METODOLOGÍA PARA GESTIONAR RIESGOS Y MEJORAR LOS NIVELES DE ATENCIÓN DE EVENTOS O INCIDENTES INFORMÁTICOS DE LAS MESAS DE SERVICIOS TI EN LAS ORGANIZACIONES

YENNY SERRANO SAENZ

Proyecto de Grado – monografía como alternativa de trabajo de grado
Para optar por el título de
ESPECIALISTA EN SEGURIDAD INFORMÁTICA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA “UNAD”
ESCUELA DE CIENCIAS BASICAS TECNOLOGIA E INGENIERÍA ECBTI
ESPECIALIZACION EN SEGURIDAD INFORMATICA
BOGOTÁ-CUNDINAMARCA
JUNIO
2023

METODOLOGÍA PARA GESTIONAR RIESGOS Y MEJORAR LOS NIVELES DE ATENCIÓN DE EVENTOS O INCIDENTES INFORMÁTICOS DE LAS MESAS DE SERVICIOS TI EN LAS ORGANIZACIONES

YENNY SERRANO SAENZ

Proyecto de Grado – monografía como alternativa de trabajo de grado
Para optar por el título de
ESPECIALISTA EN SEGURIDAD INFORMÁTICA

Ing. Edgar Dulce
Director

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA “UNAD”
ESCUELA DE CIENCIAS BASICAS TECNOLOGIA E INGENIERÍA ECBTI
ESPECIALIZACION EN SEGURIDAD INFORMATICA
BOGOTÁ-CUNDINAMARCA
JUNIO
2023

NOTA DE ACEPTACIÓN

Firma del presidente de Jurado

Firma del Jurado

Firma del Jurado

Bogotá-junio de 2023

DEDICATORIA

Con amor dedico este trabajo a mi hijo, que con su carisma y comprensión me acompañó en cada etapa vivida, colaborándome de manera indirecta, minimizando mis preocupaciones de madre, también lo dedico a mi mamá que con su apoyo, consagración y paciencia disminuyo mis tareas en el hogar permitiéndome una entrega más tranquila en el estudio y trabajo.

Yenny Serrano Saenz

AGRADECIMIENTOS

Agradezco a las directivas de la Universidad Nacional Abierta y a Distancia UNAD, quienes con su trabajo continuo nos brindan la oportunidad de estudiar y laborar, por otro lado, a cada uno de los tutores y asesores que me acompañaron en el proceso les reconozco que sin su apoyo y colaboración éste logro no hubiera sido posible.

CONTENIDO

Pág.

LISTA DE TABLAS

Pág.

LISTA DE FIGURAS

Pág.

GLOSARIO

Activos: Se tratan del software, hardware y cualquiera pieza física propiedad de la compañía.[1]

Gestión eventos: Observa los servicios y sus componentes, estableciendo una respuesta adecuada a cualquier cambio de estado que tenga relevancia la gestión de servicios[2].

Gestión Incidentes: Interrupción de servicios de TI, que afecta la continuidad del negocio[3].

Hardware: Son componentes físicos de un dispositivos o equipo de cómputo, que se pueden ver y tocar.

ITIL: Es una guía de buenas prácticas para servicios de tecnología de la información (TI), abarcando la infraestructura, desarrollo y operaciones, orientado a la mejora de la calidad del servicio.[4]

---

[1]

[2] SALVARENGA. (s.f.). *"La Gestión De Eventos Y Su Relación Con Otras Practicas De ITIL". {En linea}[https://blog.agrega.com/][Sitio Web]gestión de eventos[consulta 21 diciembre 2020].* Obtenido de https://blog.agrega.com/itsm/la-gestion-de-eventos-y-su-relacion-con-otras-practicas-de-itil/#:~:text=El%20prop%C3%B3sito%20de%20la%20gesti%C3%B3n,en%20la%20gesti%C3%B3n%20de%20servicios.

[3] MANAGEENGINE. (s.f.). *"¿Qué es la Gestión de Incidentes T": "La gestión de incidentes de TI es uno de los procesos fundamentales de la mesa de ayuda" I[En linea] {23mayo 2022} disponible en: .* Obtenido de https://www.manageengine.com/latam/service-desk/itil-incident-management/que-es-la-gestion-de-incidentes-itil.html

[4] *GlobalSuite (s.f) ¿Qué es ITIL? [https://www.globalsuitesolutions.com/ [Sitio web][consulta 08 de agosto de 2022]. Obtenido de https://www.globalsuitesolutions.com/es/que-es-itil-y-para-que-sirve/* . (s.f.).

Mesa de ayuda: Punto único de contacto que resuelve en forma oportuna los requerimientos que puedan tener los distintos tipos de usuarios de la empresa antes incidentes, consultas y peticiones de servicios de TI[5].

TIC sigla para 'tecnologías de la información y las comunicaciones' Mesa de ayuda, según el sitio especializado TechTarget, también se constituye en un término sombrilla que permite agrupar a los dispositivos, aparatos, métodos electrónicos y aplicaciones que ayudan a que la sociedad se comunique o acceda a los datos que requieren para sus actividades diarias[6].

Phishing: Son los métodos que utilizan los delincuentes cibernéticos para obtener información confidencial y realizar estafas, la técnica más utilizada es la "ingeniería social".[7]

Riesgos informáticos: un proceso que comprende la identificación de activos informáticos, sus vulnerabilidades y amenazas a los que se encuentran expuestos, fin de determinar los controles adecuados para aceptar, disminuir, transcurrir o evitar la ocurrencia del riesgo[8].

---

[5] SONDA S.A. . (s.f.). *SOPORTE DE INFRAESTRUCTURA SERVICEDESK. [en línea] El Servicedesk de SONDA opera como un único punto de contacto que resuelve de forma oportuna incidentes de servicios de TI[consulta: 2021] Disponible en: .* Obtenido de https://www.sonda.com/content/uploads/2018/12/ServiceDesk.pdf

[6] MINTIC. (s.f.). *¿Qué son las TIC?[https://www.enticconfio.gov.co/que-son-las-tic-significado] son todas las tecnologías que permiten acceder, producir, guardar, presentar y transferir información [Consulta: 17 de mayo de 2017]*. Obtenido de https://www.enticconfio.gov.co/que-son-las-tic-significado

[7] *MARCELO, Rivero (s.f) El ransomware es una forma de malware que está en auge[https://es.malwarebytes.com/][Sitio web][Consulta 07 agosto]. Obtenido https://es.malwarebytes.com/ransomware/*.

[8] FLORENCIA, L, & PAYERO, A. (s.f.). *Riesgos Informaticos [https://sites.google.com/] identificación de activos informáticos,sus vulnerabilidades y amenazas a los que se encuentran expuestos [Consulta: septiembre de 2016]*. Obtenido de https://sites.google.com/site/tecnologiadigital20/home/riesgos-informaticos

Ramsanware: Es un Malware que impide a los usuarios ingresar a su sistema (de varias formas) o documentos personales, exigiendo pago el rescate de dicha información; el método más habitual es a través de spam malicioso por medio de correo electrónico.[9]

SOC: (Security operation Center), corresponde a los centros de operaciones de Seguridad, encargado de monitorear, realizar seguimiento y análisis de las actividades de las redes datos, servidores, bases de datos, sitios web, aplicaciones…identificando actividades anormales que puedan generar incidentes o situaciones de seguridad informática[10].

Software: Son programas informáticos, que permite la ejecución de tareas específicas en el equipo de cómputo.

---

[9] *MARCELO, Rivero (s.f) El ransomware es una forma de malware que está en auge[https://es.malwarebytes.com/][Sitio web][Consulta 07 agosto]. Obtenido https://es.malwarebytes.com/ransomware/*. (s.f.).

[10] NSIT SAS. (s.f.). *Qué es un SOC: Funciones y objetivos principales[https://www.nsit.com.co/][Sitio web]implementar servicios que puedan alertar sobre un ataque venidero e incluso minutos antes de que suceda[consulta 25 febrero]*. Obtenido de https://www.nsit.com.co/que-es-un-soc-funciones-y-objetivos-principales/

RESUMEN

Teniendo presente los riesgos de Ciberseguridad en la cual se encuentra expuestas las empresas tecnológicas, los delincuentes pueden realizar acciones ilegales principalmente a la unidad de Helpdesk (Mesa de Servicios TI), causando un grave perjuicio económico y reputación buscando sacar beneficios y es en ese momento en donde la unidad debe estar preparada para dar respuesta frente a estas amenazas, que pueden afectar su credibilidad con los diferentes clientes que tienen contrato como empresas Outsourcing, aseguradoras, bancos, azucareras, hospitales, constructoras, papelerías, droguerías, impresión…entre otros; que confían plenamente en el servicio de atención para sus usuarios sin que sea vulnerada su información.

Dentro de este documento se propone cómo debería ser la organización de un grupo especializado y a su vez algunas recomendaciones para efectuar un monitoreo y análisis de actividades que se pueden presenten en la gestión de incidentes o eventos, donde se exponen a posibles riesgos y/o ataques que deben ser mitigados y controlados de forma oportuna y eficiente.

Por lo cual, es importante implementar un grupo especializado que estará responsable de realizar monitorización y análisis de las actividades que se estén ejecutando en los activos de la empresa y al contar un SOC permitirá detallar los datos relevantes de la red junto con la salvaguarda requerida para protección de los Activos por medio de diferentes metodologías, facilitando la gestión para identificación de las amenazas. (NSIT SAS, s.f.)

Palabras Claves: Ciberseguridad, Helpdesk, monitorización

ABSTRACT

Bearing in mind the Cybersecurity risks in which technology companies are exposed, criminals can carry out illegal actions mainly to the Helpdesk unit (IT Service Desk), causing serious economic damage and reputation seeking to obtain benefits and it is at that time where the unit must be prepared to respond to these threats, which can affect its credibility with the different clients that have contracts such as outsourcing companies, insurance companies, banks, sugar companies, hospitals, construction companies, stationery stores, drugstores, printing ... among others; that fully trust the customer service for their users without their information being compromised.

This document proposes how the organization of a specialized group should be and in turn some recommendations for monitoring and analyzing activities that may occur in the management of incidents or events, where they are exposed to possible risks and / or attacks. that must be mitigated and controlled in a timely and efficient manner.

Therefore, it is important to implement a specialized group that will be responsible for monitoring and analyzing the activities that are being carried out in the company's assets and, when having a SOC, detail the relevant data of the network along with the required safeguards for protection. of Assets through different methodologies, facilitating the management for the identification of threats.

Keywords: Cybersecurity, Helpdesk, monitoring

1 INTRODUCCIÓN

Los ataques informáticos en el mundo cada año dejan millones de dólares en perdida para todas las empresas, las cuales se ven afectadas y cada vez crece más ya que la seguridad de las empresas es baja teniendo en cuenta que las empresas invierten más en antivirus y no en otros tipos de seguridad que son importantes para el análisis contaste de las amenazas; es importante que todas las empresas apunten al desarrollo de un control de operaciones cibernéticas o contraten servicios de un tercero.

Actualmente las Mesas de Ayuda se encuentran expuestas a amenazas cibernéticas por los diferentes soportes que entregan a los usuarios tanto incidentes como requerimientos, realizando solicitudes de toma remota a sus equipos, desbloqueo de cuentas, cambios de contraseñas para ingreso a sus equipos, instalación de aplicativos y engaños relacionados con el Phishing[11].
Estos accesos nombrados anteriormente también se filtran los datos por medio de implementación de Active Directory (AD) insegura, como medio preferido por los atacantes, teniendo en cuenta que les facilita elevar privilegios, permitiendo al atacante realizar movimientos laterales al aprovechar fallas y configuraciones inadecuadas, sin que el especialista de seguridad puedan encontrar y solventar antes de que la afectación se convierta en un problema para el negocio sin contar con un control adecuado para mitigar estas vulnerabilidades[12].

---

[11] MALWAREBYTES LTD. (s.f.). *"Suplantación de identidad". {En linea}. (phishing)[es.malwarebytes.com]es un método para engañarle y hacer que comparta contraseñas[Consulta: 2021].* Obtenido de https://es.malwarebytes.com/phishing/

[12] TENABLE. (s.f.). *"Proteja su Active Directory e interrumpa las rutas de ataque" {En linea}. [es-la.tenable.com/]vulnerabilidades dentro de sus dominios de Active Directory[Consulta:2022].* Obtenido de https://es-la.tenable.com/products/tenable-ad?utm_campaign=gs-{16816557316}-{134801193745}-{591911499268}_00023798_fy22&utm_promoter=tenable-ad-nb-00023798&utm_source=google&utm_term=ataques%20de%20ciberseguridad&utm_medium=cpc&utm_geo=latam&gclid=EAIaIQo

2 DEFINICIÓN DEL PROBLEMA

2.1 ANTECEDENTES DEL PROBLEMA

Las mesas de servicios de TI, son un punto único de atención a usuarios de diferentes países (Colombia, Chile, Perú,, Argentina, Brasil, entre otros…), donde se atienden incidentes y requerimientos de las aplicaciones Core del negocio y por ende cuentan con una base de datos de cada uno de ellos, generado posibles riesgos, debido a que en la actualidad existen redes de atacantes y ciberdelincuente que vigilan y esperan el momento adecuado en que se produce una brecha de seguridad, para robar o secuestrar estos datos sensibles; buscando obtener acceso a los dispositivos de las organizaciones o cuentas empresariales, poniendo en peligro la estabilidad de los negocios.

Se pueden recibir diferentes tipos de ataques, como lo son ataques donde muchos computadores o dispositivos conectados a internet son vulnerados servidores DNS (Domain Name System)[13], evitando legitimidad de los usuarios por medio de la denegación del servicio y escaneo de puertos, desde donde Intentan engañar a los usuarios para que les suministre sus credenciales e información confidencial de su empresa o ingreso a su equipo para instalación de software malicioso de forma secreta; logrando control para obtener la información, los firewalls que son bloqueados por los paquetes ICMP (Internet Control Messaging Protocol)[14]establecer un canal de comunicación cifrado, creando un túnel encubierto entre dos computadoras remotas.

---

[13] TECNOLOGIA+INFORMATICA. (s.f.). *"¿Qué es el DNS?". El sistema de nombres de dominio, más comúnmente conocido por sus siglas en inglés como Domain Name System o DNS. {En linea}. {Junio 2021}*. Obtenido de https://www.tecnologia-informatica.com/que-es-dns/

[14] REDES LOCALES Y GLOBALES. (s.f.). *"Protocolo ICMP (Internet Control Messaging Protocol)". {En linea} [https://sites.google.com/site/redeslocalesyglobales] definido en el RFC 792, sirve para informar de sucesos que han ocurrido en la red [Disponible en: 27 de mayo de 2015]*. Obtenido de https://sites.google.com/site/redeslocalesyglobales/6-arquitecturas-de-redes/6-arquitectura-tcp-ip/9-protocolos-tcp-ip/protocolos-de-nivel-de-red/protocolo-icmp

2.2 FORMULACIÓN DEL PROBLEMA

Por lo anterior, es importante fortalecer el proceso de protección de activos e información con las mejores prácticas destinadas a asegurar y preservar la confidencialidad, integridad y disponibilidad de la información digital, así como la seguridad de las personas, abordando el ciclo de vida completo (Montenegro, s.f.) de las Ciber amenazas, (identificar, proteger, detectar, responder y recuperar) para que la información sea segura. Por lo anterior, surge el siguiente interrogante:

¿Cuáles son las mejores prácticas de seguridad de la información para el fortalecimiento de los procesos de atención de eventos o incidentes informáticos ofrecidos por las mesas de servicio de TI?

3 JUSTIFICACIÓN

Actualmente los diferentes riesgos de Ciberseguridad que se presentan en las organizaciones, podrían afectar la credibilidad de los procesos de negocio, así como de los líderes en tecnología encargados de las mesas de servicio de TI o Helpdesk, lo anterior, debido a la gran cantidad de datos que son compartidos en la red con diferentes países, en donde se podría exponer información confidencial y relevante del negocio de cada uno de sus aliados, por lo cual, es importante realizar un análisis y monitoreo de alertas sobre los activos, logrando ajustar defensas sobre estas amenazas que pueden causar daño.

4 OBJETIVOS

4.1 OBJETIVO GENERAL

Diseñar una metodología para mejorar los niveles de atención de eventos o incidentes informáticos de las mesas de servicios TI en las organizaciones a partir de marco ITIL V4 y el estándar ISO 27001.

4.2 OBJETIVOS ESPECÍFICOS

Analizar los marcos, estándares y metodologías para la gestión TI en relación con los procesos de atención de eventos o incidentes informáticos ofrecidos por las mesas de servicio de TI.

Proponer una metodología para gestionar riesgos y mejorar los niveles de atención de eventos o incidentes informáticos de las mesas de servicios TI en las organizaciones a partir de marco ITIL V4 y el estándar ISO 27001.

Establecer las herramientas, controles y medidas para la mitigación de riesgos necesarias en la operación de las mesas de servicio de TI.

5 MARCO REFERENCIAL

5.1 MARCO TEÓRICO

Los sistemas de seguridad informática han ido evolucionando y cambiando notablemente, por lo cual los hackers son cada vez más precisos, haciendo que la Seguridad de la información sea más compleja.

Según el artículo “Análisis de riesgos en seguridad de la información”: el uso continuo y generalizado a nivel global de internet, ha aumentado los ataques a los sistemas informáticos, llevando a las empresas a buscar estrategias que puedan ejecutar un análisis que prevengan, controlen y reduzcan los riesgos asociados a violación y vulnerabilidad de su información [15].

En el análisis de riesgos es importante que las organizaciones establezcan objetivos empresariales por medio de un análisis dando respuesta a interrogantes: “saber qué se quiere proteger, contra quién y cómo se va hacer”, teniendo en cuenta que las organizaciones se encuentran expuestas día a día a amenazas tanto internas como externas ocasionando robos de identidad e información, base de datos, información sensible clientes; por lo tanto es importantes que las empresas apliquen metodologías de protección de seguridad para análisis de riesgos.[16]
Como se puede observar en la **figura 1** las tareas principales de análisis de riesgos permiten llevar a cabo las recomendaciones por fases para mitigar la posibilidad de algún tipo de incidente de seguridad, donde se define en 5 fases o etapas comunes en la metodología[17]:

---

[15] *PULIDO, J., & JOHN, B.[revista.jdc.edu.co][Sitio web] [Consulta: 23 de diciembre de 2013]. RISK ANALYSIS IN SECURITY OF INFORMATION[https://revista.jdc.edu.co/index.php/rciyt/article/download/121/113]. 41;42.*
[16] *Ibid., p, 42.*

[17] INCIBE. (s.f.). *¡Fácil y sencillo! Análisis de riesgos en 6 pasos[www.incibe.es]dirigido a reducir los riesgos a los que está expuesta la organización hasta unos niveles aceptables a partir de un análisis de la situación*

- ✓ Fase 1: Definición de alcance: El paso inicial para realizar un análisis del riesgo estableciendo el alcance limitado que cubra las áreas estrategias para mejorar la seguridad.
- ✓ Fase 2: Identificar los activos: Después de definir el alcance, se debe identificar los activos más importantes relacionados con el proceso o sistema de estudio a modo de inventario, ejemplo: plantilla Excel con los ítems (ID, Nombre, descripción, responsable, tipo, ubicación, crítico).
- ✓ Fase 3: Identificar/seleccionar las amenazas: Se conocen los principales activos y posterior a esto se da continuidad a identificar las amenazas a las que están expuestos manteniendo un enfoque práctico y aplicado.
- ✓ Fase 4: Identificar vulnerabilidades y salvaguardas: Esta fase permite identificar puntos débiles y vulnerabilidades por medio del estudio de las características de los activos.
- ✓ Fase 5: Evaluar riesgos: En esta fase se dispone de los elementos de inventario de activos, amenazas a las que está expuesto cada activo, vulnerabilidades a las que se encuentra asociadas (si aplica), junto las medidas de seguridad; con esto se podrá dar curso a calcular el riesgo: Probabilidad*impacto por medio de criterios cualitativos o cuantitativos.
- ✓ Fase 6: Tratar el riesgo: Una vez calculado el riesgo se debe tratar los que superen el límite establecido, superior a "4" o superior a medio, por medio de alguna de las estrategias principales como transferir riesgo a terceros, eliminar el riesgo, asumir el riesgo, implantar medidas para mitigarlo.

Los problemas de Ciberseguridad, según la "Revista Criminalidad"[18], las empresas en Colombia cerca del 43% no están preparadas para enfrentar los Ciberataques, impactando negativamente los frentes económicos registrando pérdidas cerca de 1 billón de dólares por Ciberataques en el 2015[19], en el 2017 se vio afectado por Ciberataque Ramsanware secuestrando información exigiendo pagos en bitcoins a más de 12 empresas, en "el 2019 se llegó a 30.410 delitos informáticos con una distribución de Phishing (42%), suplantación de identidad (28%), envío de malware (14%), pagos medios de pagos online (16%), principalmente Bogotá, Cali, Medellín y Barranquilla"[20].

La vulnerabilidad frente a la ciberdelincuencia aumentó en **2020**, por confinamiento derivado del Coronavirus(COVID 19), como consecuencia del aumento en la

inicial [consulta 16 enero 2017]. Obtenido de https://www.incibe.es/protege-tu-empresa/blog/analisis-riesgos-pasos-sencillo

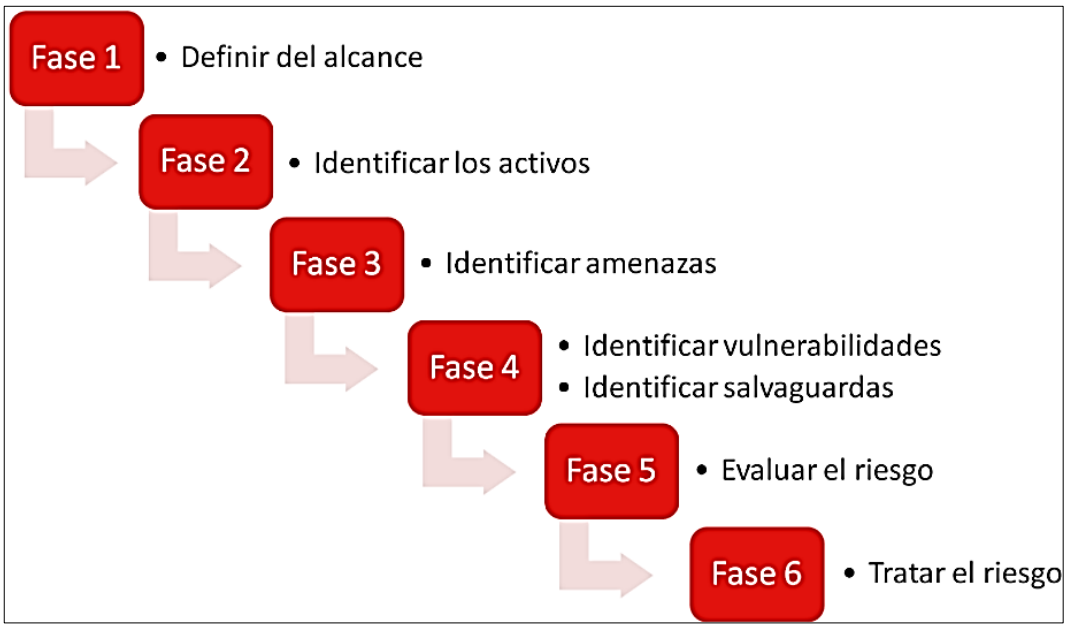
[18] OSPINA DIAZ, M. R. . *Desafíos nacionales frente a la ciberseguridad[http://www.scielo.org.co/] En la actualidad los sistemas de información, la[Consultado: 30 de marzo de 2019.]*. Obtenido de http://www.scielo.org.co/pdf/crim/v62n2/1794-3108-crim-62-02-199.pdf

[19] Ibid., p, 3

[20] Ibid., p, 3

virtualización de la vida y el trabajo (clases de forma remota, incremento el uso de aplicaciones de mensajería, transacciones bancarias online, reuniones, compras por internet, entre otras…), como resultado incrementando el uso de páginas falsas, textos desinformativos, mensajes con virus adjuntos, llamadas engañosas para obtener datos bancarios, dominios falsos, correos electrónicos con Phishing , etc…[21]

Figura 1. Fases de las metodologías para el análisis de riesgos:



Fuente: *INCIBE Instituto Nacional de Ciberseguridad "Análisis de Riesgo en 6 pasos" 2017.*

[21] Ibid., p, 3

5.2 MARCO CONCEPTUAL

Las mejores prácticas en TI son un método innovador que contribuye a la mejora y rendimiento deseado para alcanzar objetivos de la organización. "Una característica esencial en la implementación de una mejor práctica es prevenir al cliente, estar preparado y analizar los patrones de comportamiento del cliente ante cualquier situación"[22], fortaleciendo los procesos.
En los procesos son eficaces y eficientes aportando a los posibles Incidentes de cualquier tipo de impacto (bajo, alto y medio).

Dentro de los incidentes es importante tener un enfoque estructurado al modelo de gestión incidente de seguridad donde se definen roles para evaluar riesgos, manteniendo operatividad, continuidad y disponibilidad del servicio en una Mesa de servicios. [23]

Hackers: Según la RAE, un Hacker o pirata informático son personas con habilitades de investigación en los sistemas informáticos para notificar los fallos e implementar técnicas de mejoras. [24]

Riesgos informáticos: Es un proceso que identifica los activos informativos, vulnerabilidades y amenazas a los que pueden estar expuestos, como ataques externos, desastres naturales o errores humanos. [25]
Mesa de ayuda: Punto único de contacto que resuelve en forma oportuna los requerimientos que puedan tener los distintos tipos de usuarios de la empresa antes incidentes, consultas y peticiones de servicios de TI[26].

---

[22] *Ministerio de Tecnologías de la Información.. Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información.[Consulta 11 de junio de 2016] Obtenido de https://www.mintic.gov.co/gestionti/615/articles-5482_G21_Gestion_Incidentes.pdf*
[23] *Ibid., p, 11*

[24] *Tipos de Hackers[https://www.campuscyberseguridad.com][Sitio web] bilidades en el manejo de computadoras que investiga un sistema informático[Consulta:07 de mayo 2023] . (s.f.). Obtenido de https://www.campuscyberseguridad.com/blog/item/133-tipos-de-hackers*

[25] *Rodriguez, P. (s.f.). riesgos informáticos[https://www.ambit-bst.com][Sitio Web]el análisis de riesgos informáticos es la evaluación de los distintos peligros que afectan a nivel informático[Consulta: 07 de mayo 2023]. Obtenido de https://www.ambit-bst.com/blog/an%C3%A1lisis-de-riesgos-inform%C3%A1ticos-y-ciberseguridad*
[26] SONDA S.A. SOPORTE DE INFRAESTRUCTURA SERVICEDESK. [en línea] El Servicedesk de SONDA opera como un único punto de contacto que resuelve de forma oportuna incidentes de servicios de TI[consulta: 2021] Disponible en: https://www.sonda.com/content/uploads/2018/12/ServiceDesk.pdf

Phishing: Son los métodos que utilizan los delincuentes cibernéticos para obtener información confidencial y realizar estafas, la técnica más utilizada es la “ingeniería social”.[27]

SLA: “Acuerdo de Nivel de Servicios”, es un documento donde se estipulan las condiciones comprometidas(proveedor) al prestador del servicio para cumplir los niveles de calidad del servicio contratados con el cliente. Dentro del apartado se debe incluir la definición, provisión, disponibilidad, atención al cliente, tiempo de respuesta, mantenimiento, penalización.[28]

[27] *MARCELO Rivero (s.f) El ransomware es una forma de malware que está en auge[https://es.malwarebytes.com/][Sitio web][Consulta 07 agosto]. Obtenido https://es.malwarebytes.com/ransomware/*

[28] ACENSWHITEPAPERS. (s.f.). *"¿Qué es el SLA?"[https://www.acens.com][Sitio Web] Service Level Agreement, traducido como Acuerdo de Nivel de Servicio[Consulta:05 de mayo 2023]*. Obtenido de https://www.acens.com/file_download/176/acens_que_es_el_sla_baja.pdf

5.3 MARCO HISTÓRICO

En la siguiente tabla se encuentra la información general de Metodología para identificación y valoración de riesgos y salvaguardas en una mesa de ayuda tecnológica. Esta metodología fue seleccionada teniendo en cuenta que se encuentra alineada a la necesidad de la identificación de los riesgos a la que se pueda encontrar expuesta una mesa de ayuda.

Tabla 1 Metodologías

Información General	
Tipo de documento	Web
Acceso al documento	http://repository.unipiloto.edu.co/handle/20.500.12277/2633
Título del documento	Metodología para identificación y valoración de riesgos y salvaguardas en una mesa de ayuda tecnológica.
Autor(es)	Ruge Pinzón, Jeison Nicolás
Director	García Rondón, Richard / Asesor
Fecha de publicación	6/03/2013
Unidad Patrocinante	Universidad Piloto de Colombia
Palabras Claves	riesgos, organizaciones , mesa de ayuda, activos
2. Resumen	
Las organizaciones financieras tienen implementada una mesa de ayuda tecnológica que es la encargada de la atención de las solicitudes o servicios relacionados con los activos de información tecnológicos, siendo un proceso necesario e importante para la organización se hace necesario mostrar una metodología que permita identificar y valorar los riesgos y salvaguardas que se asocian al proceso y que servirá como una guía o serie de pasos para las	

organizaciones en la implementación de mesas de ayuda o la revisión de una que ya esté implementada. Para la identificación de la metodología que se aplicó al proceso de mesa de ayuda, se decidió realizar una serie de tablas de comparación entre algunas metodologías de análisis de riesgos como son COBRA, COBIT, CRAMM, MAGERIT y OCTAVE esta comparación arrojo como resultado que la metodología para la identificación y valoración de riesgos y salvaguardas de una mesa de ayuda es MAGERIT. La metodología de MAGERIT define una metodología que se explica y en la que se aplican cuatro pasos como son la identificación y valoración de activos, la identificación y valoración de amenazas., la determinación del riesgo y la identificación y valoración de salvaguardas. El análisis de la mesa de ayuda en cada uno de estos pasos permite identificar factores y criterios se deben tener en cuenta para identificar y valorar los riesgos y salvaguardas que se presentan en el proceso que comprende a la mesa de ayuda tecnológica.

Fuente: *Elaboración propia con investigación realizada*

En la **tabla 2** se encuentra la propuesta de gestión de seguridad de la información

Tabla 2 Propuesta de Gestión de Seguridad de la Información

1. Información General	
Tipo de documento	Web
Acceso al documento	http://hdl.handle.net/20.500.11799/80295
Título del documento	Propuesta de gestión de seguridad de la información de mesas de servicio de la empresa sonda México S.A
Autor(es)	Vázquez García, Delfina
Director	
Fecha de publicación	2017-05
Unidad Patrocinante	Universidad Piloto de Colombia
Palabras Claves	Gestión, Información, Empresa
2. Resumen	
La propuesta está basada en la seguridad de la información de la norma de ISO/IEC 27001:2013, se implementarán políticas y controles en la unidad de	

negocio del Services Desk de la empresa SONDA, se realizará un análisis de riesgo el cual nos ayudará a identificar los riesgos de seguridad, amenazas, vulnerabilidades, probabilidad e impacto, con la finalidad de resguardar, proteger y preservar la confidencialidad, integridad y disponibilidad de la seguridad de la información. Todo activo identificado como riesgo se clasificará por activo de apoyo como software, hardware, recursos humanos, información, sistemas y/o infraestructura. Todos los riesgos identificados deben de tener un tratamiento, existen cuatro formas para el tratamiento, uno aceptar el riesgo, dos eludir o evitar el riesgo, tres trasferir el riesgo, cuatro mitigar el riesgo, el tratamiento es uno de los puntos más importantes para reducir un riesgo, se debe saber cómo clasificar el riesgo ya que dependiendo del resultado podemos tratar el riesgo, para llevar a cabo el tratamiento se deberá de llenar un formato de control de riesgos. Hoy en día están muy de moda los virus como Phishing y Ransomware. Los virus son las amenazas externas que puede acabar con los equipos que no tienen instalado o actualizado el antivirus, es importante tener protegida la información, es por ello por lo que la seguridad de la información es muy importante para las empresas que se dedican a la tecnología de la información. Cada dos meses deberá haber una reunión del comité de seguridad, donde se muestren los avances de los riesgos identificados, las métricas, hallazgos e informes, toda información que se ve en el comité de seguridad se debe presentar en la siguiente reunión, los encargados de cada unidad de negoción son responsables de monitorear y dar seguimiento a sus hallazgos y riesgos de seguridad.

Fuente: *Elaboración propia con investigación realizada*

6 DESARROLLO DE LOS OBJETIVOS

6.1 ANALIZAR LOS MARCOS, ESTÁNDARES Y METODOLOGÍAS PARA LA GESTIÓN TI EN RELACIÓN CON LOS PROCESOS DE ATENCIÓN DE EVENTOS O INCIDENTES INFORMÁTICOS OFRECIDOS POR LAS MESAS DE SERVICIO DE TI.

Actualmente la preservación de la Seguridad Informática exige agotar una de las etapas más importantes que corresponde a la identificación, análisis y tratamiento de riesgos en toda la organización, permitiendo validar oportunidades y amenazas, logrando alcanzar objetivos del negocio, por lo cual el análisis de riesgos informáticos pasa a ser una parte fundamental en la administración de seguridad logrando beneficios que permitan identificar los puntos más débiles de la estructura, con el objetivo de la planificación de reducción de riesgos, prevención de accidentes, visualización y detección de las debilidades existentes en los sistemas y toma de mejores decisiones en materia de la seguridad de la información.[29]. Las metodologías que sobresalen son las siguientes:

- **OCTAVE** (Operationally Critical Threat, Asset, and Vulnerability Evaluation): Es la metodología de análisis de riesgos que más utiliza las empresas, donde se describe un conjunto de criterios para desarrollar métodos que se adhieran a las guías que proponen un plan de mitigación dentro de la organización enfocados en concientizarlos en que la seguridad informática no es asunto solamente técnico, sino también los aspectos no técnicos[30], realizando

[29] ALEMAN NOVOA, H. A., & RODRIGUEZ BARRERA, C. (Metodologías Parael análisisde riesgosenlos sgsi. *[Consulta:16 de mayo de 2014]* Obtenido de https://hemeroteca.unad.edu.co/index.php/publicaciones-e investigacion/article/view/1435/1754

[30] ISOTOOLS EXCELLENCE. (s.f.). *"Blog especializado en Sistemas de Gestión".{En línea}. (09 de septiembre de 2021). Metodología OCTAVE para el análisis de riesgos en SGSI. Obtenido de https://www.pmg-ssi.com/2021/09/metodologia-octave-para-el-analisis-de-riesgos-en-sgsi*

diversos procesos para después asignar un valor estimado para la organización., ejecutando desarrollo de la misión de procesos de auto dirigido, flexible "evolucionado y fases de perfil de amenazadas basados en activos, identificación de vulnerabilidades de la infraestructura y desarrollo de estrategia y planes de seguridad"[31].

- **MAGERIT**: Es la metodología de análisis y gestión de riesgos de la información desarrollada por el Consejo Superior de Administración electrónica[32], en esta metodología sobresalen objetivos principales de los cuales se estudia los riesgos que soporta un sistema de información y su entorno asociado; esta metodología detalla diferentes perspectivas para realizar un análisis de los estados de riesgos y su mitigación, las tareas básicas para realizar un proyecto de análisis de gestión de riesgos y series de aspectos prácticos acumuladas a la experiencia y tiempo de análisis de gestión[33].

- **MEHARI**: Método armonizado de análisis de riesgos, fue propuesta y desarrollada por el Club Francés de la Seguridad de la información CLUSIF en el años 1996, es público para todo tipo de organizaciones, apoya a la

[31] HURTADO, M. (s.f.). *GESTIÓN DE RIESGO METODOLOGÍAS OCTAVE y MAGERIT[http://polux.unipiloto.edu.co/] plantea una gestión [Consulta:2002:].* Obtenido de http://polux.unipiloto.edu.co:8080/00004420.pdf

[32] Ministerio de Hacienda y Administraciones Públicas. (octubre de 2012). *MAGERIT v.3 : Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información*. Obtenido de https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.VRMl5_yG8ms

[33] Libro I - Método. (s.f.). *Metodología de Análisis y Gestión[Consulta octubre 2012]. Disponible en https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html.*

responsabilidades de la Seguridad Informática mediante el análisis de principales factores de riesgos, evaluando cuantitativamente situaciones de la organización donde se requiera análisis por parte de los auditores y gestores de riesgos[34].

- **NIST SP 800 – 30**: (National Institute of Standards and Technology), es una guía que da a conocer un conjunto de recomendaciones y actividades para una adecuada gestión de riesgos en la gestión de sistemas de información, pero no es suficiente teniendo en cuenta que se requiere apoyo de toda la organización para que los objetivos y el alcance de gestión de riesgos, sean un éxito; se encuentra compuesta por 9 pasos básicos para análisis de riesgos como lo es la caracterización de sistemas, identificación de amenazas y vulnerabilidades, control de análisis y determinación del riesgo, análisis de impacto y recomendaciones de control.[35].

- **CORAS – CONSTRUC**: un grupo de investigadores noruegos financiados por organizaciones del sector público y privado, cuya misión es proporcionar un marco de trabajo encaminado a sistemas en los que la seguridad es crítica. Su aplicación permite la detección de fallas de seguridad, inconsistencias, redundancia y el descubrimiento de vulnerabilidades de seguridad exploradas en siete etapas (Presentación- Análisis de alto nivel-

[34] *ISOTools Excellence. (23 de septiembre de 2021). Metodología Mehari para el análisis de Riesgos en SGSI. Obtenido de https://www.pmg-ssi.com/2021/09/metodologia-mehari-para-el-analisis-de-riesgos-en-sgsi/*.

[35] *AVALOS SERRANO, V. (2007). Repositorio Institucional de la Universidad de las Fuerzas Armadas ESPE. Obtenido de http://repositorio.espe.edu.ec/handle/21000/233*

Aprobación - Identificación de riesgos- Estimación de riesgo - Evaluación de riesgo Tratamiento del riesgo)[36].

- **CRAMM** (CCTA risk analysis and management method): Es una metodología de análisis de riesgos, desarrollada por el Central Communication and Telecommunication Agency (CCTA) del gobierno del Reino Unido, utilizada, por lo general, en Europa y dirigida a grandes industrias, entre otras, organizaciones gubernamentales.[37]

Teniendo en cuenta información anterior para la gestión de eventos o incidentes informáticos se debe tener claro el alcance que abarca las metodologías manifestadas anteriormente por medio da detección, registro de solución de forma oportuna y eficiente, logrando evidenciar los impactos que pueden afectar la operación de los servicios de TI; los incidentes pueden generarse por riegos de sucesos incluyendo la partes operativa por procesos inadecuados, normativas u otros factores controlables generando amenazas, vulnerabilidades y riesgos de TI[38] por lo cual se debe proceder con el tratamiento que puedan reducir estos niveles con estrategias basados en la guía COBIT 5 [39]. De las metodologías nombradas anteriormente la "**MAGERIT" (**Metodología de Análisis y Gestión de Riesgos de los

[36] *SEGURIDAD 7 "A" . (s.f.). Metodología CORAS (COnstruct a platform for Risk Analysis of Security critical system). Obtenido de http://seguridades7a.blogspot.com/p/coras.html*.

[38] ABIT TEAMS. (s.f.). *Metodología ITIL:[https://www.ambit-bst.com/] gestión de incidencias y objetivos[Consulta: 17 noviembre del 2021]*. Obtenido de https://www.ambit-bst.com/blog/metodolog%C3%ADa-itil-gesti%C3%B3n-de-incidencias-y-objetivos

[39] PAE. (s.f.). *electrónica, MAGERIT v.3 : "Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información". {En linea}. {octubre 2012} Obtenido de http://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html*.

Sistemas de Información)[40] facilita la gestión en el proceso de atención de eventos o incidentes en la Mesa de Ayuda, esta metodología tipifica los activos con criterios que identifican las amenazas potenciales y salvaguardar la naturaleza diferentes tipos de activos:

- ✓ Datos
- ✓ Criptográficas
- ✓ Servicios
- ✓ Software
- ✓ Hardware
- ✓ Comunicaciones
- ✓ Soporte
- ✓ Auxiliar
- ✓ Instalaciones
- ✓ Personal

Estos activos tienen una probabilidad de vulneración (Muy rara, Poco probable Posible, Probable, Prácticamente seguro); llevando un nivel de aceptación según las amenazas de cada uno de los nombres de activos. Las amenazas según MAGERIT pueden ser por:

Tabla 3 Amenazas según MAGERIT

[E1]	Errores de los usuarios
[E2]	Errores del administrador
[E10]	Errores de secuencia
[E15]	Alteración accidental de la información
[A11]	Acceso no autorizado
[A19]	Divulgación de información
[E20]	Vulnerabilidades de los programas (software)
[A24]	Denegación de servicio

40 PAE. (s.f.). *electrónica, MAGERIT v.3 : "Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información". {En linea}. {octubre 2012} Obtenido de http://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html*.

Otros

Fuente: *Elaboración propia con investigación realizada*

En las Mesas de Servicios de debe trabajar para controlar cada uno de estas amenazas que se puedan ver reflejadas en incidentes aplicando un plan de tratamiento efectivo y documentado, por ejemplo se pueden evidenciar incidentes por:

- Falta de controles de ingreso en el sitio donde se almacenan estos activos
- Mal manejo de las credenciales de la nube
- Proceso de autenticación, por lo que un atacante puede obtener el control completo del equipo de manera remota.
- Divulgar información sin autorización del personal
- Falsificación de solicitudes entre sitios, que se debe al hecho de que las aplicaciones WEB no verifican adecuadamente si las solicitudes provienen de usuarios confiables.
- Error en la configuración de reglas de Spam.
- Robo del equipo el trabajo par falta de controles en el acceso físico a la oficina.

La Gestión de incidentes en las Mesas de Ayuda, busca recuperar la operación normal de los servicios de TI en el menor tiempo posible, minimizando el impacto en los procesos de negocio, por medio de la detección, registro y solución de IM (Incidente mayor)[41] de forma oportuna y eficiente permitiendo evidenciar los impactos que puede afectar la correcta operación de los servicios de TI. El procedimiento se encuentra conformado por los responsables de cada una de las actividades involucrados para solución como lo es el analista resolutor N1 y Gestor

[41] ABIT TEAMS. (s.f.). *Metodología ITIL:[https://www.ambit-bst.com/] gestión de incidencias y objetivos[Consulta: 17 noviembre del 2021]*. Obtenido de https://www.ambit-bst.com/blog/metodolog%C3%ADa-itil-gesti%C3%B3n-de-incidencias-y-objetivos

de incidente quién se encarga de contactar a las personas especialistas de la aplicación afectadas, dando seguimiento hasta confirmar recuperación de la falla y cierre del ticket; finalmente se debe realizar un informe técnico de causa raíz por parte del grupo resolutor[42]. Respecto a los incidentes la metodología **MAGERIT** analiza la amenaza que puede perjudicar un activo por medio de sentidos de degradación (daño causado por un incidente en el supuesto que ocurriría) y probabilidad (probabilidad que se materialice la amenaza)[43] Los eventos son situaciones/sucesos que se pueden producir en la organización, afectando específicamente la prestación del servicio del soporte Mesa de Ayuda por medio de la monitorización desde la infraestructura de TI, gestionando posibles incidencias[44].

[42] SONDACHILE.sharepoint.com. 2021. GESTIÓN D E INCIDENTES. Consulta [Consultado el 23 de noviembre de 2021].] Disponible en: <https://sondachile.sharepoint.com/sites/Intranet_Colombia/FAQ/Paginas/GESTI%C3%93N%20DE%20INCIDENTES.aspx>

[43] Ccn-cert.cni.es. 2021. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. [Sitio web] Disponible en: <https://www.ccn-cert.cni.es/documentos-

[44] El Blog de Proactivanet. 2021. Gestión de Incidencias, software y Eventos en ITIL. [Sitio web] Disponible en: <https://www.proactivanet.com/blog/gestion-de-incidencias/software-gestion-de-eventos-itil/> [Consultado el 24 de noviembre de 2021].

6.2 METODOLOGÍA PARA GESTIONAR RIESGOS Y MEJORAR LOS NIVELES DE ATENCIÓN DE EVENTOS O INCIDENTES INFORMÁTICOS DE LAS MESAS DE SERVICIOS TI EN LAS ORGANIZACIONES A PARTIR DE MARCO ITIL V4 Y EL ESTÁNDAR ISO 27001

Es importante conocer los pasos de gestión de riesgos según la norma ISO, donde establece el plan de comunicación, el contexto organizacional, valoración de los riesgos, tratamiento de los riesgos y monitoreo y mejora continua de los procesos de gestión como se mencionan en la **Figura 2** y se encuentra diseñado para permitir a las organizaciones evaluar los riesgos de seguridad por medio de los sistemas y controles.[45]

Figura 3 : Ciclo de vida de la gestión de riesgos

Fuente: *Planificación en ISO 27001, (2022)*

A continuación, se contextualiza el proceso del ciclo:

[45] *PLANIFICACIÓN EN ISO 27001, 2022. permitir a las organizaciones identificar, analizar y evaluar sistemáticamente los riesgos de seguridad [Sitio web] [Consultado el 10 de agosto de 2022] Disponible en https://normaiso27001.es/planificacion-en-iso-27001/*

- Establecimiento del plan de comunicación: Corresponde a la capacitación adecuada a los diferentes tipos de usuarios que utilizan la tecnología dentro de la organización y tienen asignados equipos de trabajo (multidisciplinarios - heterogéneos) y no siempre están las personas expertas en TI, que tienen claro los conceptos de seguridad de la información y procesos de gestión de riesgos, por lo cual se puede presentar cualquier amenaza en las aplicaciones de la metodología y es donde el equipo debe estar capacitado ante gestión de riesgos y el plan de comunicación debe estar diseña de tal manera puede concientizar a los usuario; la estructura debe estar dividida en 3 etapas: comunicación inicial, comunicación en la marcha y comunicación de los resultados, aplicando etapas internas y externas según la estructura de la organización. [46]

- Establecimiento del contexto organizacional: Todas las empresas contienen a nivel interno su misión, visión, políticas, objetivos, estrategias, metas, roles y responsabilidades, estructura, normativas internas – externas, entre otras…e interactúan con su entorno en cuanto a aspectos necesarios como lo es la competencia, regulaciones legales, economía, política, tecnología, cultura, teniendo en cuenta información anterior es importante conocer y comprender estos aspectos para que se necesita proteger y las limitaciones para su cumplimiento; su objetivo es conocer completamente la organización y poder validar cuál podría ser su afectación a nivel interno y externo y de acuerdo a su recurso actual establecer el nivel de aceptación de riesgos. [47]

[46] ISO/IEC. (2009). Obtenido de https://www.iso.org/obp/ui/%7B#}iso:std:iso-iec:27005:ed-2:v1:en
[47] OMG. (s.f.). *"Object Management Group. (1997 - 2021)". " Modelo y notación de procesos de negocio del grupo de gestión de objetos". {En línea} Disponible en https://www.bpmn.org*

- Valoración de los riesgos: En esta etapa se identifica principalmente los activos que se requiere proteger y sus debilidades y amenazas que se encuentra expuesta, por lo cual se recomiendo controles para mitigar sus riesgos. Por medio de la valoración de activos se debe tener en cuenta inicialmente los activos relevante, junto con procesos, información, datos y activos de soporte.

- Tratamientos de los riesgos: Establecen en implementan acciones a tomar para mitigar los riesgos encontrados y lograr riesgos residuales aceptables por la organización. [48]

- Monitoreo y mejora continua del proceso de gestión: Es un control de cambios que debe realizarse sobre los activos, procesos, vulnerabilidades, amenazas, controles, documentación de políticas y procedimientos para establecer acciones sobre los cambios, también se busca con el monitoreo y mejora continua, asegurar la constante revisión de gestión de riesgos. [49]

En la Mesa de Ayuda se debe llevar un control para cumplimiento de cada uno de los pasos nombrados, permitiendo afrontar los problemas de Seguridad en relación a los riesgos que generan pérdidas de su confidencialidad, integridad y disponibilidad, por medio de la norma **ISO 27001** es necesario establecer estos criterios para identificar los activos de información y la forma se pueden reconocer en la organización, principalmente el cumplimiento de:

---

[48] *Oficina de Seguridad para las Redes Informáticas. (s.f.). METODOLOGÍA PARA LA GESTIÓN DE SEGURIDAD INFORMÁTICA. Obtenido de https://instituciones.sld.cu/dnspminsap/files/2013/08/Metodologia-PSI-NUEVAProyecto.pdf*

[49] EPHPO. (s.f.). *Control y Mejora continua de los procesos[http://www.ephpo.es/]diseño de un proceso asistencial se describen las etapas necesarias para obtener el mejor resultado[Consulta 2021].* Obtenido de http://www.ephpo.es/Procesos/GUIA_DISENO_MEJORA/5.pdf

- Inventario de Activos: Se deben tener identificados para proteger cada uno, junto con los procesos que lo utilizan.

- Propiedad de los Activos: Toda la información y los activos deben estar asociados a un procedimiento de propiedad designada a la organización, determinando interacción con activos de información, como lo es:

    - Propiedad de información: Grupo de trabajo que define a quiénes se le otorga el acceso a la información y requisitos para que se salvaguarde frente “accesos no autorizados, modificación, perdida de confidencialidad o destrucción deliberada”[50], junto con definición de cómo proceder con la información no requerida.
    - Custodia técnicos: Es la parte encargada de administrar y hacer que los controles de seguridad sean efectivos (copias de seguridad, privilegios, accesos, modificaciones y borrados), por medio de los controles establecidos.
    - Usuario: Se definen los derechos a nivel de accesos a los activos de información (lectura, escritura, borrado, entre otros…)

- Directrices de clasificación: es la clasificación de los términos de valor y requisitos legales para establecer términos de su confidencialidad, clasificados por niveles de accesos permitidos, métodos de distribución y/o transmisión, Condiciones de almacenamiento, Condiciones de entrega de terceros, destrucción.

[50] *VARELA, F. A. (s.f.). GESTIONES DE SEGURIDAD DE LA INFORMACIÓN. Obtenido de https://www.novasec.co/blog/62-gestion-integral-de-la-seguridad-de-la-informacion*

La aplicación de la metodología de "**ITIL"**[51] en la Mesa de Ayuda, aporta mejorar procesos de atención, construyendo relación de confianza con el cliente, para gestionar los riesgos y mejoras de atención respecto a los incidentes, por medio de análisis y priorización; garantizando el mantenimiento de calidad y disponibilidad del servicio en cualquier momento, restableciendo rápidamente el servicio. Dentro de la operación del servicio, los eventos que son cambios de estado que tenga importancia para la gestión de un elemento de configuración (CI), se pueden presentar eventos frecuentes, pero menos importantes, como hay otros que son menos frecuentes pero tienen mayor relevancia:

- Eventos informativos, ocurren y son parte de la operación normal del servicio (logueo de usuarios a herramienta, respaldos, cierre de sesión), informa sobre la operación del servicio.

- Eventos de Advertencia, anuales, avisan que está sucediendo algo, temas donde se está llegando a límites de almacenamientos, se va a cumplir tiempo para dar respuesta frente a una solicitud, o eventos inusuales frente a un OS .
- Eventos de Excepción, donde se encuentran situaciones que pone en riesgo la operación del servicio (**Incidente**), posibles **Problemas** de seguridad, dispara una alerta y es registro del Incidente..

Para poder detectar los eventos es necesario monitorear los elementos de configuración (CI), para detectar condiciones de importancia potencial, rastrear, registrar su estado(logs) y proporcionar la información a las partes interesadas, estos seguimientos se realizan por medio de monitoreo proactivo(tomar decisiones

[51] *MALVES. (2021). ¿Cómo aplicar la metodología ITIL en el Help Desk? Obtenido de https://milvus.online/blog/como-aplicar-la-metodologia-itil-en-el-help-desk/*

basadas en el análisis de los patrones de los eventos que han sucedido para evitar ocurra una situación) y reactivo (se responde da manera y oportuna para disminuir el impacto que pueda ocurrir), esto nos permite analizar los componentes de los servicios, priorizar los eventos relevantes y gestionarlos a través de todo el ciclo de vida y poder tener control y visibilidad de cómo se está comportando el servicio[52].

Según lo expuesto anteriormente la metodología **MAGERIT** se ajusta al proyecto, por cumplimiento en los pasos para gestionar riesgos, mejora de atención y eventos; por medio de la validación de activos con criterios que identifican la amenaza, desde la el establecimiento de un plan comunicación hasta el monitoreo continuo, permitiendo alertar y confrontar los problemas de seguridad de manera proactiva y reactiva. De esta forma se da cumplimiento a los indicadores contratados para gestión de riesgos en las Mesas de Ayuda, como lo son los KPIs[53] (indicadores claves de rendimiento), permitiendo evaluar el éxito de las actividades propuesta en la metodología.

En la gestión de Incidentes, la metodología **MAGERIT,** hace que las personas involucradas en la operación tengan un papel relevante en prevenir problemas de los activos y reaccionar con agilidad para cuando se produzcan puedan atajar las emergencias, sobreviviendo a los incidentes y seguir operando de la mejor forma por medio del análisis y tratamiento de riesgos, 0 estimar el impacto y el riesgo.[54]

---

[52] *EnevaSys. (agosto de 2021). ITIL con #Jira - 6) Gestión y Monitoreo de Eventos. Obtenido de* https://www.youtube.com/watch?v=PbgbGZX03yY

53 BLOG.es.logicalis.com. 2021. KPI's ¿Qué son, para qué sirven y por qué y cómo utilizarlos? . [Sitio web] Disponible en: <https://blog.es.logicalis.com/analytics/kpis-qu%C3%A9-son-para-qu%C3%A9-sirven-y-por-qu%C3%A9 -yc% C3% B3mo-utilizarlos> [Consultado el 28 de noviembre de 2021].

[54] Libro I - Método. (s.f.). *Metodología de Análisis y Gestión[Consulta octubre 2012]. Disponible en https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html.*

La ejecución de esta metodología se realiza con una serie de pasos que ayudan a la mesa de servicios a mantener los riesgos bajo control detectando a tiempo su existencia, prepara a la organización para procesos de auditoría y certificación y por medio de esta metodología se ofrece un análisis más completo desde los objetivos de seguridad.[55]

[55] PINZON, J. N. (s.f.). *Universidad Piloto de Colombia. {En line}.Metodología para identificación y valoración de riesgos y Salvaguardas en una Mesa de Ayuda[Consultado 2011]. Disponible en chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/http://polux.unipiloto.edu.co:8080/0.*

6.3 ESTABLECER LAS HERRAMIENTAS, CONTROLES Y MEDIDAS PARA LA MITIGACIÓN DE RIESGOS NECESARIAS EN LA OPERACIÓN DE LAS MESAS DE SERVICIO DE TI.

En el Sistema de Gestión de Seguridad se debe conformar por estrategias de controles requeridos para realizar un análisis de riesgos para tomar decisiones como lo es: Determinar qué se trata de proteger, de qué es necesario protegerse, cuan probable son las amenazas, implementación de controles que protejan los bienes informáticos de manera rentable, revisar y perfeccionar continuamente proceso cada vez que sea encontrada una vulnerabilidad[56].El enfoque de las metodologías se encuentra basados en procesos con el fin de establecer, implementar, operar ,dar seguimiento, mantener y mejorar el SGSI adoptando modelo del proceso PHVA(Planificar, hacer, verificar, actuar), permitiendo estructurar proceso de la ISO 27001.

En la gestión de eventos o incidentes es necesario construir una matriz donde se definen los controles mencionados permitiendo mitigar los riesgos que se puedan presentar en la Mesa de Servicios, clasificándolos por impacto y Urgencia.[57]

---

[56] *Oficina de Seguridad para las Redes Informáticas. (s.f.). METODOLOGÍA PARA LA GESTIÓN DE SEGURIDAD INFORMÁTICA. Obtenido de https://instituciones.sld.cu/dnspminsap/files/2013/08/Metodologia-PSI-NUEVAProyecto.pdf*

[57] MONA CARDONA, L., & URIBE SERNA, A. (s.f.). *SISTEMA DE GESTIÓN DE INCIDENTES DE SEGURIDAD INFORMÁTICA PARA CORBETA[http://bibliotecadigital.usbcali.edu.co/]a los riesgos [Consuta: 2015].* Obtenido de http://bibliotecadigital.usbcali.edu.co/bitstream/10819/3932/3/Sistema_Gestion_Incidentes_Seguridad_Mona_2015.pdf

- Impacto: es la importancia del incidente según la afectación de proceso del negocio/número de usuarios
- Urgencia: el tiempo máximo de demora para resolución del incidente aceptado por el cliente.

Dentro de los niveles de prioridad es importante establecer protocolos que determinen la prioridad de incidente con horas hábiles según el ANS (Alta, media y baja). Los mecanismos de control el COBIT permite validar los principios de la Seguridad de la información dando cumplimiento a los "principios de Confidencialidad, Integridad y Disponibilidad"[58]

- APO13- Gestionar la seguridad: Alinear, Planificar y Organizar (APO)
- BAI04 - Gestionar la Disponibilidad y la Capacidad: Construir, adquirir e implementar.
- BAI08 - Gestionar el Conocimiento: Construir, adquirir e implementar.
- DSS04 – Gestionar la Continuidad: Entrega, servicio y soporte (DSS)
- DSS05 - Gestionar servicios de seguridad: Entrega, servicio y soporte (DSS)

En las Mesas de ayuda junto con el oficial de Seguridad se debe analizan riesgos de terceros a la información confidencial, estableciendo acciones correctivas, preventivas y/o mejoramiento de los controles, promoviendo tomas de conciencia en temas de seguridad de la información. "Dentro de los controles se debe considerar riesgos para software sin soporte,

[58] *BOADA, P. E.. EVALUACIÓN DE SEGURIDAD PARA EL PROCESO DE MESA DE AYUDA. [alejandria.poligran.edu.co][Consulta 2017].Disponible en https://alejandria.poligran.edu.co/bitstream/handle/10823/1044/Evaluaci%C3%B3n%20de%20seguridad%20para%20el%20proceso%20de%20mesa%20de%20ayuda.pdf?sequence=1&isAllowed=y*

instalación de parches liberados por el fabricante de administración de directorio activo, la instalación de software deberá estar clasificada por listado de software y equipos, la instalación de software debe ser ejecutada por personal autorizado”[59].

Dentro del análisis para analizar los riesgos en las Mesas de Ayuda, es importante contar con acceso a la herramienta de registro ticket´s CA[60], en donde se encuentra los reportes por día de los incidentes reportados por cada uno de los clientes, permitiendo revisar los posibles riesgos en los activos.

La herramienta **LANSWEEPER** (Software de gestión de activos de TI para profesionales de TI) permite gestionar activos y mapeo de red, validando todos los equipos y dispositivos; evidenciando software no autorizados, OS inferior, antivirus desactualizado…entre otros[61].
Esta herramienta permite descubrir, analizar, controlar y coordinar toda el área de tecnología por medio de automatizaciones de tareas claves de escaneo único de LANSWEEPER , puede descubrir redes de todos los tamaños explorando cualquier entorno de TI con protocolos de red, adicional según el tipo de activo puede recuperar todo tipo de información

---

59 SONDA DE COLOMBIA S.A Y FILIALES. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN [https://sondachile.sharepoint.com]. [Consulta: 27 de octubre de 2021] Disponible en:https://sondachile.sharepoint.com/sites/Intranet_Colombia/GestionInterna/SISTEMA%20GESTI%c3%93N%20INTEGRAL/SGI/DIRECTRICES%20SGI/POLITICAS/741001%20-%20Pol%c3%adtica%20de%20seguridad%20de%20la%20informaci%c3%b3n.pdf

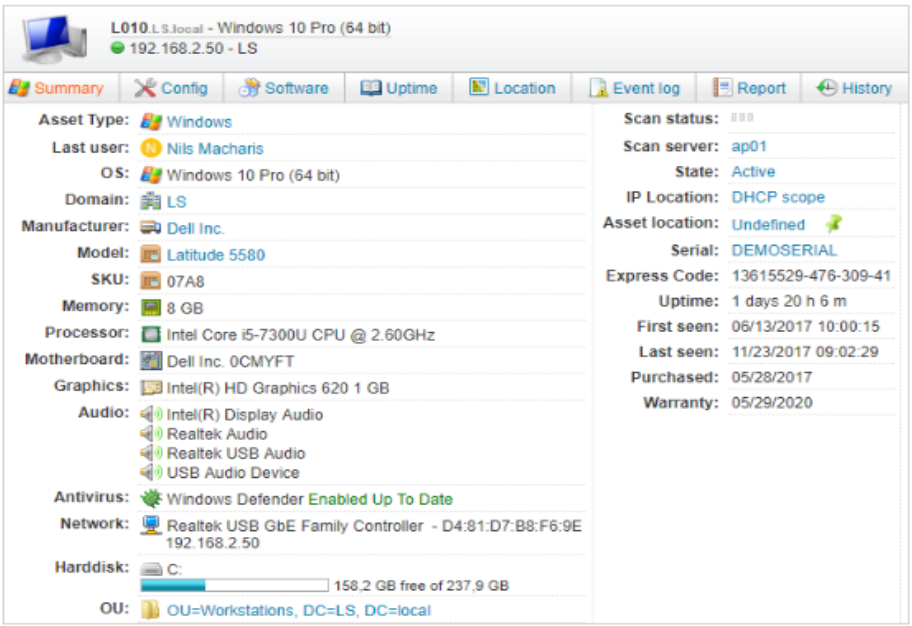
60 *CA Guía de administración. (Sitio web.). CA Service Desk Manager. Obtenido de https://ftpdocs.broadcom.com/cadocs/0/j027931s.pdf*

61 *Cybersecurity Asset Management [https://www.lansweeper.com/] Get an Asset Inventory That Works for Cybersecurity[Consulta 19 de agosto]Obtenido de https://www.lansweeper.com/use-cases/lansweeper-for-cyber-security/*

de hardware especifica del dispositivo de los activos demás de una extensa lista de software instalado e información de la base de datos del servidor , host de máquinas invitadas instaladas; encontrando información general de todas las interfaces activos y conectados, permitiendo mapear fácilmente su red, también información a nivel de impresoras permitiendo tomar medidas antes de que se agoten.

Después de recopilar los datos de la red se puede usar la herramienta de análisis integrado de LANSWEEPER como se evidencia en la **Figura 4,** logrando escanear todo y brindar información detallada para que se pueda usar en estrategias de Ciberseguridad y también el seguimiento de otras partes como lo es control de accesos de gestión de identidad y la gestión de eventos, que son importantes y forman parte de lo que el LANSWEEPER hacer.[62]

Figura 5 Interfaz LANSWEEPER



[62] *Cybersecurity Asset Management [https://www.lansweeper.com/] Get an Asset Inventory That Works for Cybersecurity[Consulta 19 de agosto]Obtenido de https://www.lansweeper.com/use-cases/lansweeper-for-cyber-security/*

Fuente: *lansweeper Cybersecurity Asset Management, (2022)*

Los **controles** permiten mitigar los riesgos en las Mesas de servicios de TI, en conjunto con el plan de tratamiento de norma a partir de la norma ISO 27001:2013 donde se tienen en cuenta los dominios a la cual pertenecen cada uno de los activos con el fin de aplicar controles ya sea como: Requerimiento Legal, obligación contractual, requerimiento del negocio, análisis de riesgo; mitigando las vulnerabilidades que se pueden presentar en la Mesa de Ayuda, por ejemplo[63]: En la **Figura 7** podemos ver los diferente controles operaciones y sus tipos, que permiten adaptar el plan de control dando cumplimiento al lineamiento que solicita la norma.

[63] MINTIC. *Controles de Seguridad y Privacidad de la Información[https://mintic.gov.co/]*se debe implementar con el fin de dar cumplimiento a la política definida [Consulta 14 de marzo de 2016]. Obtenido de https://mintic.gov.co/gestionti/615/articles-5482_G8_Controles_Seguridad.pdf

Figura 6 Controles del Anexo A del estándar ISO/IEC 27001:2013 y dominios a los que pertenece

A.9	Control de acceso		
A.9.1	Requisitos del negocio para control de acceso		Objetivo: Limitar el acceso a información y a instalaciones de procesamiento de información.
A.9.1.1	Política de control de acceso		Control: Se debería establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de seguridad de la información.
A.9.1.2	Política sobre el uso de los servicios de red		Control: Solo se debería permitir acceso de los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente.
A.9.2	Gestión de acceso de usuarios		Objetivo: Asegurar el acceso de los usuarios autorizados y evitar el acceso no autorizado a sistemas y servicios.
A.9.2.1	Registro y cancelación del registro de usuarios		Control: Se debería implementar un proceso formal de registro y de cancelación de registro de usuarios, para posibilitar la asignación de los derechos de acceso.
A.9.2.2	Suministro de acceso de usuarios		Control: Se debería implementar un proceso de suministro de acceso formal de usuarios para asignar o revocar los derechos de acceso a todo tipo de usuarios para todos los sistemas y servicios.
A.9.2.3	Gestión de derechos de acceso privilegiado		Control: Se debería restringir y controlar la asignación y uso de derechos de acceso privilegiado.
A.9.2.4	Gestión de información de autenticación secreta de usuarios		Control: La asignación de la información secreta se debería controlar por medio de un proceso de gestión formal.
A.9.2.5	Revisión de los derechos de acceso de usuarios		Control: Los propietarios de los activos deberían revisar los derechos de acceso de los usuarios, a intervalos regulares.
A.9.2.6	Retiro o ajuste de los derechos de acceso		Control: Los derechos de acceso de todos los empleados y de usuarios externos a la información y a las instalaciones de procesamiento de información se deberían retirar al terminar su empleo, contrato o acuerdo, o se deberían ajustar cuando se hagan cambios.
A.9.3	Responsabilidades de los usuarios		Objetivo: Hacer que los usuarios rindan cuentas por la salvaguarda de su información de autenticación.
A.9.3.1	Uso de la información de autenticación secreta		Control: Se debería exigir a los usuarios que cumplan las prácticas de la organización para el uso de información de autenticación secreta.
A.9.4	Control de acceso a sistemas y aplicaciones		Objetivo: Evitar el acceso no autorizado a sistemas y aplicaciones.
A.9.4.1	Restricción de acceso Información		Control: El acceso a la información y a las funciones de los sistemas de las aplicaciones se debería restringir de acuerdo con la política de control de acceso.

Fuente: *MINTIC, 2016*

Los controles se encuentran establecidos por rangos:

Rango 1: No tiene establecido medidas de seguridad.

Rango 2: Existen algunas medidas, pero no se establece pausa completa ni periodicidad.

Rango 3: Existen series de medidas establecidas, sin un determinado de evaluación.

Rango 4: Se tiene establecido una periodicidad en los controles en un SGSI, junto con evaluación y seguimiento.

Rango 5: Son un factor interno de la empresa que gestiona, las actividades que estén ligadas a su propia organización.

Las empresas lideres de la tecnología y específicamente en las Mesas de Ayuda, validan que tipo de rango de control se requiere para asegurar la Seguridad de la información.

todos estos controles en un SGSI tienen un proceso de ciclo de mejora continua:

- Estándares: La información necesaria para desarrollar la actividad del negocio, donde se pueden ver afectados por diferentes riesgos y amenazas y es necesario prepararse y actuar de inmediato de forma eficaz, estableciendo controles que permitan evaluarlos.

- Directrices: Es dar manejo de la Seguridad de la información de acuerdo a las necesidades de la organización y la legislación vigente, donde se establecen las pautas de gestión para el caso de los incidentes, definiendo responsabilidades.

- Políticas: Corresponde a un documento de utilidad en la organización, donde define las responsabilidades generales y específicas, incluyendo los roles sin indicar las personas concretas dentro de la organización, este documento debe estar completamente actualizado por lo cual es importante que sea revisado y modificado anualmente.[64]

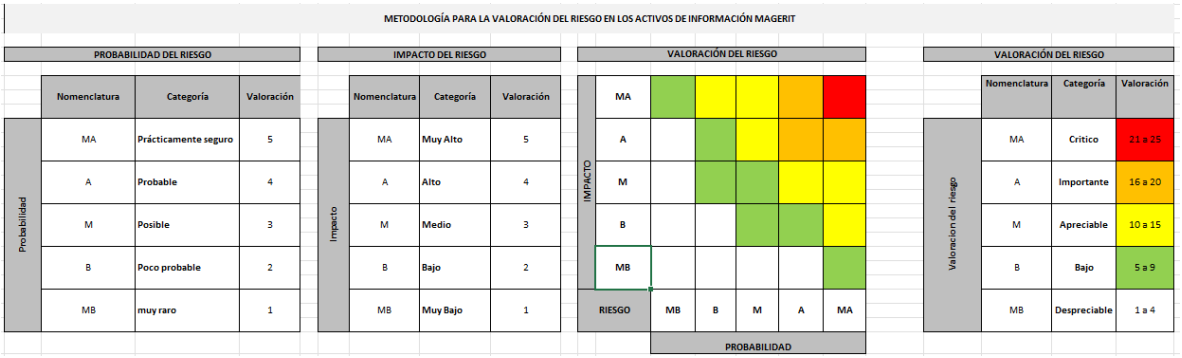
Las medidas de mitigación de riesgos en la Operación, se aplica a partir de los dominios y controles para su aplicación en las vulnerabilidades de los activos, permitiendo verificar el sistema de información, como se puede evidenciar en la **Figura 8,** donde se muestra la matriz de inventario, probabilidades, impacto y valoración de riesgos de los activos de información mediante el uso de la metodología MAGERIT; según la escala de su clasificación se determina el nivel de aceptación de la vulnerabilidad.[65]

---

[64] *Implantación de un SGSI en la empresa* . (s.f.). Obtenido de DIFERENCIA ENTRE ESTÁNDARES, DIRECTRICES, PROCEDIMIENTOS, POLÍTICAS Y NORMAS PARA EL SGSI.

[65] MA*GERIT. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, 2012. [en línea], [consultado en Marzo de 2015.]. Disponible en: http://administracionelectronica.gob.es/pae_Home/dms/pae_Home/documentos/Documentacion/Me todologias-y-guias/Mageritv3/2012_Magerit_v3_libro1_metodo_ES_NIPO_630-12-171-8/2012_Magerit_v3_libro1_m%C3%A9todo_es_NIPO_630-12-171-8.pdf*

Figura 7: Metodología Para la Valoración del Riesgo En Los Activos de Información MAGERIT



METODOLOGÍA PARA LA VALORACIÓN DEL RIESGO EN LOS ACTIVOS DE INFORMACIÓN MAGERIT

PROBABILIDAD DEL RIESGO

	Nomenclatura	Categoría	Valoración
Probabilidad	MA	Prácticamente seguro	5
	A	Probable	4
	M	Posible	3
	B	Poco probable	2
	MB	muy raro	1

IMPACTO DEL RIESGO

	Nomenclatura	Categoría	Valoración
Impacto	MA	Muy Alto	5
	A	Alto	4
	M	Medio	3
	B	Bajo	2
	MB	Muy Bajo	1

VALORACIÓN DEL RIESGO

IMPACTO						
	MA					
	A					
	M					
	B					
	MB					
RIESGO	MB	B	M	A	MA	
PROBABILIDAD						

VALORACIÓN DEL RIESGO

	Nomenclatura	Categoría	Valoración
Valoracion del riesgo	MA	Critico	21 a 25
	A	Importante	16 a 20
	M	Apreciable	10 a 15
	B	Bajo	5 a 9
	MB	Despreciable	1 a 4

Fuente: *Ecu@Risk, Una metodología para la gestión de Riesgos aplicada a las MPYMEs.*

Teniendo en cuenta información anterior las Mesas de Ayuda, deben contar un tratamiento de riesgos que permita realizar monitoreo en los sistemas de información, permitiendo tener un plan de tratamiento de riesgos para aplicación de las vulnerabilidades de cada uno de los activos de la operación.

7 CONCLUSIONES

El presente trabajo se identificaron las metodologías para la gestión de TI, en relación a la atención de eventos o incidentes que se puede presentar en la Mesa de Ayuda, a través de la validación de puntos débiles de su estructura, inicialmente la metodología MAGERIT que permite estudiar los riesgos de los activos, evidenciando los niveles de aceptación según la criticidad de las amenazas y vulnerabilidades y dimensión(autenticidad, trazabilidad, confidencialidad, integridad, disponibilidad) de los activos.

Se identificó las principales metodologías y normas en la gestión de riesgos informáticos, seleccionando la metodología **MAGERIT,** por mejores criterios para la identificación de amenazas y salvaguarda para los diferentes activos, facilitando la gestión en el proceso de atención de eventos o incidentes de Mesa de Ayuda.

Se establece los pasos para gestión de riesgos y mejora en los niveles de atención, por medio de la metodología MAGERIT, permitiendo identificar las amenazas con un plan de identificación y monitoreo, junto con el cumplimiento de los KPIs en Mesa de Ayuda.

Esta metodología ayuda a descubrir y planificar las medidas oportunas, respecto a los incidentes para mantener los riesgos bajo control, adicional prepara a la empresa para procesos de evaluación y auditoria y acreditación para legitimar al sistema respecto a la seguridad.

8 RECOMENDACIONES

Reforzar seguimiento a los eventos o incidentes que se presentan en la Mesa de Ayuda, por medio de la metodología MAGERIT, desde donde se evidencian posibles vulnerabilidades para cada uno de los activos.

Recalcar el monitoreo continuo para el cumplimiento del plan de tratamiento de riesgos, a partir de las buenas prácticas en las Mesas de Servicios (ITIL V4, ISO 27001), documentando cada uno de estos tratamientos en la base de datos de conocimientos.

Analizar riesgos en la mesa de ayuda por medio de controles periódicos, desde herramientas corporativas (CA - Lansweeper) para control de software no autorizados y desactualizados, permitiendo generar plan de acción ante vulnerabilidades.

9 DIVULGACIÓN

El desarrollo del presente proyecto de grado será dado a conocer en colaboración de la biblioteca de la Universidad Nacional Abierta y a Distancia – UNAD, a través de su aplicativo en línea, en donde se publicará un archivo PDF correspondiente al documento final presentado ante los jurados, posterior a la sustentación de este (Si es informe técnico por seminario o créditos de maestría, no tiene jurado); con el fin de que todos los estudiantes de la Universidad que se encuentren interesados en el tema de Metodologías para Gestión de Riesgos, puedan acceder al documento.

BIBLIOGRAFÍA

ABIT TEAMS. (s.f.). *Metodología ITIL:[https://www.ambit-bst.com/] gestión de incidencias y objetivos[Consulta: 17 noviembre del 2021]*. Obtenido de https://www.ambit-bst.com/blog/metodolog%C3%ADa-itil-gesti%C3%B3n-de-incidencias-y-objetivos

ACENSWHITEPAPERS. (s.f.). *"¿Qué es el SLA?"[https://www.acens.com][Sitio Web] Service Level Agreement, traducido como Acuerdo de Nivel de Servicio[Consulta:05 de mayo 2023]*. Obtenido de https://www.acens.com/file_download/176/acens_que_es_el_sla_baja.pdf

ALEMAN NOVOA, E., & RODRIGUEZ BARRERA, C. (22 de octubre de 2015). *Metodologías para el análisis de riesgos en los sgsi*. Obtenido de https://hemeroteca.unad.edu.co/index.php/publicaciones-e-investigacion/article/view/1435

ALEMAN NOVOA, H. A., & RODRIGUEZ BARRERA, C. (16 de mayo de 2014). Metodologías Parael análisisde riesgosenlos sgsi. Obtenido de https://hemeroteca.unad.edu.co/index.php/publicaciones-e-investigacion/article/view/1435/1754. (s.f.).

ALFARO CAMPOS, J. (junio de 2017). Metodología para la gestión de riesgos de TI basada en COBIT 5. Obtenido de https://repositoriotec.tec.ac.cr/bitstream/handle/2238/11060/metodologia_gestion_riesgos_ti_basada_cobit5.pdf?sequence=1&isAllowed=y. (s.f.).

ALFARO CAMPOS, J. (junio de 2017). *Metodología para la gestión de riesgos de TI basada en COBIT 5*. Obtenido de https://repositoriotec.tec.ac.cr/bitstream/handle/2238/11060/metodologia_gestion_riesgos_ti_basada_cobit5.pdf?sequence=1&isAllowed=y

AVALOS SERRANO, V. (2007). Repositorio Institucional de la Universidad de las Fuerzas Armadas ESPE. Obtenido de http://repositorio.espe.edu.ec/handle/21000/2333. (s.f.).

CA Guía de administración. (s.f.). CA Service Desk Manager. Obtenido de https://ftpdocs.broadcom.com/cadocs/0/j027931s.pdf. (s.f.).

Cybersecurity Asset Management [https://www.lansweeper.com/] Get an Asset Inventory That Works for Cybersecurity[Consulta 19 de agosto]Obtenido de https://www.lansweeper.com/use-cases/lansweeper-for-cyber-security/. (s.f.).

DONADO CORONELL, A. (2013). DIAGNOSTICO Y MODELAMIENTO DE LOS PROCESOS DE GESTIÓN DE NCIDENTES Y GESTIÓN DE PROBLEMAS. Obtenido de https://repositorio.cuc.edu.co/bitstream/handle/11323/531/Monograf%C3%ADa%20Trabajo%20de%20Grado-%20Adriana%20Donado.pdf?seq. (s.f.).

DONADO CORONELL, A. (2013). *DIAGNOSTICO Y MODELAMIENTO DE LOS PROCESOS DE GESTIÓN DE NCIDENTES Y GESTIÓN DE PROBLEMAS*. Obtenido de https://repositorio.cuc.edu.co/bitstream/handle/11323/531/Monograf%C3%ADa%20Trabajo%20de%20Grado-%20Adriana%20Donado.pdf?sequence=1

ENIIT. (s.f.). *"Tipos de Hackers". [https://www.campuscyberseguridad.com][Sitio web] bilidades en el manejo de computadoras que investiga un sistema informático. {En linea}. [Consulta:07 de mayo 2023]*. Obtenido de https://www.campuscyberseguridad.com/blog/item/133-tipos-de-hackers

EPHPO. (s.f.). *Control y Mejora continua de los procesos[http://www.ephpo.es/]diseño de un proceso asistencial se describen las etapas necesarias para obtener el mejor resultado[Consulta 2021].* Obtenido de http://www.ephpo.es/Procesos/GUIA_DISENO_MEJORA/5.pdf

FLORENCIA, L, & PAYERO, A. (s.f.). *Riesgos Informaticos [https://sites.google.com/] identificación de activos informáticos,sus vulnerabilidades y amenazas a los que se encuentran expuestos [Consulta: septiembre de 2016]*. Obtenido de https://sites.google.com/site/tecnologiadigital20/home/riesgos-informaticos

GlobalSuite (s.f) ¿Qué es ITIL? [https://www.globalsuitesolutions.com/ [Sitio web][consulta 08 de agosto de 2022]. Obtenido de https://www.globalsuitesolutions.com/es/que-es-itil-y-para-que-sirve/ . (s.f.).

HURTADO, M. (s.f.). *GESTIÓN DE RIESGO METODOLOGÍAS OCTAVE y MAGERIT[http://polux.unipiloto.edu.co/] plantea una gestión [Consulta:2002:].* Obtenido de http://polux.unipiloto.edu.co:8080/00004420.pdf

Implantación de un SGSI en la empresa . (s.f.). Obtenido de DIFERENCIA ENTRE ESTÁNDARES, DIRECTRICES, PROCEDIMIENTOS, POLÍTICAS Y NORMAS PARA EL SGSI.

INCIBE. (s.f.). *¡Fácil y sencillo! Análisis de riesgos en 6 pasos[www.incibe.es]dirigido a reducir los riesgos a los que está expuesta la organización hasta unos niveles aceptables a partir de un análisis de la situación inicial [consulta 16 enero 2017]*. Obtenido de https://www.incibe.es/protege-tu-empresa/blog/analisis-riesgos-pasos-sencillo

ISOTOOLS EXCELLENCE. (s.f.). *"Blog especializado en Sistemas de Gestión".{En línea}. (09 de septiembre de 2021). Metodología OCTAVE para el análisis de riesgos en SGSI. Obtenido de https://www.pmg-ssi.com/2021/09/metodologia-octave-para-el-analisis-de-riesgos-en-sgsi/*.

ISOTools Excellence. (23 de septiembre de 2021). Metodología Mehari para el análisis de Riesgos en SGSI. Obtenido de https://www.pmg-ssi.com/2021/09/metodologia-mehari-para-el-analisis-de-riesgos-en-sgsi/. (s.f.).

KRISTEN, K. (s.f.). *ISACA Publica la Guía COBIT 5 para Aseguramiento[https://www.businesswire.com/] nivel de comodidad en los procesos[Consulta: 30 mayo de 2013]*. Obtenido de https://www.businesswire.com/news/home/20130530005692/es/

Lansweeper. (221). Lansweeper: conozca su tecnología. Obtenido de https://content.lansweeper.com/Branded?utm_source=google&utm_medium=cpc&utm_campaign=Brand&utm_term=Brand&utm_term=lansweeper&utm_campaign=%5BEU%5D+Search+utm_7C+Brand=%204846545452%20y%20h. (s.f.).

Libro I - Método. (s.f.). *Metodología de Análisis y Gestión[Consulta octubre 2012]. Disponible en https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html.*

MAGERIT. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información,. (s.f.).

MALDONADO, D. (s.f.). *¿Qué es la Gestión de Activos de TI?[http://www.icorp.com.mx/][Sitio web]es un conjunto de prácticas de negocios que sostienen el ciclo de vida de la gestión para informar sobre la toma de decisiones estratégicas[Consulta: 5 de Enero de 2019]Disponible en*. Obtenido de http://www.icorp.com.mx/blog/que-es-la-gestion-de-activos-de-ti/

MALWAREBYTES LTD. (s.f.). *"Suplantación de identidad". {En linea}. (phishing)[es.malwarebytes.com]es un método para engañarle y hacer que comparta contraseñas[Consulta: 2021].* Obtenido de https://es.malwarebytes.com/phishing/

MANAGEENGINE. (s.f.). *"¿Qué es la Gestión de Incidentes T": "La gestión de incidentes de TI es uno de los procesos fundamentales de la mesa de ayuda" l[En linea] {23mayo 2022} disponible en: .* Obtenido de https://www.manageengine.com/latam/service-desk/itil-incident-management/que-es-la-gestion-de-incidentes-itil.html

MARCELO, Rivero (s.f) El ransomware es una forma de malware que está en auge[https://es.malwarebytes.com/][Sitio web][Consulta 07 agosto]. Obtenido https://es.malwarebytes.com/ransomware/. (s.f.).

MILVUS. (2021). ¿Cómo aplicar la metodología ITIL en el Help Desk? Obtenido de https://milvus.online/blog/como-aplicar-la-metodologia-itil-en-el-help-desk/. (s.f.).

Ministerio de Hacienda y Administraciones Públicas. {octubre de 201}. MAGERIT v.3 : Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Obtenido de https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog. (s.f.).

Ministerio de Tecnologías de la Información. (11 de junio de 2016). Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información. Obtenido de https://www.mintic.gov.co/gestionti/615/articles-5482_G21_Gestion_Incidentes.pdf. (s.f.).

MINTIC. (s.f.). *¿Qué son las TIC?[https://www.enticconfio.gov.co/que-son-las-tic-significado] son todas las tecnologías que permiten acceder, producir, guardar, presentar y transferir información [Consulta: 17 de mayo de 2017]*. Obtenido de https://www.enticconfio.gov.co/que-son-las-tic-significado

MINTIC. (14 de marzo de 2016). *Controles de Seguridad y Privacidad de la Información*. Obtenido de https://mintic.gov.co/gestionti/615/articles-5482_G8_Controles_Seguridad.pdf

MONA CARDONA, L., & URIBE SERNA, A. (s.f.). *SISTEMA DE GESTIÓN DE INCIDENTES DE SEGURIDAD INFORMÁTICA PARA CORBETA[http://bibliotecadigital.usbcali.edu.co/]a los riesgos [Consuta: 2015].* Obtenido de http://bibliotecadigital.usbcali.edu.co/bitstream/10819/3932/3/Sistema_Gestion_Incidentes_Seguridad_Mona_2015.pdf

NSIT SAS. (s.f.). *Qué es un SOC: Funciones y objetivos principales[https://www.nsit.com.co/][Sitio web]implementar servicios que puedan alertar sobre un ataque venidero e incluso minutos antes de que suceda[consulta 25 febrero]*. Obtenido de https://www.nsit.com.co/que-es-un-soc-funciones-y-objetivos-principales/

Oficina de Seguridad para las Redes Informáticas. (s.f.). METODOLOGÍA PARA LA GESTIÓN DE SEGURIDAD INFORMÁTICA. Obtenido de https://instituciones.sld.cu/dnspminsap/files/2013/08/Metodologia-PSI-NUEVAProyecto.pdf. (s.f.).

OMG. (s.f.). *"Object Management Group. (1997 - 2021)". " Modelo y notación de procesos de negocio del grupo de gestión de objetos". {En línea} Disponible en https://www.bpmn.org/*.

OSPINA DIAZ, M. R. (s.f.). *Desafíos nacionales frente a la ciberseguridad[http://www.scielo.org.co/] En la actualidad los sistemas de información, la[Consultado: 30 de marzo de 2019.]*. Obtenido de http://www.scielo.org.co/pdf/crim/v62n2/1794-3108-crim-62-02-199.pdf

OSPINA DIAZ, M. R. (30 de marzo de 2019). *Desafíos nacionales frente a la ciberseguridad en el*. Obtenido de http://www.scielo.org.co/pdf/crim/v62n2/1794-3108-crim-62-02-199.pdf

OSPINA DIAZ, M. R., & SANABRIA RANGEL, P. E. (26 de noviembre de 2020). Revista Criminalidad. Obtenido de http://www.scielo.org.co/scielo.php?pid=S1794-31082020000200199&script=sci_abstract&tlng=en. (s.f.).

PAE. (s.f.). *electrónica, MAGERIT v.3 : "Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información". {En linea}. {octubre 2012} Obtenido de http://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html*.

PINZON, J. N. (s.f.). *Universidad Piloto de Colombia. {En line}.Metodología para identificación y valoración de riesgos y Salvaguardas en una Mesa de Ayuda[Consultado 2011]. Disponible en chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/http://polux.unipiloto.edu.co:8080/0.*

PLANIFICACIÓN EN ISO 27001, 2022. permitir a las organizaciones identificar, analizar y evaluar sistemáticamente los riesgos de seguridad [Sitio web] [Consultado el 10 de agosto de 2022] Disponible en https://normaiso27001.es/planificacion-en-iso-27001/. (s.f.).

PULIDO, J., & JOHN, B. (23 de diciembre de 2013). RISK ANALYSIS IN SECURITY OFINFORMATION[https://revista.jdc.edu.co/index.php/rciyt/article/download/121/113]. 41;42.

REDES LOCALES Y GLOBALES. (s.f.). *"Protocolo ICMP (Internet Control Messaging Protocol)". {En linea} [https://sites.google.com/site/redeslocalesyglobales] definido en el RFC 792, sirve para informar de sucesos que han ocurrido en la red [Disponible en: 27 de mayo de 2015]*. Obtenido de https://sites.google.com/site/redeslocalesyglobales/6-arquitecturas-de-redes/6-arquitectura-tcp-ip/9-protocolos-tcp-ip/protocolos-de-nivel-de-red/protocolo-icmp

REDES LOCALES Y GLOBALES. (s.f.). *"Protocolo ICMP (Internet Control Messaging Protocol)".{En línea}. {27 julio 2015} disponeble en:* . Obtenido de https://sites.google.com/site/redeslocalesyglobales/6-arquitecturas-de-redes/6-arquitectura-tcp-ip/9-protocolos-tcp-ip/protocolos-de-nivel-de-red/protocolo-icmp

RIVERO, M. (s.f.). *¿QUÉ ES EL PHISHING. " ¿Qué tipo de información roba?". {En linea}. [https://www.infospyware.com/][Consulta:08 de agosto].Obtenido de https://www.infospyware.com/articulos/que-es-el-phishing/]*.

RODIGUEZ, P. (s.f.). *"Riesgos informáticos"[https://www.ambit-bst.com][Sitio Web]el análisis de riesgos informáticos es la evaluación de los distintos peligros que afectan a nivel informático. {En linea} [Consulta: 07 de mayo 2023]*. Obtenido de https://www.ambit-bst.com/blog/an%C3%A1lisis-de-riesgos-inform%C3%A1ticos-y-ciberseguridad

SALVARENGA. (s.f.). *"La Gestión De Eventos Y Su Relación Con Otras Practicas De ITIL". {En linea}[https://blog.agrega.com/][Sitio Web]gestión de eventos[consulta 21 diciembre 2020].* Obtenido de https://blog.agrega.com/itsm/la-gestion-de-eventos-y-su-relacion-con-otras-practicas-de-itil/#:~:text=El%20prop%C3%B3sito%20de%20la%20gesti%C3%B3n,en%20la%20gesti%C3%B3n%20de%20servicios.

SEGURIDAD 7 "A" . (s.f.). *Metodología CORAS (COnstruct a platform for Risk Analysis of Security critical system)*. Obtenido de http://seguridades7a.blogspot.com/p/coras.html

SEGURIDAD 7 "A" . (s.f.). Metodología CORAS (COnstruct a platform for Risk Analysis of Security critical system). Obtenido de http://seguridades7a.blogspot.com/p/coras.html. (s.f.).

SONDA S.A. . (s.f.). *SOPORTE DE INFRAESTRUCTURA SERVICEDESK. [en línea] El Servicedesk de SONDA opera como un único punto de contacto que resuelve de forma oportuna incidentes de servicios de TI[consulta: 2021] Disponible en: .* Obtenido de https://www.sonda.com/content/uploads/2018/12/ServiceDesk.pdf

TECNOLOGIA+INFORMATICA. (s.f.). *"¿Qué es el DNS?". El sistema de nombres de dominio, más comúnmente conocido por sus siglas en inglés como Domain Name System o DNS. {En linea}. {Junio 2021}*. Obtenido de https://www.tecnologia-informatica.com/que-es-dns/

TECNOLOGÍA+INFORMÁTICA. (s.f.). *¿Qué es el DNS? [tecnologia-informatica.com] DNS es un conjunto de grandes bases de datos distribuidas en*

servidores de todo el mundo [Consulta: 2021]. Obtenido de https://www.tecnologia-informatica.com/que-es-dns/

TENABLE. (s.f.). *"Proteja su Active Directory e interrumpa las rutas de ataque" {En linea}. [es-la.tenable.com/]vulnerabilidades dentro de sus dominios de Active Directory[Consulta:2022].* Obtenido de https://es-la.tenable.com/products/tenable-ad?utm_campaign=gs-{16816557316}-{134801193745}-{591911499268}_00023798_fy22&utm_promoter=tenable-ad-nb-00023798&utm_source=google&utm_term=ataques%20de%20ciberseguridad&utm_medium=cpc&utm_geo=latam&gclid=EAIaIQo