Kaspersky registra 45 ataques por segundo en América Latina¨ Disponible https://latam.kaspersky.com/blog/kaspersky-registra-45-ataques-por-segundo-en-america-latina/15274/

[3] UIT, “Decisiones destacadas de Guadalajara Ciberseguridad,” Actual. la UIT, vol. Nov, no. 9, p. 22, 2010.

[4] IAIS, “Issues Paper on Cyber Risk to the Insurance Sector,” Int. Assoc. Insur. Superv., vol. Ag, p. 38, 2016.

[5] MINTIC, “Modelo de Seguridad y Privacidad de la Información Modelo,” Model. Segur. y Privacidad la Inf., vol. Julio, 2016.

[6] MINTIC - GCISI, “Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información,” no. 21. p. 29, 2014.

[7] IEC 31010, Risk management — Risk assessment techniques

[8] r. Delvasto ramírez, “modelo de gestión de incidentes de seguridad de la información para pymes ramiro,” no. June, 2016.

[9] NIST, “Computer Security Incident Handling Guide Recommendations of the National Institute of Standards and Technology,” vol. Special Pu, no. Revision 2, 2012.

[10] A. M. Rea-Guaman, I. D. Sanchez-Garcia, T. S. Feliu, and J. A. Calvo-Manzano, “Modelos de Madurez en Ciberseguridad: una revisión sistemática,” Iber. Conf. Inf. Syst. Technol. Cist., 2017.

[11] ISACA “Comprendiendo la Ciberseguridad a través de un marco de mejores prácticas Temas a tratar” 2017

[12] Sabillon, Regner, et al. "A comprehensive cybersecurity audit model to improve cybersecurity assurance: The cybersecurity audit model (CSAM)." 2017 International Conference on Information Systems and Computer Science (INCISCOS).

[13] Rathod, Paresh, and Timo Hämäläinen. "A novel model for cybersecurity economics and analysis." 2017 IEEE International Conference on Computer and Information Technology (CIT).

[14] R. Paredes, “Diseño y dimensionamiento de un equipo de un equipo de respuesta ante incidentes de seguridad informática (CSIRT),” vol. 84, pp. 487–492, 2013.

[15] Chicano, “Procedimiento para la seguridad de la información”, 2014

[16] j. E. G. Díaz, “guía de gestión de incidentes de seguridad de la información para la oficina de tecnología de la información y la comunicación – otic del miNISTerio de salud y protección social, tomando como base la norma iso 27001:2013,” no. June, 2016.

[17] ISO, “Estandar Internacional Iso / Iec 27005,” vol. 2018, pp. 1–170, 2005.

[18] H. F. Vargas Montoya, “Propuesta para la planeación e emplementación de un SGSI basado en la ISO/IEC 27001:2005 para una empresa de telecomunicaciones,” 2014.

[19] Alcaldía Mayor de Bogotá, “Instructivo para la Elaboración de la Matriz de Riesgos,” p. 21, 2014.

[20] Deloitte, “Las preocupaciones del CISO El estado de la ciberseguridad en el 2019” p.15, 2019

[21] ISO/IEC , “Information technology — Security techniques — Information security incident management,” 27035, First Edition 2012-mm-dd

[22] Microsoft “¿Qué es middleware?” .[En línea]. Disponible en: https://azure.microsoft.com/es-es/overview/what-is-middleware/ [Accedido: 27-abril-2021]

[23] Barrios, A, “el comunicador en el entorno digital”, cuadernos.info nº 34 / junio 2014 / issn 0719-3661 / versión electrónica: www.cuadernos.info / issn 0719-367x

[24] Instituto Nacional de Estándares y Tecnología, “Marco para la mejora de la seguridad cibernética en infraestructuras críticas” Versión 1.1; 2016

[25] ISACA, “Success Story: ISACA”. [En línea]. Disponible en https://www.NIST.gov/cyberframework/success-stories/isaca [Accedido: 05-abril-2020]