DEBILIDADES EN LA ADMINISTRACIÓN DE LAS PLATAFORMAS INFORMÁTICA QUE EXPONEN LA SEGURIDAD DE LA INFORMACIÓN SENSIBLE EN LAS ORGANIZACIONES.

DIANA GÓMEZ MARTÍNEZ
VICTOR ALFONSO LÓPEZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
BOGOTÁ
2018

DEBILIDADES EN LA ADMINISTRACIÓN DE LAS PLATAFORMAS INFORMÁTICA QUE EXPONEN LA SEGURIDAD DE LA INFORMACIÓN SENSIBLE EN LAS ORGANIZACIONES.

DIANA GÓMEZ MARTÍNEZ
VICTOR ALFONSO LÓPEZ

MONOGRAFÍA

DIRECTOR: MARIANO ESTEBAN ROMERO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
BOGOTÁ
2018

Las ideas y contenido expresados en el presente documento son de exclusiva responsabilidad de sus autores y no comprometen la ideología de la Universidad Nacional Abierta y a Distancia UNAD

Nota de Aceptación

_____

_____

_____

_____

_____

_____

Firma presidente del Jurado

_____

Firma del Jurado

_____

Firma del Jurado

CONTENIDO

pág.

LISTA DE FIGURAS

pág.

LISTA DE ANEXOS

pág.

INTRODUCCIÓN

Por medio de la presente monografía se busca realizar el análisis de la gestión de la administración de las plataformas de seguridad abordándolo desde el punto de vista de algunos funcionarios del área de seguridad de algunas organizaciones consultadas del sector petrolero, salud, financiero y telecomunicaciones, lo cual permitirá conocer el estado actual de la protección de la información sensible, por lo anterior se busca identificar posibles fallas o capacidades de mejoramiento para brindar recomendaciones que logren mitigar este hecho.

Se analizará la continuidad de las configuraciones de las plataformas, su mantenimiento y ajuste para mejorar la seguridad de la información sensible de la organización, así mismo el seguimiento, controles y plan de mejoramiento continuo.

Muchas organizaciones en Colombia protegen la información sensible dada la regulación a la cual están sujetas, como puede ser la circular de la superintendencia financiera (la cual regula los requerimientos de seguridad de las entidades que realizan transacciones financieras en el país), ley de protección de datos personales (la ley 1581 de 2012 establecida para proteger la información personal de los usuarios o clientes de las organizaciones), normatividad internacional como PCI (protección de información financiera como tarjetas de crédito y sus transacciones), HIPAA (protección de historial médico de los pacientes), SOX (control de las modificaciones realizadas a la información manteniendo sus registros y velando por el control en su publicación), entre otras, las cuales son exigidas a cada organización según su actividad económica, manejo de información o vínculos comerciales que tengan, para esto las organizaciones realizan inversiones en herramientas de auditoría y protección de la información, estas son adquiridas a empresas fabricantes o distribuidoras de estos productos, quienes implementan y entregan los parámetros básicos, dejando la continuidad, ajuste y parametrización en manos de la organización

1. PLANTEAMIENTO DE PROBLEMA

1.1 DESCRIPCIÓN DEL PROBLEMA

A nivel mundial, existen grandes organizaciones que ofrecen soluciones de seguridad, sin embargo, cada día las amenazas avanzan y las soluciones intentan alcanzarlas, generando nuevas funcionalidades, integraciones, módulos, complementos, entre otros, con el objetivo de brindar un buen servicio con un buen producto a sus clientes.

En el momento de adquirir las plataformas en la mayoría de los casos, se realizan las mejores prácticas de despliegue, realizando el levantamiento de información de acuerdo a las necesidades de cada organización para así lograr la implementación idónea de cada solución; desde un antivirus, soluciones perimetrales, hasta herramientas de protección específica para servicios Core del negocio; sin embargo en diferentes ocasiones durante la operación, después de realizada la implementación no se mantienen las recomendaciones del diseño inicial, durante las tareas realizadas a diario se requiere la asignación de permisos o excepciones que van cambiando estas configuraciones iniciales y deja brechas de acceso que se convierten en grandes riesgos de seguridad de la información.

Por otro lado, una organización al adquirir una solución de seguridad se puede exponer a un nuevo desafío, dado que al presentarse nuevos dispositivos en su red de datos se requiere capacitar a sus ingenieros administradores los cuales cuentan con la responsabilidad de mantener al día la plataforma para proteger la información sensible de la organización ante nuevas amenazas, aplicando recomendaciones de fabricantes de las diferentes soluciones implementadas y actualizando las versiones que sean necesarias.

Generalmente los ingenieros administradores de las plataformas de seguridad no cuenta con el tiempo suficiente para corregir y/o continuar con las configuraciones de seguridad recomendadas o ideales para su organización, las cuales en muchas ocasiones deben contratar servicios con empresas externas para que les ayuden a evaluar sus condiciones de seguridad y les entreguen estrategias de configuración, procesos, capacitación, entre otros, generando recomendaciones para mejorar su estado de seguridad actual, ya sea con el perfilamiento, ajuste de las herramientas actuales o adquiriendo nuevas.

Por lo anterior, se desarrolla la presente monografía, con la intención de entender el punto de vista de las organizaciones analizadas y poder generar

recomendaciones de buenas prácticas que permitan llevar a las compañías al mejor uso de sus plataformas, conociendo los puntos básicos en protección de la información y dándole a conocer las fallas comunes que se pueden presentar. Esto permitirá realizar de manera rápida la autoevaluación de sus dispositivos de seguridad y ejecutar un plan de remediación a corto, mediano y largo plazo.

1.2 FORMULACIÓN DEL PROBLEMA

Las organizaciones en Colombia de diferentes sectores de operación, como gobierno, financiero, educación, entre otros, se preocupan por la protección de su información sensible, así mismo se encuentran obligadas a cumplir con la regulación vigente, como puede ser la circular de la superintendencia financiera (la cual regula los requerimientos de seguridad de las entidades que realizan transacciones financieras en el país), ley de protección de datos personales (la ley 1581 de 2012 establecida para proteger la información personal de los usuarios o clientes de las organizaciones), normatividad internacional como PCI (protección de información financiera como tarjetas de crédito y sus transacciones), HIPAA (protección de historial médico de los pacientes), SOX (control de las modificaciones realizadas a la información manteniendo sus registros y velando por el control en su publicación), entre otras, por lo tanto, realizan inversiones en infraestructura tecnológica para protección de su información sensible, la cual puede ser datos del negocio, transacciones financiera, protección de datos personales de sus clientes o de sus empleados; sin embargo, en la operación de estas herramientas se encuentran varias falencias, es decir las organizaciones adquieren herramientas de seguridad, pero los riesgos siguen existiendo por fallas en las configuraciones, desconocimiento de administración y gestión poco proactiva de las plataformas. Lo anterior representa grandes riesgos en la seguridad de la información, dado que cualquier mala configuración representa una puerta abierta para los atacantes y las infecciones o incidentes de seguridad.

La presente monografía está enfocada a realizar la investigación referente a la problemática presentada en las organizaciones con grandes inversiones en solución de seguridad, pero que cuentan con problemas de administración y malas configuraciones o procesos de gestión inadecuados por ser reactivos y no proactivos.

Lo anterior nos lleva a cuestionar ¿Cuáles son las principales debilidades en la gestión y/o administración de plataformas de seguridad que representan un riesgo para la información sensible de las organizaciones?

1.3 OBJETIVOS

1.3.1 Objetivo general

Analizar el estado actual de las plataformas de seguridad de la información en las organizaciones consultadas para lograr el reconocimiento de las debilidades en la gestión y configuración de los dispositivos encargados de la protección de la información sensible.

1.3.2 Objetivos específicos

- Identificar el sector y tamaño de las organizaciones analizadas, así como los cargos o roles de las personas de acuerdo con las respuestas obtenidas.
- Evidenciar los aspectos críticos en la gestión y/o administración de plataformas de seguridad de cada una de las organizaciones consultadas.
- Identificar los procedimientos ejecutados y controles en las configuraciones de cada una de las plataformas de seguridad, de acuerdo con la información recolectada.
- Realizar análisis de los problemas detectados en la gestión y/o administración de las plataformas de seguridad encargadas de la protección de la información sensible, con la información obtenida.
- Generar recomendaciones de buenas prácticas que permitan mejorar la seguridad para proteger la información sensible de la organización.

1.4 JUSTIFICACIÓN

Las organizaciones realizan grandes inversiones en herramientas de seguridad informática, el objetivo es evitar ser víctima de ataques informáticos, prevenir la fuga de información y cualquier incidente de seguridad que ponga en riesgo la operación de la organización o su información sensible, así mismo se encuentran obligados por la ley para proteger la información, contar con controles y auditorias de acceso y la evaluación de riesgos para mitigarlos.

Por lo anterior es importante para las organizaciones revisar las configuraciones de sus plataformas y establecer procedimientos proactivos para el aseguramiento de la información sensible, esto generará conciencia en la inversión de soluciones junto con procesos y estrategias para protección de la información de manera eficiente sin tener que esperar a tener un incidente de seguridad o que un tercero les ayude en este proceso.

Al realizar la implementación de manera adecuada, las organizaciones podrán evitar riesgos de incidentes de seguridad, fuga de información sensible y en algunos casos evitar la inversión de otras soluciones de seguridad complementarias, dado que al optimizar las actuales podrían mantener segura su información.

1.5 ALCANCE Y DELIMITACIÓN

La presente monografía tiene como base las actividades de investigación realizada por los estudiantes de acuerdo con la documentación encontrada relacionada con el análisis de la gestión de las plataformas de seguridad y su posibles inconvenientes que expongan la información sensible, en donde se analizarán los estudios previamente ejecutados, documentación relacionada y otros, así mismo se generará un instrumento de recolección de información que será compartido a algunos funcionarios de organizaciones seleccionadas (máximo 5), del sector petrolero, salud, financiero y telecomunicaciones, con formato de encuesta para realizar el levantamiento de información requerido, posteriormente se desarrollará el documento que busca analizar las fallas o problemas detectados en la gestión de las plataformas y las recomendaciones del análisis ejecutado.

2. MARCO DE REFERENCIA

En este capítulo se realizará un recorrido sobre los conceptos a tener a cuenta para el desarrollo de la monografía. En primera instancia, se busca determinar conceptos inherentes al tema, como lo es la seguridad informática enfocada a la protección de la información, vulnerabilidades, fenómenos, amenazas comunes, normatividad, auditoria, fallas comunes en la administración de dispositivos de seguridad y herramientas de seguridad informática.

2.1 ANTECEDENTES

La seguridad informática evoluciona cada día, sin embargo, es indispensable identificar los trabajos previamente realizados, los cuales permitirán establecer bases sólidas para el desarrollo del trabajo de investigación, para ello, se han revisado varios trabajos similares de investigación o desarrollo de contenidos que buscan mejorar las estrategias o herramientas de seguridad en las organizaciones.

CONCIENCIACIÓN EN SEGURIDAD DE LA INFORMACIÓN, LA ESTRATEGIA PARA FORTALECER EL ESLABÓN MÁS DÉBIL DE LA CADENA, por Víctor Enrique Martínez Saravia, Bogotá D.C., Colombia, enero de 2010.

En la cual el autor propone una solución a los dentro de una compañía para sus dificultades en seguridad de la información, pretende adquirir al interior actividades de concienciación y sensibilización implementando buenas prácticas para los usuarios dentro de sus actividades cotidianas, generando interés en la protección de los activos de la organización que administran, así mismo velar por los riesgos que se tienen digitalmente que sean representativos frente a sus competidores.

El autor concluye que la cultura es la base fundamental para llegar al éxito en la protección de la información, identificando las practicas necesarias para alinearse con los requerimientos de la organización, así mismo, se requiere que la organización no solo defina las políticas de protección, sino que las publique y socialice haciendo participe a todos los funcionarios.

ANÁLISIS DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN, por Juan Manuel Matalobos Veiga, Madrid, España, mayo 2009

El cual consiste en la evaluación a nivel de seguridad de la información de los riesgos que tengan, lo cual permitirá medir y comparar de acuerdo con los controles

implementados si los requerimientos cumplen a satisfacción con las medidas tomadas.

Por medio de este análisis, se evidencian adicional de las diferentes metodologías para analizar los riesgos, la importancia de tener establecido un radar de riesgos en la organización, que permita estableces los controles necesarios para garantizar la seguridad de la información, contando con esta base es posible identificar la manera correcta de diseñar y proteger la infraestructura tecnológica.

PLAN DE SEGURIDAD INFORMÁTICA, por María Dolores Cerini y Pablo Ignacio Prá, Córdoba, Argentina, octubre 2002

Los autores pretenden promover la implementación de un modelo de seguridad en la organización, identificando las vulnerabilidades existentes en los controles de seguridad de la información dentro de la organización.

Se concluye que disponer de una política de seguridad es importante, pero más allá de ello, se requiere fomentar su uso entre los usuarios, dado que es un desafío su implementación y requiere el apoyo de todos los miembros de la organización, de esta forma, el plan de acción preventivo y correctivo para incidentes de seguridad tendrá el apoyo de un mayor número y no solo del oficial de seguridad o su grupo de TI.

SEGURIDAD EN INFORMÁTICA, por Luis Daniel Álvarez Basaldúa, Ciudad de México, México, abril 2005

El autor establece una política de seguridad, teniendo en cuenta las auditorías y controles necesarios para medir los riesgos presentes y la probabilidad que tienen, así mismo, incorporando a los usuarios para que apoyen en la mitigación de los incidentes, evitando se manifiesten.

Se concluye que es necesario realizar trabajos de auditoria de forma periódica, para garantizar que la seguridad de la red corporativa y la seguridad de la información sensible son óptimas, el continuo cambio de configuraciones, adquisición de nuevas soluciones o actualizaciones requieren revisiones para garantizar el óptimo funcionamiento

PROPUESTA SEGURIDAD DE LA INFORMACIÓN, por Fernando Bugarini Hernández, Ciudad de México, México, noviembre 2007.

El autor realizó un diagnostico aplicando un FODA, analizando diferentes escenarios de riesgos en los que se puede situar una empresa, identificando la falta de seguridad en los datos sensibles.

Se concluye que muchos de los ataques son dirigidos contra el cliente y no contra el propio sistema, dado que es el más vulnerable, luego del análisis se obtuvo un panorama identificando como se conforma la organización en sus sistemas de información, lo cual permite identificar los riesgos y con ello el plan de acción idóneo para contrarrestarlos.

2.2 MARCO TEÓRICO CONCEPTUAL

2.2.1 Seguridad Informática

El concepto de Seguridad informática se ha consolidado desde que el internet se convirtió en un medio de interconexión global ya que los incidentes relacionados con sistemas informáticos se han incrementado de manera exponencial. El objetivo principal de la seguridad informática es proteger los recursos informáticos valiosos para la organización, como son el hardware y el software, esto con el uso de estrategias adecuadas para la protección del activo más importante que es la información, Según Garfinkel y Spafford (1999) en Seguridad y comercio en el web " *La seguridad en el web es un conjunto de procedimientos, prácticas y tecnologías para proteger a los servidores y usuarios de la web y las organizaciones que los rodean. La seguridad es una protección contra el comportamiento inesperado*"

Todos en la red se encuentran expuestos a distintos tipos de ataques informáticos, algunos pueden simplemente afectar el sistema o quitar el acceso a recursos de internet, sin embargo, otros van más allá, en donde se llega a afectar con el robo de información confidencial, datos personales, información financiera, registros de tarjeta de crédito, entre otros, que pueden generar pérdidas de grandes sumas de dinero, detrás de estos últimos se encuentran los delincuentes informáticos

El internet hace posible la comunicación de millones de redes y así mismo de millones de usuarios dónde se pueden infiltrar hackers, se puede plantear que internet es una red de dos sentidos dónde en esta época las organizaciones lo utilizan para distribuir información importante y realizar sinnúmero de transacciones comerciales, para todo este tipo de comunicaciones se requiere protección así que una de los valores más importantes de la Seguridad informática es hacer implementar un conjunto de medidas preventivas ante un incidente o desastre ya que es menos traumático para una organización prevenir un incidente que recuperarse del mismo.

Cuando se produce un incidente de seguridad, es decir, cuando se materializa una amenaza, se produce una pérdida que es necesaria valorar, es allí donde toma importancia la clasificación y la naturaleza de las posibles pérdidas, ya que estas pueden ser bastante graves llegando a producir daños irreparables. (Melían, 2011)

"Estadísticas recientes indican que una de cada tres empresas ha tenido un incidente de seguridad grave en un plazo máximo de 2 años que han causado grandes pérdidas para las corporaciones". Pérdidas que pueden ser de diferente naturaleza, tales como:

- Materiales: daños de recursos informáticos, robos de los mismos, entre otros.
- Alteraciones de la normalidad: retrasos en procesos que generan pérdidas de ingresos.
- Pérdidas de integridad: alteraciones de archivos y programas.
- Salidas indeseadas: Robo de datos e información importante.

Además de las pérdidas anteriormente definidas, existen muchos más daños lógicos y humanos, que hacen que esta tipificación no sea única, por lo que también se utilizan otras clasificaciones con base a su magnitud.

2.2.2 Fenómenos y Amenazas Comunes

Según el diccionario (Ibarra, 1980) análisis es: *"un estudio detallado de una distinción o separación de las partes de un todo hasta llegar a conocer los principios o elementos de este".* La vulnerabilidad (Ibarra, 1980) es definida como: *"la incapacidad de resistencia cuando se presenta un fenómeno amenazante".* A través de un análisis de este tipo se puede definir el estado de un sistema o conjunto de ellos, permitiendo detectar oportunamente las debilidades existentes para priorizarlas y remediarlas eficazmente, por lo que se define el análisis de vulnerabilidad en nuestro caso como el estudio detallado de la red con el fin de conocer las incapacidades que se presentan ante cualquier fenómeno amenazante que pueda poner en peligro el sistema.

(Markus, 2009) *"Un fenómeno amenazante es la posibilidad de ocurrencia de cualquier tipo de evento o acción que puede producir un daño sobre los elementos de un sistema",* en el caso de la seguridad en informática hablamos tanto de elementos físicos como lógicos, generados por accesos no autorizados, ataques a sistemas informáticos, entre otros:

La primera amenaza y más conocida se centra en los Virus informáticos que se suelen conocer. (Vergara, 2011) *"Un virus no es más que un programa codificado con la intención de alterar el correcto funcionamiento del sistema"*, es decir es un

programa que se aprovecha de las inseguridades de los servidores con el fin de alterar su funcionamiento, es necesario aclarar que las infecciones de Virus no se ejecutan por sí solas, necesitan ejecutarse junto a otra aplicación para poder distribuirse por nuestro computador.

Los dispositivos de almacenamiento extraíbles son medios de uso común que suelen infectar nuestros computadores, como: Memorias USB, CD-Roms, entre otros.

Los Troyanos o caballos de troyanos (Ximo as, 2012) *"son fragmentos de software hostil que actúan como servidores ocultos, permitiendo a los intrusos asumir el control de un equipo remoto sin conocimiento del propietario"*. Es decir, los troyanos se instalan como programas ocultos, infectando el computador por medio de conexión sin permiso, que pueden ser evitadas por medio de la activación del Firewall y el Antivirus.

Las Bombas Lógicas (Vergara, Blog informático, 2010). *"son programas ocultos en la memoria del sistema o en los discos, en archivos ejecutables con extensión .com o .exe y que espera una fecha para realizar la infección"* es decir son virus programados que se ejecutan cuando el usuario utiliza alguna aplicación como Messenger.

Los Gusanos o Worms tienen como objetivo hacer copias de su misma información en el computador ocasionando lentitud en el procesamiento. Spyware según (Castro, 2010) *"Es un programa que se instala en el computador, usualmente con el propósito de recopilar y enviar información, que puede ser de tus datos personales"*. El objetivo de este tipo de virus es espiar las aplicaciones en las que se ingresan datos importantes como números de cuentas bancarias, claves, números de documentos, entre otros.

Los hoax no están relacionados dentro de los virus porque no tienen la capacidad de reproducirse por sí solos, pero se manifiestan en forma de cadenas que suelen apelar a los sentimientos como, por ejemplo: Ayuda a buscar un niño desaparecido o víctima de cáncer.

El Spam es el correo electrónico no deseado que satura la bandeja de entrada, el cual suele ser en su mayoría mensajes publicitarios.

El Phishing son los mensajes de correo electrónico que suplantan organizaciones, como por ejemplo bancos, donde es solicitado ingresar datos personales.

Anteriormente solo se mencionan algunas de las amenazas informáticas más comunes y perjudiciales, ya que no se puede definir una cantidad exacta existente porque han llegado a aumentarse de forma considerable, de tal manera que pueden ser clasificables por características como: forma de ataque, modo de operación, medios de utilización, entre otros.

2.2.3 Normatividad

El uso y seguimiento de la normatividad constituye una medición de la seguridad de la información, por lo que el sistema de gestión de la seguridad de la información ayuda a evaluar e identificar los procesos o normas ineficaces del mismo, reasignando prioridades y tomando acciones sobre los controles aplicados. Cabe aclarar que el objetivo de la norma se fundamenta en el fortalecimiento de la institución y proporciona información fiable a la entidad sobre los riesgos que corre en relación con la seguridad de información

La normativa ISO/IEC 27004 lleva como nombre (IsecT, 2012) *"Information technology – Security techniques – Information security management – Measurement, cuya traducción en español sería ISO / IEC 27004 Tecnología de la información - Técnicas de seguridad-Gestión de la seguridad de la información – Medida."* Normatividad basada en la serie de normas ISO27000 que se produjo como complemento de la norma ISO 27001, pretendiendo comprobar la efectividad de un SGSI (Sistema de Gestión de la Seguridad de la información) a través de controles medibles, es decir, la norma ISO/IEC 27004 es aplicada a través de una serie de controles que revisan procesos, objetivos, planeaciones, políticas y procedimientos que se llevan a cabo dentro de una organización con el fin de realizar y mantener un SGSI adecuado, detectando así, si uno de los procesos o controles necesitan ser modificados o mejorados, es muy importante para los profesionales de seguridad de la información tener en cuenta las recomendaciones y controles establecidos para asegurar los activos sensibles de la organización

3. METODOLOGIA DE DESARROLLO

Para la realización de la monografía, inicialmente se describen las características y las fases que determinan su desarrollo. En un primer momento se establecen las categorías de análisis, construidas a partir del marco teórico, seguido a esto, se presenta el instrumento de recolección de datos el cual es una encuesta realizada a un ingeniero administrador de infraestructura de seguridad de diferentes organizaciones.

Teniendo en cuenta que el objetivo principal de esta monografía es analizar el estado actual de las plataformas de seguridad de la información en algunas organizaciones del sector petrolero, salud, financiero y telecomunicaciones para identificar las fallas en configuración de los equipos que protegen la información sensible, es primordial, conocer el estado de las diferentes redes administradas por los ingenieros, estos datos se recolectan para realizar el respectivo análisis.

3.1 FUENTES DE INFORMACIÓN

Una vez identificada la situación problema, se realizó una búsqueda de las investigaciones y trabajos adelantados en torno a nuestro problema. Es importante mencionar que se encontraron trabajos que abordan optimización y mejoramiento en cuanto diseño de red, sin embargo, no existen evidencias de trabajos que enfaticen en problemas de administración y malas configuraciones.

Así mismo, se construyó el marco teórico de la investigación, con el cual se establecieron las categorías de análisis y permitió dar luz al diseño de la encuesta, teniendo en cuenta los aspectos importantes de una red segura y bien administrada.

Hernández, Fernández y Baptista (2003) señalan que la integración de los dos métodos: “agrega complejidad al diseño de estudio; pero contempla todas las ventajas de cada uno de los enfoques”. (p. 21); de igual manera, según Flick (2002) “la perspectiva cualitativa y cuantitativa se complementan mutuamente en el estudio de un problema; esta complementación se concibe como la compensación de los puntos débiles y ciegos de los métodos. (Jick, 1983)” (p.280).

La perspectiva cualitativa busca establecer no solo la manera cómo se enfocan los problemas, sino también la forma cómo se buscan las respuestas a los mismos, lo que propicia el análisis que se quiere llevar a cabo dentro de la investigación. Es

por ello que para el desarrollo de este trabajo la perspectiva cualitativa será de tipo descriptiva y exploratoria.

Hernández et al. (2003), citando a Danke, afirman que los estudios descriptivos "(…) buscan especificar las propiedades, las características y los perfiles importantes de personas, grupos comunidades o cualquier otro fenómeno que es sometido a un análisis" (p. 117). En nuestro caso, permite establecer elementos del contexto, descripción de la población y estado actual de la administración de las plataformas.

Ahora bien, considerando que no se han encontrado propuestas que a partir del análisis permitan conocer los procedimientos y configuraciones de cada una de las plataformas de las organizaciones la investigación es de tipo exploratoria, pues como lo sustenta Sabino (1994) "en el enfoque exploratorio el tema escogido ha sido poco estudiado hasta el momento y no existe sobre el mismo un conocimiento tal que permita formular hipótesis precisas".

Dentro de la perspectiva cualitativa se procedió por medio de un estudio de caso, que según Sabino (1994) "la nota particular de este diseño la constituye el estudio profundizado y exhaustivo de uno o muy pocos objetos de investigación, lo que permite obtener un conocimiento amplio y detallado del mismo" (p. 80). Así, la aplicación a mínimo 1 (un) ingeniero de 5 (cinco) diferentes organizaciones consultando su estado actual de configuración de las plataformas de seguridad y consultándoles acerca de la problemática base de este proyecto.

3.2 FASE DE RECOLECCIÓN DE INFORMACIÓN

Es el punto de partida de la observación realizada, que se caracteriza por explicitar y precisar que es lo que se va a analizar y por qué, en este primer momento se identificó como una situación problema (Planteamiento del problema) que las organizaciones con grandes inversiones en seguridad cuentan con problemas de administración y malas configuraciones o procesos de gestión inadecuados por ser reactivos y no proactivos. Como insumo de indagación se darán las entrevistas a administradores, analistas, consultores y directivos encargados de la seguridad de la información de las organizaciones escogidas.

3.2.1 Instrumento de recolección de información.

Para el diseño de la encuesta se tuvo en cuenta las categorías de análisis determinadas en el marco teórico. El instrumento cuenta con veinte preguntas.

El levantamiento de información se realiza a través de un formulario de Google, en el cual se creó una encuesta que fue compartida por los contactos del área de tecnología o directivos de las organizaciones objetivo. La encuesta generada se observa en el Anexo C y se encuentra en el enlace siguiente:

https://goo.gl/forms/kMEqEHY7ZVHVgq4p2

3.2.2 Población y muestra.

Para el desarrollo del proyecto se realizará el estudio de documentación actual existente y entrevistas a mínimo 1 (un) ingeniero de 5 (cinco) diferentes organizaciones consultando su estado actual de configuración de las plataformas de seguridad y consultándoles acerca de la problemática base de este proyecto, para identificar sus puntos de vista, sus estrategias y procedimientos para mejorar las configuraciones de sus plataformas, los datos recolectados servirán de insumo para la elaboración de resultados encontrados y brindar un punto de vista personal como profesionales en seguridad informática, así mismo con recomendaciones generales para implementar procesos que permitan establecer revisiones para control de seguridad de información sensible.

La monografía desarrollada permite obtener resultados basados en una encuesta realizada a varias personas de diferentes organizaciones con un perfil técnico idóneo para el análisis; dentro de los resultados obtenidos se identifica:

- Sector de las organizaciones encuestadas.
- Cada uno de los aspectos críticos identificados en las organizaciones consultadas, por medio de la información suministrada en la encuesta.
- Los procedimientos existentes en las configuraciones de las plataformas de seguridad o los puntos de vista referentes a este proceso.
- Identificación de los problemas detectado en las organizaciones consultadas, encontrando la causa de estas y sus posibles fuentes, para identificar el plan de acción de mejora.
- Finalmente, se establecen recomendaciones de mejora para establecer prácticas y/o controles que mejoren la seguridad de la información sensible.

La información obtenida a través del instrumento de recolección diseñado, permite identificar el tipo de público que la responde, en la cual se identifica el perfil del encuestado, su rol en la compañía, así como el sector en el cual la organización se encuentra, la encuesta diseñada para el levantamiento de información, fue enviada a ingenieros de diferentes organizaciones que trabajan en el área de seguridad informática, de acuerdo con las respuestas obtenidas, los siguientes son los cargos de los encuestados.

- Consultor Especialista
- Coordinación de Seguridad de la Información
- Administrador en Seguridad de la información
- Analista de Seguridad
- CISO
- Profesional Especialista en seguridad
- Director de Seguridad
- Analista de Ciberseguridad

3.3 FASE DE ANÁLISIS DE DATOS

Una vez obtenidos los insumos con la aplicación de la encuesta, se realizará la clasificación y sistematización de los datos, a partir de las categorías propuestas, con los resultados se efectuará el análisis para obtener la descripción más detallada de la administración de los dispositivos por parte de los ingenieros encargados de las organizaciones.

El análisis de la información requiere conocer el contexto de cada una de las respuestas, así como de la muestra en general, por ello es importante conocer el cargo de la persona encuestada, sus funciones, tiempo trabajando en dicha compañía y perspectivas frente a la seguridad de la información de la organización, de igual manera, se requiere identificar el tamaño de la empresa y el nivel de madurez frente a la gestión de las herramientas de seguridad de infraestructura y protección de información sensible.

Cada respuesta sistematizada permitirá conocer a nivel general y particular el estado de la seguridad y gestión o configuración de las herramientas de protección de la infraestructura e información sensible de la organización, esto ayudará el análisis de factores en común o comportamientos frecuentes que sirvan de insumos en el desarrollo de recomendaciones de acuerdo con los hallazgos encontrados.

La información obtenida permitirá evidenciar el estado de seguridad según las personas encuestadas dentro de sus organizaciones, se pretende entender de forma general el nivel de madurez que tengan, tanto a nivel de herramientas como de su gestión, será de gran importancia identificar el nivel de madurez de configuraciones que tengan y si se han llevado a cabo procesos de mejoramiento continuo o por el contrario se ha evidenciado malas prácticas de administración.

Dentro del análisis de información se evidenciará el estado de procedimientos y buenas prácticas establecidas en la gestión de plataforma, para ellos se realizarán consultas enfocadas a las actividades de gestión frente a configuraciones, revisiones periódicas, actividades de mantenimiento, entre otras que puedan llevar a identificar parámetros de procesos de las organizaciones establecidos y su cumplimiento que permitan mejorar su nivel de seguridad informática.

3.4 FASE GENERACIÓN DE RECOMENDACIONES

Después de realizar la recolección de la información solicitada en la encuesta y analizar los datos se pretende dar recomendaciones útiles enfocadas a las mejores prácticas, esto se realiza teniendo en cuenta tres grupos; protocolos, accesos y gestión.

Las recomendaciones enfocadas a protocolos buscarán sugerir la mejor manera para establecer sesiones entre diferentes dispositivos, teniendo en cuenta protocolos seguros que no están siendo usados o no se han implementado de la mejor manera.

Para todas las organizaciones donde existan dispositivos de red es importante garantizar que al momento de ser gestionados tengan un acceso seguro, es clave tomar una serie de medidas y buenas prácticas que mitiguen los riesgos de seguridad en cuanto a contraseñas e ingresos a sus plataformas y red de datos.

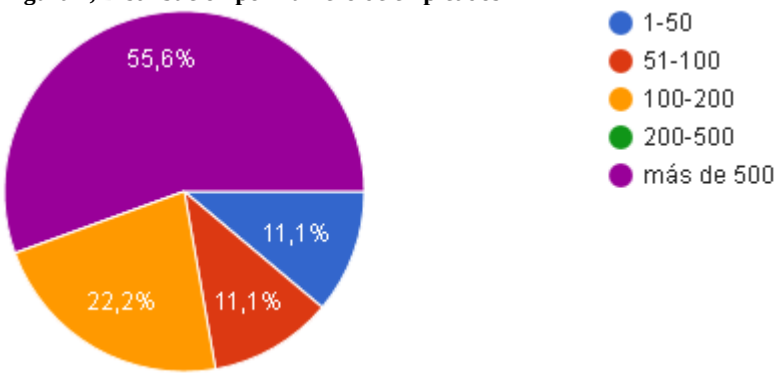
La gestión tiene un papel vital en las empresas por eso con base a los observado en la frecuencia de incidentes en las organizaciones y los problemas de seguridad presentados se enlistará recomendaciones de auditoria, control interno y tratamiento de vulnerabilidades.

4. IDENTIFICACIÓN DEL SECTOR Y TAMAÑO DE LAS ORGANIZACIONES

De acuerdo con las respuestas de la pregunta número tres (3) de la encuesta, en su mayoría, con un 77,7% son organizaciones con más de 100 trabajadores, lo cual se estima como compañías medianas a grandes que cuentan con herramientas protección y un interés de crear o ya establecido el sistema de gestión de seguridad de la información y/o controles similares, que les permitan proteger los datos sensibles, generando políticas y respuesta a los incidentes presentados.

El detalle de las respuestas para el número de empleados de las organizaciones se ilustra en la figura 1,

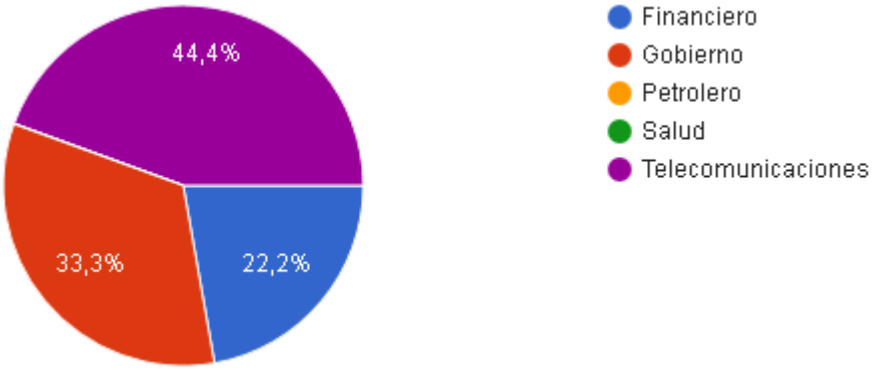
Figura 1, Distribución por número de empleados



Fuente: Resultados encuesta de Monografía

Así mismo, dentro de las consultas realizadas fue posible identificar el sector de la organización al cual pertenece dentro de las opciones establecidas en el alcance, se consultaron 5 diferentes sectores, sin embargo, dado que existe dependencia de la participación de las personas que recibieron la encuesta, para lo cual se informaba a los encuestados el destino de la información y se consultaba si deseaban participar en la recolección de la información o no, dentro de las respuestas obtenidas su participación por sectores fue del 44,4% para telecomunicaciones, 33,3% Gobierno y 22,2% para el sector financiero. La participación fue aceptada para la revisión de resultados, dado que la importancia en la muestra era la diversidad de tipos de organización para lo cual 3 sectores diferentes se estableció como suficiente para la evaluación. La figura 2 ilustra los resultados obtenidos.

Figura 2, Distribución de sectores



Fuente: Resultados encuesta de Monografía

5. ASPECTOS CRÍTICOS IDENTIFICADOS

De acuerdo con la información obtenida, las respuestas de las encuestas permitieron encontrar algunos hallazgos de la gestión de las plataformas que pueden llegar a representar inconvenientes para la correcta administración de los dispositivos de seguridad.

La primera evaluación realizada corresponde al nivel de conocimiento o experiencia de los administradores de las soluciones de seguridad, para lo cual se obtuvo que el 40% de las personas consultadas han indicado que el personal con el que cuentan es suficiente, para el 60% restante existe un déficit en la experiencia o nivel de conocimiento. Así mismo las herramientas de seguridad cuentan con funcionalidades avanzadas que requieren niveles de experiencia idóneos para su configuración, por lo tanto, no es posible implementar nuevas funcionalidades.

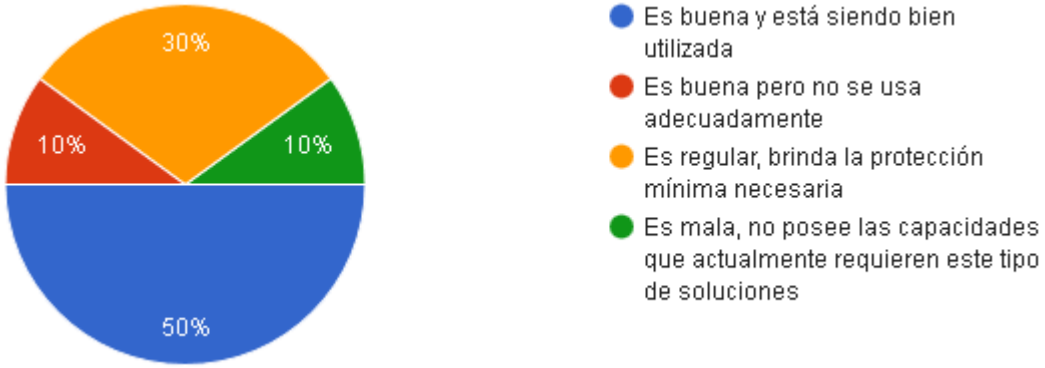
En el área de tecnología se cuenta con poco tiempo de experiencia en la compañía, si bien los recursos cuentan con gran conocimiento y habilidades, la alta rotación de personal no permite el conocimiento a profundidad del negocio, lo cual se esperaría para un grupo de administradores de herramientas que se encargan de proteger la información sensible de las organizaciones.

Se logró evidenciar que las organizaciones cuentan con varias herramientas de seguridad implementadas, el 50% tienen soluciones como las siguientes:

- Antivirus, comúnmente conocido como una herramienta de software instalada en un sistema operativo para prevenir y detectar software o código malicioso.
- Firewall perimetral, herramienta generalmente de tipo dispositivo ya sea físico o virtual que sirve para permitir o restringir el acceso de las redes o equipos que se controlen, hacia otras redes internas o externas.
- Control y protección de correo electrónico, herramienta de software, hardware físico o virtual o solución en la nube que permite proteger el correo electrónico de mensajes no deseados, fraudulentos, con links a páginas maliciosas o con archivos infectados.
- Control y protección de navegación, herramienta de software, hardware físico o virtual o solución en la nube que permite proteger el acceso a internet de los usuarios, estableciendo controles para categorías no permitidas o sitios maliciosos, así como la descarga de archivos infectados.
- NAC, significa control de acceso a la red, es una herramienta que permite controlar los dispositivos y accesos en una red corporativa, a nivel de la red cableada o por puntos inalámbricos.

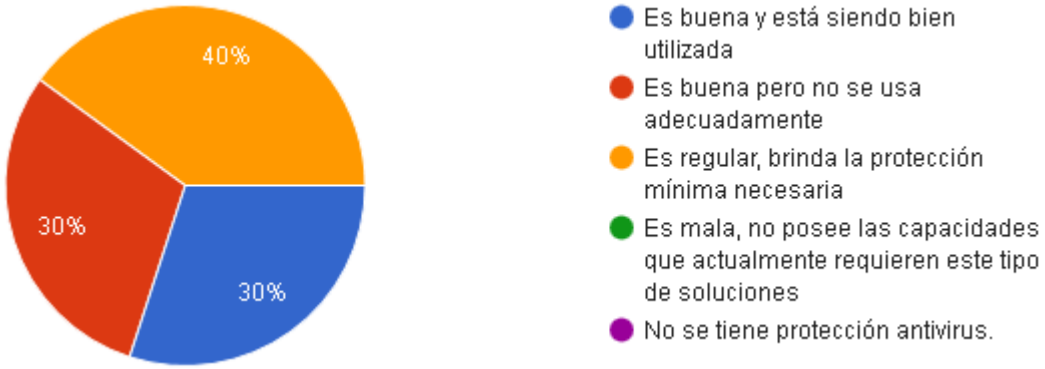
Las anteriores completan las herramientas o soluciones en su estrategia de seguridad informática, sin embargo, el conocimiento o experiencia es fundamental para aplicar mejora continua en cada una de estas herramientas implementadas. Generalmente estas soluciones fueron instaladas por personal idóneo, ya sea por el mismo fabricante o algún tercero especializado en cada una de las soluciones, pero dadas las respuestas obtenidas puede que no se haya dado continuidad para su perfilamiento adecuado, muchas herramientas de seguridad están siendo utilizadas con las configuraciones recomendadas por fabricantes, pero estas son genéricas y no personalizadas, las figuras 3 y 4 ilustradas a continuación, muestran que no se cuenta con el aprovechamiento de todas las funcionalidades que ofrece cada una de estas herramientas.

Figura 3, Distribución por percepción de configuración del firewall



Fuente: Resultados encuesta de Monografía

Figura 4, Distribución por percepción de configuración del Antivirus



Fuente: Resultados encuesta de Monografía

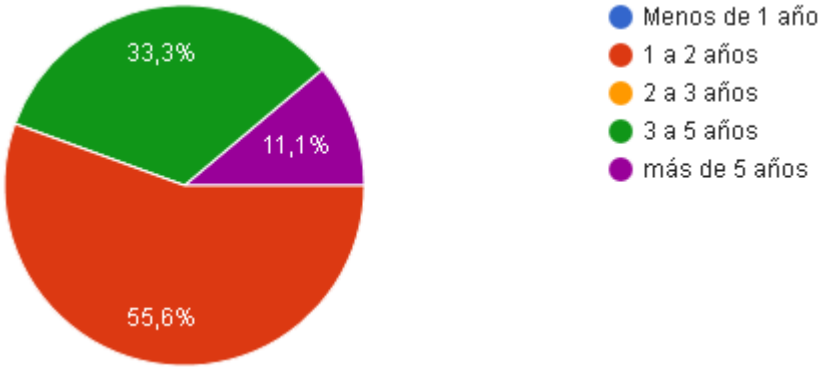
Como se ilustra en los resultados de la encuesta, si bien las soluciones pueden ser idóneas existe un alto nivel de percepción en faltantes de configuración que pueden mejorar su configuración y por consecuente la protección en la información sensible.

Se evidencia la adquisición de herramientas de seguridad acorde con el negocio, según sus necesidades cuentan con las soluciones de infraestructura requeridas, sin embargo, los recursos son limitados, los ingenieros encargados difícilmente cuentan con tiempo suficiente para generar planes de revisión y mejora continua, no se ha dado continuidad para su perfilamiento adecuado, muchas herramientas de seguridad han sido utilizadas con las configuraciones recomendadas por fabricantes, pero estas son genéricas, se deberían personalizar teniendo en cuenta las necesidades del negocio y su infraestructura

Las organizaciones consultadas cuentan con plataformas de seguridad acordes con sus necesidades, sin embargo, no se están aprovechando las herramientas, tienen módulos deshabilitados o malas configuraciones, dado que no hay inversión en su mantenimiento, estableciendo controles y mejora continua de su configuración

Teniendo en cuenta que es muy importante alinear el negocio con todas las áreas de la cual TI o Seguridad Informática hace parte de ello, es muy importante contar con personal con antigüedad laboral en la organización, esto ayuda a entender el negocio y promover políticas y controles con un nivel avanzado de madurez, sin embargo, dentro de los resultados obtenidos, el 55,6% lleva máximo 2 años trabajando en la organización, el 33,3% lleva menos de 5 años y tan solo el 11,1% supera los 5 años de antigüedad, como se ilustra en la figura 5 de los resultados de la encuesta.

Figura 5, Distribución por antigüedad



Fuente: Resultados encuesta de Monografía

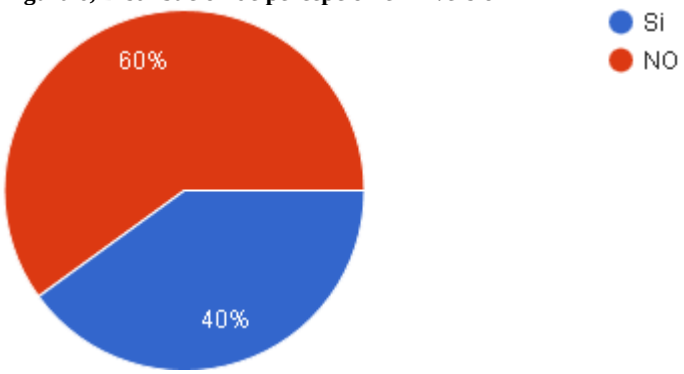
Según indica según John Badel, gerente general de Lee Hecht Harrison para Colombia[1] existe un impacto con el tiempo que lleva una persona en una organización, en donde se estima casi 1 año para que se encuentre en optimo

[1] http://www.eltiempo.com/economia/sectores/impacto-de-la-rotacion-de-personal-en-las-empresas-46479

desempeño para su función, así mismo Gualis y Oliveri en el artículo Antigüedad en el Empleo y Rotación Laboral en América Latina[2] indican que más experiencia dentro de la empresa favorece la productividad laboral y produce un círculo virtuoso entre las empresas y los trabajadores.

La inversión en seguridad es muy importante, ya sea para soluciones que no se tengan actualmente, renovación o crecimiento de las actuales, contratación de personal idóneo, entre otras, de acuerdo con la información recolectada, el 60% de los encuestados ha manifestado tener percepción de inversión baja para la seguridad de la información, la figura 6 ilustra estos resultados de la encuesta.

Figura 6, Distribución de percepción en inversión



Fuente: Resultados encuesta de Monografía

Lo anterior podría reflejarse en fallas o problemas de seguridad para la organización o falta de controles para los incidentes detectados; Como podría ser el caso de la evidencia de fuga de información sin tener herramientas de tipo DLP o control de acceso a los datos estructurados o no estructurados de la organización, es indispensable contar con el apoyo de directivos y alta gerencia para invertir en seguridad mostrando el retorno a la inversión que tienen por asegurar la información, en su integridad y confidencialidad principalmente.

Se requiere contar con el apoyo de los directivos de la organización para apoyar las inversiones de infraestructura, esto acompañado de un plan estratégico de seguridad de la información con retorno de inversión, demostrando el impacto negativo que tiene los incidentes informáticos y el valor en ahorro por prevenirlos.

[2] https://publications.iadb.org/bitstream/handle/11319/7770/Antiguedad-en-el-Empleo-y-Rotacion-Laboral-en-America-Latina.pdf?sequence=1

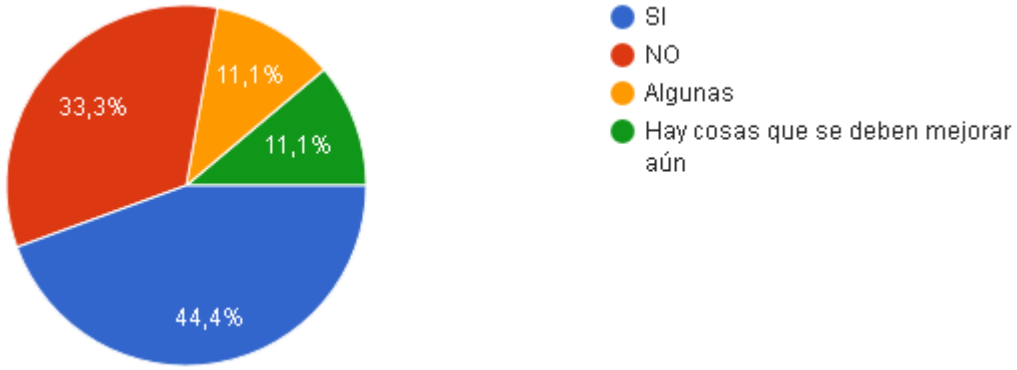
6. IDENTIFICACIÓN DE LOS PROCEDIMIENTOS EJECUTADOS

La confidencialidad, integridad y disponibilidad de la información, son tres pilares esenciales la gestión de recursos y protección de la información, de la siguiente manera.

- Confidencialidad, se trata de velar para que los datos no lleguen a usuarios no autorizados; manteniendo un entorno de privacidad de la información.
- Integridad, busca garantizar que la información es original, que no se ha interceptado o manipulado afectando su contenido.
- Disponibilidad, garantizar para aquellos usuarios autorizados la información se encuentre accesible en todo momento.

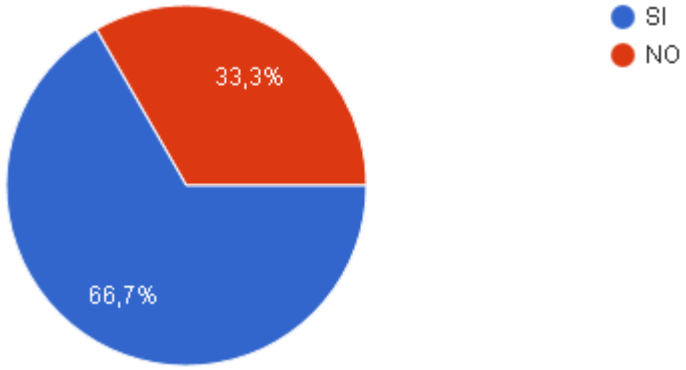
Alrededor de un 50% de los resultados obtenidos muestra inconvenientes para cumplir con estos, por lo tanto, puede representar fallas en los procedimientos y configuraciones de sus plataformas, dado que a pesar de contar con ellas se presentan fallas, como se ilustra en las figuras 7, 8 y 9 con los siguientes resultados.

Figura 7, Distribución por cumplimiento de confidencialidad



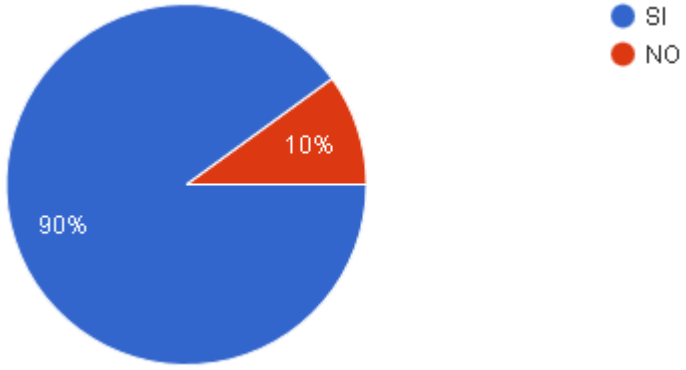
Fuente: Resultados encuesta de Monografía

Figura 8, Distribución de cumplimiento de Disponibilidad



Fuente: Resultados encuesta de Monografía

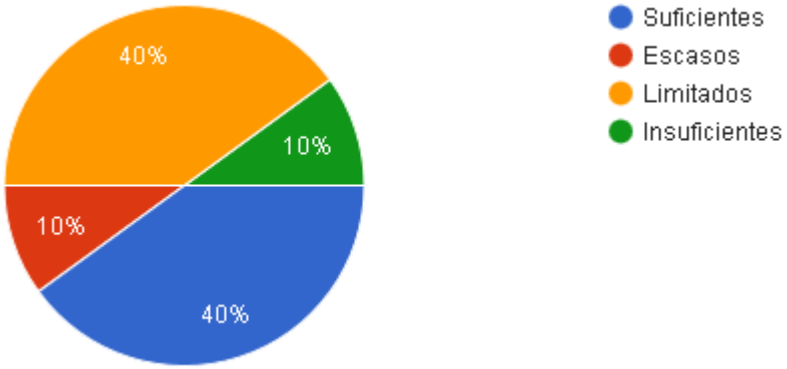
Figura 9, Distribución de cumplimiento de Integridad



Fuente: Resultados encuesta de Monografía

Así mismo se pueden presentar fallas en la atención de incidentes, dado que el 40% indica que las políticas y controles aplicados son suficientes, por lo tanto, es posible que no existan procedimientos claros ni plan de gestión de incidentes establecidos, de acuerdo con los resultados ilustrados en la figura 10.

Figura 10, Distribución por estado de controles y políticas



Fuente: Resultados encuesta de Monografía

Con la información recolectada se evidencia que las organizaciones cuentan con plataformas de seguridad acordes con sus necesidades, es decir que pueden proteger su infraestructura con lo que tienen implementado actualmente, sin embargo alrededor del 50% siente que no se están aprovechando las herramientas, que tienen módulos deshabilitados o malas configuraciones, lo cual demuestra que la inversión si bien se requiere para adquirir las plataformas, en realidad no importa cual se adquiera, siempre y cuando se invierta en su mantenimiento, estableciendo controles y mejora continua de su configuración, lo cual será más efectivo que adquirir soluciones costosas sin el respectivo perfilamiento y su proceso de mejora continua requerido.

El 70% y 50% de los encuestados consideran que las soluciones de Antivirus y Firewall respectivamente, requieren mejoramiento de sus configuraciones, dado que son soluciones que pueden llegar a ser suficientes para los requerimientos de la entidad pero requiere de seguimiento y mejoramiento continuo, únicamente el 10% de los encuestados indica que las soluciones no son idóneas, por los datos obtenidos se puede indicar que las herramientas de protección adquiridas por las organizaciones son buenas e idóneas para las necesidades de la organización, sin embargo, se pueden presentar fallas o ausencia de mejoramiento, causando mala configuración o gestión de estas, permitiendo su funcionamiento sin el aprovechamiento que debiera tenerse.

Las vulnerabilidades de los sistemas o aplicaciones son encontradas frecuentemente, ya sea por alguna comunidad o atacantes que se dedican a hallarlas, para remediarlo se requieren de la actualización a través de nuevas versiones o parches de seguridad emitidos por los fabricantes, por ejemplo, Microsoft entrega al menos una vez al mes actualizaciones a los sistemas operativos, de acuerdo con las respuestas obtenidas, el 60% de las organizaciones no realizan actualizaciones con buena frecuencia (más de 6 meses), lo cual representa riesgos de seguridad por vulnerabilidades conocidas que se encuentran publicadas y latentes a ser aprovechadas por un atacante.

7. ANÁLISIS DE LOS PROBLEMAS DETECTADOS

Constantemente las organizaciones se encuentran expuestas a una gran variedad de amenazas; algunas de estas generadas intencionalmente y otras que surgen como resultado de acontecimientos inesperados dados por actualizaciones, cambios de configuraciones, cambios en la estructura de la organización, procedimientos no ejecutados, etc., debido a esto las organizaciones encuentran muy preocupante el mantener la continuidad del negocio frente a diversas amenazas o vulnerabilidades a las cuales se encuentran expuestas poniendo en riesgo la confidencialidad, disponibilidad e integridad de la información.

De acuerdo con las variables evaluadas en estas organizaciones se encuentra deficiencia en los siguientes aspectos:

- Procedimiento para asignación y cambio de contraseñas en las plataformas
- Manejo de información confidencial y sensible
- Procedimientos de actualización de plataformas
- Análisis de vulnerabilidades.
- Revocación de accesos

Procedimiento para asignación y cambio de contraseñas en las plataformas: No se cuenta con un procedimiento con las mejores prácticas (Longitud de la contraseña, complejidad de contraseña, método de generación de contraseñas) establecido para realizar esta actividad lo cual hace sus equipos vulnerables a un ingreso no autorizado.

Manejo de información confidencial y sensible: Aunque existe una política en donde se menciona el uso correcto de esta información no se han realizado campañas de sensibilización, ni se ha realizado su respectiva divulgación de acuerdo a esto el personal que manipula información confidencial y sensible dentro de las organizaciones la salvaguarda según su criterio puesto que no se tiene conocimiento del impacto que tendría la falta de integridad, confidencialidad y disponibilidad de esta información.

Procedimientos de actualización de plataformas: En el análisis realizado respecto a las versiones de firmware en la que se encuentran las plataformas de seguridad se puede concluir que muchas de estas plataformas se encuentran en una versión no recomendada por sus proveedores lo cual conlleva a brechas de seguridad que pueden llegar a afectar la continuidad del negocio o versiones desactualizadas. Aunque se tienen procesos establecidos de actualización de

equipos no son tenidos en cuenta ya que se tiene un histórico de incidentes ocasionados a partir de actualizaciones realizadas en donde no se contemplaron aspectos como capacidad, inconvenientes de la versión a instalar, laboratorios para identificar conflictos con los servicios ofrecidos en las organizaciones.

Análisis de vulnerabilidades: El análisis de vulnerabilidades es una prueba de importancia realizada en todo tipo de infraestructura monitoreable y gestionable, ya que permite la detección proactiva de las vulnerabilidades que presentan riesgos que impactan significativamente a la compañía. Mediante el uso de herramientas y con el apoyo del análisis de las personas, se pueden identificar y corregir las deficiencias antes de que sean explotadas. Sin embargo, no se cuenta con procedimientos adecuados para realizar remediaciones oportunas y eficaces

Proceso de revocación de accesos: Debido a la rotación de personal es importante contar con proceso de revocación de accesos, este trabajo debe realizarse engranado con el área de recursos humanos para que está notifique y se realice eliminación de permisos, desvinculación de cuentas, etc.

8. RECOMENDACIONES QUE PERMITAN MEJORAR LA SEGURIDAD PARA PROTEGER LA INFORMACIÓN SENSIBLE EN LAS ORGANIZACIONES CONSULTADAS

Dadas las redes de datos de las organizaciones, su continuo crecimiento y su preocupación por la adquisición e implementación de herramientas de seguridad es importante contemplar de manera general como adoptar un uso adecuado de las mismas y los protocolos de seguridad; de acá nace la importancia de dar a conocer porque el uso de una ciertas características y no de otras; a continuación se realizan recomendaciones basadas en información encontrada en organizaciones de diferentes sectores después de realizar una consulta apoyada en una encuesta.

Estas recomendaciones se clasifican en tres grupos; protocolos, accesos y gestión; es importante tener en cuenta que estas categorías están encaminadas a realizar una recomendación de manera general, teniendo en cuenta los requerimientos de seguridad mínimos en las redes de datos de cualquier organización.

8.1 PROTOCOLOS

Para la presente categoría se sugiere:

- Generar un control en las organizaciones que relacione la configuración de la versión de SNMP, mínimo en su versión 2.
- Es recomendable que las organizaciones agreguen un control para deshabilitar la administración de los dispositivos a través de HTTP debido a que es un protocolo inseguro, por otra parte es importante contar con la configuración de un tiempo límite de inactividad en las sesiones administrativas HTTPS.
- Se recomienda hacer uso de SSH para realizar la administración de los dispositivos de red y deshabilitar el Telnet.
- Restringir el número máximo de sesiones concurrentes por SSH a no más de 5.

8.1.1 SNMP

Dentro de los protocolos de intercambio de información se encuentra el protocolo SNMP, este es utilizado en casi todas las redes de datos para la comunicación entre dispositivos de red de telecomunicaciones por el cual se realiza el envío de información de propiedades de un componente de red; a la fecha se han desarrollado tres versiones diferentes para este protocolo; SNMPv1, SNMPv2 y SNMPv3.

- **SNMPv1:** Esta versión es muy fácil de configurar solo se requiere una comunidad en texto plano, sin formato alguno. Esta versión no tiene ningún tipo de seguridad por lo que puede significar un riesgo.

- **SNMPv2:** Es una versión compatible con SNMPv1, su formato de mensaje es diferente y posee funciones de autenticación y cifrado.

- **SNMPv3:** Esta versión proporciona un acceso seguro mediante autenticación y cifrado de los mensajes, es posible calcular la autenticación por medio de un HASH.

8.1.2 HTTPS

Los navegadores realizan la conexión a los servidores web por medio del protocolo HTTP, este no es seguro ya que acá la información es compartida sin ningún tipo de cifrado. HTTPS es un protocolo de conexión seguro el cual permite realizar un cifrado de los datos, para este protocolo se utiliza SSL (Secure Sockets Layer) o TLS (Transport Layer Security); estos protocolos realizan la negociación de algún algoritmo para cifrar la información, es importante conocer que TLS es una evolución del SSL. En la figura 11 se relaciona un diagrama donde se muestra cómo se establece la conexión a un sitio web por alguno de los dos protocolos seguros.

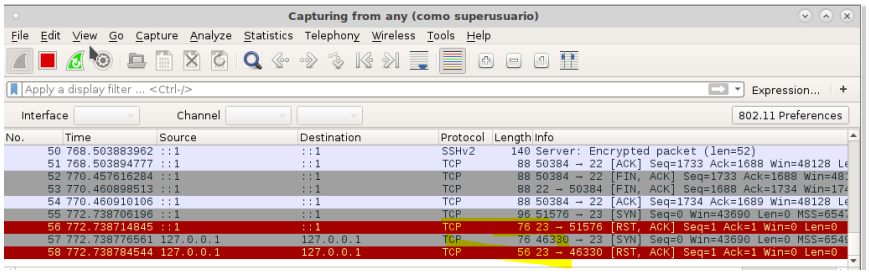
Figura 11, Conexión a un sitio web

Fuente: El autor

8.1.3 SSH

Existen diferentes protocolos de administración remota de los dispositivos de red, uno de ellos es Telnet y el otro SSH, la diferencia entre estos dos es que Telnet no es seguro y SSH si, como se muestra en la figura 12, al realizar una inspección de tráfico en una red usando Telnet es posible visualizar la información que se transfiere, en cambio al realizarla por SSH, en una herramienta como de inspección de tráfico se puede ver el únicamente el puerto de transmisión.

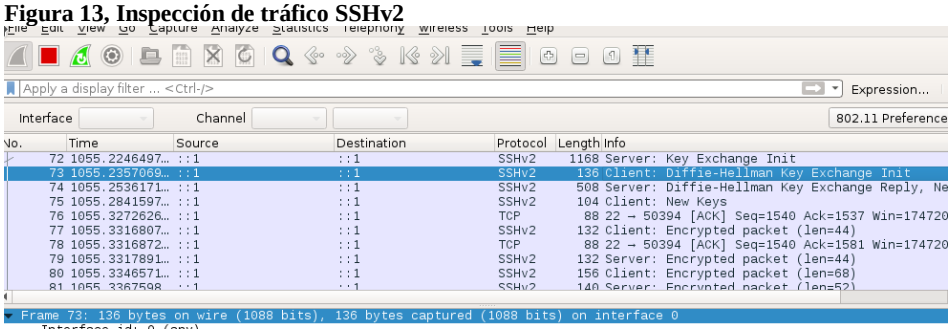
Figura 12, Inspección de tráfico TELNET



Fuente: El autor

La figura 13, muestra que al lanzar una petición por SSH es posible visualizar el puerto destino el cual es el 22, el protocolo de cifrado que para el ejemplo es Diffie-Hellman y la versión de SSH que es SSHv2.

Figura 13, Inspección de tráfico SSHv2



Fuente: El autor

8.2 ACCESOS

Para la categoría correspondiente a accesos se realizan las siguientes recomendaciones:

- Las contraseñas deben ser almacenadas cifradas y no en texto claro.
- Debe existir un control en el que se especifique la longitud y características de la contraseña de acuerdo con la normativa vigente de cada una de las organizaciones.
- Realizar la creación de listas de asignando únicamente un grupo de direcciones ip's o host que pueden tener administración del dispositivo.

Hay diferentes métodos utilizados por los atacantes para encontrar las contraseñas que se utilizan para ingreso a cualquier dispositivo de red; a continuación, se listan algunos de ellos:

- **Ingeniería social:** Es posible que un atacante por medio de una llamada, mensaje, o visita al personal administrador haga que le sean reveladas las contraseñas de administración, haciendo diferentes preguntas y ganándose la confianza de estos.

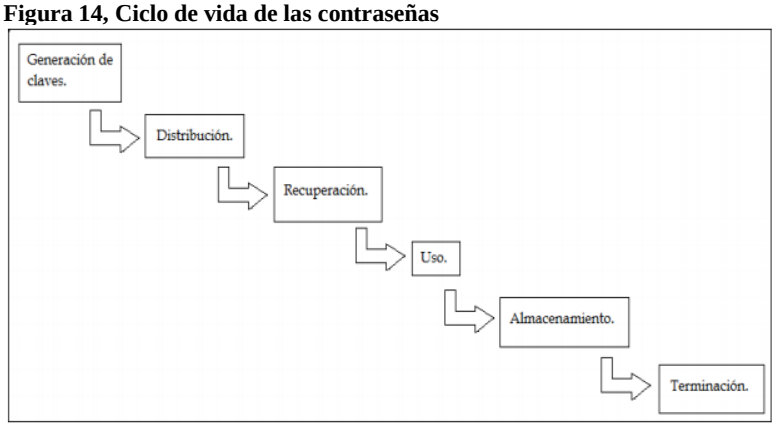
- **Ataque de fuerza bruta:** Un atacante puede realizar diferentes intentos de contraseñas hasta encontrar la que le permita el acceso al dispositivo.

- **Keylogger:** Es un programa que se instala en el PC del administrador y captura lo que se teclea.

- Otro método puede ser que el administrador exponga las contraseñas de ingreso delante de terceros, por ejemplo, si hay alguna persona ajena al grupo administrador y solicita alguna información "urgente", el usuario ingresa a algún dispositivo que está bajo su administración y el tercero se da cuenta de cuál es la contraseña.

En la figura 14, Echeverry Ana. (2016), en "*Política de gestión de contraseña para usuarios finales"*, define un ciclo de vida de las contraseñas el cual permite el uso de políticas y buenas prácticas para esto.

Figura 14, Ciclo de vida de las contraseñas



Fuente: Política de gestión de contraseñas para usuarios finales

Para la generación de contraseñas se recomienda no usar solo palabras o solo números sino usar frases alfanuméricas en combinación con caracteres especiales, hay herramientas para la creación de contraseñas aleatorias y que cumplen los

estándares mencionados, algunas de ellas son: Password Generator, KeePass y LastPass.

En la distribución de contraseñas se recomienda si es necesario realizar el envío por correo electrónico hacer uso de una firma digital, otra opción es realizarlo vía telefónica y tener en cuenta que este sea un medio seguro y nadie más este escuchándolos.

Para realizar la recuperación de una contraseña es importante definir un protocolo y tener en cuenta cuales son los requerimientos de cada uno de los fabricantes en caso de que este proceso se requiera.

El uso de las contraseñas de los dispositivos en una organización debe ser confidencial, no debe ser revelada absolutamente a nadie ni revelarla frente a otros.

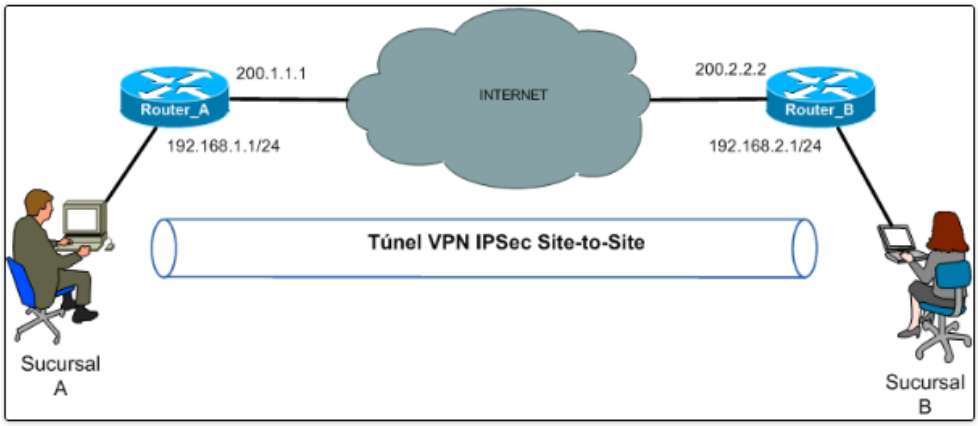
Se recomienda hacer uso de aplicaciones donde se pueden almacenar las contraseñas de manera cifrada.

Se deben tener en cuenta un ciclo de vida útil de la contraseña no mayor a tres meses, después de este periodo de tiempo se debe realizar la generación de una nueva y borrar la anterior de todos los sitios donde se encuentre almacenada.

Por otra parte para garantizar la confidencialidad e integridad del acceso a la información almacenada en los dispositivos de red y su función es importante contar con restricciones de direccionamiento para el ingreso a estos, si un atacante posee alguna de las contraseñas de administración pero existe una restricción del direccionamiento IP desde donde se realiza la conexión el equipo no le permitirá el ingreso; existen opciones de configurar listas de acceso en los equipos para que no se presenten conexiones desde sitios no permitidos.

Debido a que hay organizaciones que solicitan a empresas externas realizar tareas de monitoreo, gestión y/o administración en su red, es importante brindar un acceso restringido y seguro para ellos, la solución más óptima para estos casos es implementar una conexión a través de una VPN sitio a sitio, como se puede visualizar en la figura 15, esta conexión lo que realiza es brindar seguridad desde el punto A al punto B por medio del uso de protocolos seguros, cifrando la información que viaja a través del mismo. Al requerirse generar un acceso a terceros a su infraestructura se recomienda generar un perfil dependiendo la necesidad, por ejemplo, si la organización quiere que una empresa externa mantenga un continuo monitoreo de sus dispositivos se puede crear un perfil de lectura para ellos, acá tendrán un acceso restringido y una visualización puntual de lo que se requiere, esto ayudará con la mitigación de cambios a nivel de configuración en los equipos.

Figura 15, Conexión VPN sitio a sitio



Fuente: http://www.redescisco.net/sitio/2010/10/07/interconectando-sucursales-mediante-una-vpn-ipsec-site-site/

8.3 GESTIÓN

Para la presente categoría se sugiere:

- Se sugiere realizar un plan de auditorías de seguridad anual, donde se establezca los parámetros a evaluar y la frecuencia a realizarlas en el año.

- Realizar un análisis de riesgo de cada uno de los sistemas que intervienen en los procesos de TI la organización.

- Contar con un comité de riesgos el cual tenga como objetivo establecer controles para identificar fallas que se presenten por debilidades en la gestión, mantenimientos o versiones instaladas en cada una de las herramientas que se encargan de la protección de la información.

- Contar con procedimientos establecidos para la atención de incidentes, ya sea con herramientas de atención de solicitudes o registro por correo electrónico, es indispensable realizar:
- Valoración del evento que ingresa al grupo de atención de incidentes.
- Establecer el impacto y urgencia que tiene, de acuerdo con el tipo de evento, si afecta el core del negocio o algún activo importante.
- Categorizar el incidente
- Documentar el proceso que deben realizar por cada una de las categorías disponibles, se puede realizar durante la solución y manejo de eventos reales.

- Establecer una base de conocimiento con el procedimiento a realizar y validaciones necesarias para confirmar la solución adecuada en caso de que el incidente se repita.

- Realizar revisiones periódicas para establecer un control de cambios, si bien cada uno de los cambios establecidos en las plataformas requieren documentación, es indispensable revisar los cambios ejecutados para identificar posibles fallas por riesgos que puedan representar, dado que por habilitar algún permiso especifico es posible crear políticas que pongan en riesgo la seguridad de la información, por ello es necesario validar cada una de las configuraciones existentes para identificar cambios que deban hacerse para mejorar la seguridad, por lo anterior, se requiere:
- Validar periódicamente cada una de las políticas configuradas en las plataformas, permisos de acceso, bloqueos y otros eventos configurados.
- Verificar logs para identificar que está permitido o denegado.
- Establecer propuestas de mejoramiento para aplicar las configuraciones idóneas, que permitan cerrar brechas y optimizar los recursos.

8.3.1 Auditorias

Las auditorías internas son actividades en busca de mejoras en cuanto a su organización y el cuidado de los riesgos para brindar una mejor calidad en sus procesos mediante una sistematización de evaluaciones y proposiciones que lleven adelante cualquier organización de una forma ordenada y con un alto grado de gestión.

Es una actividad independiente con el objetivo de asegurar y medir los procesos institucionales, esta práctica ayuda con un sistema sistemático el cumplimiento de las metas para evaluar y proponer mejoras de los diferentes procesos en cuanto al riesgo y controles que proporciona una entidad o empresa.

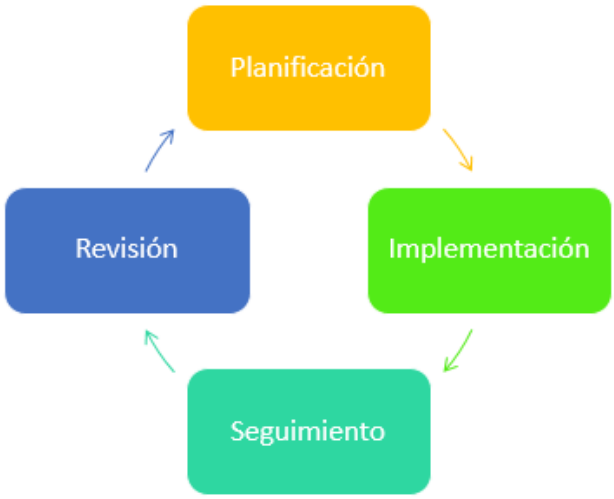
Los objetivos de una auditoria interna consisten en realizar un seguimiento a la gestión de un negocio, así como la aplicación de metodologías que ayudan a realizar un análisis en qué medida se cumplen los procedimientos, revisión y evaluación de las mejoras en la gestión y administración del negocio.
En otras palabreas se busca promover y evaluar la seguridad de los diferentes activos, la calidad en los servicios prestados tanto administrativos como sociales, todo esto en busca de la mejora continua, en la figura 16 se muestra el plan de mejoramiento continuo sugerido.

Para cumplir con los objetivos se debe realizar los siguientes pasos:

- Evaluar los riesgos de todos los componentes en una organización.

- Promover un sistema de control.
- Proponer las mejoras en cada uno de los procesos con el propósito de mejorar su eficacia y eficiencia.
- Mantener un programa de seguimiento a las observaciones o no conformidades encontradas en los informes y realizar los diferentes cambios a los controles, políticas existentes.

Figura 16, Plan de mejoramiento continúo



Fuente: https://www.escuelaeuropeaexcelencia.com/2016/07/auditoria-interna-iso-9001-mejora-continua/

- **Planificar la auditoría interna de la empresa según la norma ISO 9001:** En este paso lo que se debe hacer es listar todos los procesos que existan en la empresa, si es posible se puede tomar la información de los mapas de procesos, si los tiene.

- **Definir los objetivos de la auditoria interna:** Estos objetivos pueden ser los que se plantearon en la planificación estos pueden ser específicos o genéricos, en este paso lo que se busca hacer es para donde vamos y como lo vamos hacer y cual seria los resultados.

- **Conocer a la empresa a la que se plantea auditar:** Se debe hacer un reconocimiento tanto documental como físico para conocer cuáles son sus alcances en caso de ser certificados y cuáles son los objetivos de la empresa.

- **Definir el método de cómo realizar la auditoria interna:** Ya definido un método de auditoria (por procesos) lo que se podría hacer es tomar la información del mapa de procesos y verificar toda la información tanto la que entra como la que sale y evaluar si se aplica a la norma que está asignada.

- **Informe de auditoría interna:** Se debe crear un informe que describa que áreas se auditaron cuales no están conformes y por qué, explicando los hallazgos que no están de acuerdo a la norma o procedimientos establecidos, siendo muy puntuales y concretos para que estos también puedan ser interpretados por las altas directivas.

- **Cierre de desviaciones:** Luego del informe y haber concertado con los líderes de las diferentes áreas cuales fueron las inconsistencias se acuerda una fecha para que se tomen las respectivas correcciones o planes de mejora se procede hacer el cierre de estas mismas

- **Presentación de resultados en la revisión por la dirección:** En la presentación se puede incorporar algunas nuevas mejoras o acciones en busca de una mejora continua.

8.3.2 Control Interno

Como primera instancia se define lo que es el control interno informático, "Identificado como un sistema compañero del proceso administrativo, referente a planear, organizar dirigir y gestionar los procedimientos y operaciones para proteger los elementos informáticos, con el objetivo de proteger la economía de la organización y el buen uso de los elementos de manera eficiente y efectiva. (Auditoría Informática – Aplicaciones en Producción – José Dagoberto Pinilla)".

El control interno se puede dar a través de diferentes maneras teniendo en cuenta la empresa y sus labores prestadas. Además de esto, también debe tener en cuenta los distintos enfoques administrativos para que no resulten afectados los mecanismos de acción, con esto, se puede llegar inclusive a medir el funcionamiento de un empleado y su manera eficaz y eficiente de desempeñarse frente a su labor.

El resultado de la aplicación de un buen control interno es el mejoramiento continuo en todas las actividades que se realizan, calidad en los resultados y las metas, con el buen desempeño de todas las labores y teniendo a nivel de control interno autocontrol, autogestión y autorregulación.

Teniendo en cuenta lo anterior, se tiene el control interno informático el cual se refiere a una función de la oficina de TI o sistemas, el cual tiene por objetivo velar por el cumplimiento de los procesos y normas establecidos, confirmar la aplicabilidad de las normas legales, interceder para la capacitación que requiera el personal, apoyar durante las actividades de revisión y auditorías, implementar los mecanismos necesarios para medir las metas establecidas para el grupo con los procesos y medios adecuados.

A continuación, se relacionan algunas funciones específicas del control interno informático:

- Publicar y velar por el cumplimiento de las normas, procesos y procedimientos establecido para los colaboradores.
- Establecer el sistema de control interno en la Dirección de TI, teniendo en cuenta, El mantenimiento y continuo mejoramiento del software utilizado por las aplicaciones, validar los servidores en producción y su licenciamiento o software utilizado, confirmar a nivel organizacional las redes, licenciamiento y otras licencias o contratos necesarios para la operación, sean tratados directamente o a través de terceros, velar por el cumplimiento de los controles y estableces una cultura de protección de los activos de la organización.

Por consiguiente, se describen los métodos de la aplicación del control interno, se debe tener en cuenta que dichos métodos varían teniendo en cuenta el tipo de organización que se esté manejando. El primero de estos hace referencia al informe COSO por medio del cual se precisa el Control Interno como el conjunto de normas, procedimientos, prácticas y estructuras organizativas que se han diseñado con el fin de establecer parámetros a nivel de seguridad estableciendo control sobre cualquier evento no esperado, previniendo, detectando y corrigiéndolo.

Los controles que se pueden aplicar en el control interno de una organización son: el control operativo, el control de legalidad, el control de evaluación y verificación, el control financiero, el control de gestión y el control informático. A continuación, se describirán cada uno de estos:

Control operativo: Este tipo de control es el que se efectúa día a día en el proceso normal de la empresa para que así se logren los objetivos planteados o lo que sea su cometido social o empresarial. Tiene que ver con las actividades cuyo fin sea verificar los métodos y procedimientos en las operaciones que se realizan, también, tiene que ver con investigar cualquier practica comercial desleal, lesivas o restrictivas, que se hayan presentado de acuerdo con la normatividad vigente dentro de la organización. Es utilizado para la verificación del correcto funcionamiento e implementación de los procedimientos y controles los cuales se deben desarrollar bajos las condiciones especificadas en la normatividad vigente.

Control de legalidad: Es tipo de control es usado para realizar la verificación y evaluación precontractual y legal de las operaciones y actos administrativos que realizan las empresas determinando o estableciendo que cumplan con el debido proceso y las normas constitucionales y legales que se encuentran vigentes en el país.

Control de evaluación y verificación: Tiene que ver con la responsabilidad de la Oficina de Control Interno de realizar la medición con el fin de evaluar, planear, dirigir y organizar en forma independiente la eficiencia, eficacia y economía del sistema, donde se debe velar por la forma por la forma como se están administrando los recurso de la empresa si se están usando eficientemente y esto debe dar como resultado un informe a los directivos en la continuidad del proceso administrativo, la revaluación de los planes establecidos y en la introducción de los correctivos necesarios para el cumplimiento de las metas u objetivos planteados dentro de su cometido.

Control financiero: Es aplicado con el fin de tener el control de las finanzas de las empresas los cual tiene que ver con la evaluación ejecutada en la aceptación de las normas establecidas, lo anterior permite controlar las operaciones, procesos, modificaciones entre otras actividades de la situación financiera de la organización, dando soporte a la creación de controles y procesos para las transacciones financieras que permitan ser verificables ante las autoridades que requieran su validación. Un control riguroso de las finanzas incrementa la eficiencia de una empresa y a la vez las protege de una mala gestión financiera y les permite verificar más fácilmente las operaciones registradas en las contabilidades y que se vaya cumpliendo con lo planeado.

Control de gestión: Por medio de este se realiza la evaluación que establece la eficiencia y eficacia de las organizaciones en la administración de los recursos, esto con el fin de establecer mediante dicho examen el eficaz funcionamiento de sus procesos administrativos, el uso de medidores de crecimiento y adecuado proceso para identificar su rentabilidad en beneficios o excedentes producidos dentro del servicio prestado como core del negocio.

El control de gestión está determinado por fases las cuales son: diagnóstico de la institución, referente al proceso de control a todo el sistema que deba contar con procesos establecidos, el objetivo es encontrar fallas o dificultades que se puedan presentar e intervendrán con el sistema, así como identificar el entorno requerido para el correcto funcionamiento. Un buen diagnóstico permitirá identificar cuales elementos son idóneos para el proceso de la organización en revisión, asi se podrán usar para garantizar el éxito.

Control informático: Este hace referencia a la evaluación objetiva, crítica, sistemática, y selectiva de los controles y políticas establecidas, que pueden ser procesos, procedimientos normatividad u otras que permitan brindar una opinión referente al uso adecuado de los recursos del área de infraestructura tecnológica.

Estos controles tienen áreas de aplicación como son:

- **Controles generales organizativos:** Los cuales se basan en la planificación, control y evaluación del departamento de Informática de la empresa.

- **Controles de los Sistemas de Información:** Estos permiten contar con la eficiencia, estabilidad financiera, integridad, protección de la información a través de seguir las regulaciones del proceso para desarrollo seguro de aplicaciones.

- **Controles de ejecución de los sistemas:** Se refiere a la administración de los recursos necesarios para la correcta implementación y operación de las herramientas de software, de acuerdo con los requerimientos de hardware.

- **Controles de Aplicación:** Las aplicaciones desarrolladas debe contener controles incorporados eficientes que permitan validar las entradas, actualizaciones, salida y datos exactos de las salidas de las aplicaciones.

- **Controles en Gestión para datos estructurados:** Estos deben permitir tener asegurados los 3 pilares fundamentales de la seguridad informática como son asegurar la integridad como el primer pilar de la seguridad, la disponibilidad de los datos y mantener su confidencialidad.

- **Controles de conexiones de red:** Pretende que la arquitectura de red, su mantenimiento y aseguramiento centralizadas y distribuidas en una forma segura en el entorno empresarial.

- **Controles sobre computadores y LAN**: Estos permiten que se relacionen las políticas para la adquisición, instalación y soporte técnico y la seguridad de estos.

8.3.3 Vulnerabilidades:

El análisis de vulnerabilidades es una prueba de importancia realizada en todo tipo de infraestructura monitoreable y gestionable, ya que permite la detección proactiva de las vulnerabilidades que presentan riesgos que impactan significativamente a la compañía. Mediante el uso de herramientas y con el apoyo del análisis de las personas, se pueden identificar y corregir las deficiencias antes de que sean explotadas.

Para la ejecución análisis de vulnerabilidades, es posible basarse en las siguientes herramientas.

8.3.3.1 Analizador de vulnerabilidades “Tenable Nessus Professional Feed”

La figura 17, muestra el icono de Nessus, esta herramienta es una aplicación que corre sobre otro sistema operativo, el cual permite identificar vulnerabilidades en los equipos de la red. Las características de esta herramienta son:

- Detectar las vulnerabilidades de los equipos de la organización.

- Brindar recomendaciones para mitigar las vulnerabilidades detectadas.

Figura 17, Analizador de vulnerabilidades.

Fuente: https://www.tenable.com/products/nessus/nessus-professional

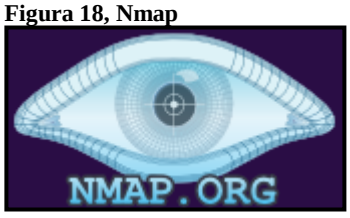
8.3.3.2 Nmap ("Network Mapper")

La figura 18, muestra el icono de Nmap, esta es una aplicación de uso libre y con código abierto para analizar la red, buscando identificar anomalías a nivel general.

Nmap pretende identificar los equipos disponibles en la red y los servicios que estos prestan, identificando las aplicaciones y las versiones que tienen, asi mismo a nivel de sistema operativo identifica su versión y tipo. Nmap puede hacer uso de sentencias o filtros avanzados para activar otras características de inspección.

Es posible ejecutar Nmap en todos los tipos de sistemas operativos.

Figura 18, Nmap



Fuente:https://nmap.org/

8.3.3.3 Definición de Bases de Datos Consultadas

Para los correspondientes análisis de vulnerabilidades, se recomienda apoyarse en bases de datos, sustentadas por las entidades relacionadas en la figura 19:

Figura 19, Bases de datos Vulnerabilidades.

Fuente: https://www.rediris.es/cert/links/vuldb.html.es

8.3.3.4 Identificación de Activos de Cada Línea de Servicio

Dentro de todo el proceso de gestión de vulnerabilidades la primera actividad es la de identificación de los activos de cada línea de servicio, esta actividad se realiza en cada uno de los periodos debido a que la cantidad de activos cambia de forma significativa.

Es muy importante poder identificar los activos porque entre cada periodo cambia la infraestructura a analizar, otra de las razones de esta actividad es establecer exactamente los activos a los cuales se les realiza el debido tratamiento de análisis de vulnerabilidades.

A continuación, se sugiere como diligenciar los campos:

Nombre de la Línea de Servicio: Línea de Servicio.
Responsable: Responsable de la línea de servicio.
Fecha de escaneo de vulnerabilidades: Fecha exacta del día del escaneo de vulnerabilidades.
Número de dispositivos analizados: Cantidad de los dispositivos que se escanearon.
Periodo de Gestión de Vulnerabilidades: Periodo de Gestión de Vulnerabilidades.
Informe Técnico: Referencia al presente informe técnico.

No.: Número consecutivo de activos a analizar.
NOMBRE DEL ACTIVO: Nombre del activo
DIRECCIÓN IP: Dirección IP (Interntet Protocol) identificador único.
FABRICANTE: Nombre del fabricante del activo.

SERIE: Número único de serie del activo .
UBICACIÓN: Ubicación física del activo dentro de la organización.

Nombre de la Vulnerabilidad: Descripción de la vulnerabilidad en inglés, tal y como está en el informe de la herramienta seleccionada.

Descripción: Descripción de la vulnerabilidad realizada por el responsable de la línea base.

IP: Dirección única de Internet Protocol, IP.

Integridad: ¿Afecta la integridad del activo analizado? La Integridad es la propiedad de la información, por la que se garantiza que está no se modificará o se alterará dicha información. Responde SI o NO.

Confidencialidad: ¿Afecta la confidencialidad del activo analizado? Confidencialidad es la propiedad de la información, por la que se garantiza que está accesible únicamente a personal autorizado a acceder a dicha información. Responde SI o NO.

Disponibilidad: ¿Afecta la disponibilidad del .activo analizado? La Disponibilidad es la propiedad de la información, por la que se garantiza que está es accesible o no a dicha información. Responde SI o NO.

Explotabilidad: La explotabilidad se define como el vector o el escenario en el que se encuentra un atacante para poder aprovechar esta vulnerabilidad, así mismo como la dificultad de materialización de la vulnerabilidad. Cada responsable del análisis de vulnerabilidades de la línea base con base a sus conocimientos, deberá identificar si la explotabilidad de esta vulnerabilidad se puede llegar a materializarse de forma FÁCIL o de forma DIFÍCIL.

Código CVE: Common Vulnerabilities and Exposures, siglas CVE, es una lista de información registrada sobre vulnerabilidades conocidas de seguridad, donde cada referencia tiene un número de identificación único. De esta forma provee una nomenclatura común para el conocimiento público de este tipo de problemas y así facilitar la compartición de datos sobre dichas vulnerabilidades.

- Se sugiere ejecutar un escaneo periódico de vulnerabilidades a los componentes de TI, realizar su análisis y las debidas remediaciones.

- De ser posible, programar una tarea que realice periódicamente los backups de configuración de los equipos y que envíe este backup a un almacenamiento remoto a través de una conexión segura.

- Para las configuraciones temporales en los dispositivos de seguridad de red aplicar un Schedule, esto con el objetivo de que, si los administradores no tienen presente que ya no se necesitan estas, se desactiven de manera programada.

- Capacitar de manera periódica al personal de toda la organización acerca de las buenas prácticas y el correcto uso de las herramientas de TI.

- Capacitar de manera periódica al personal administrador de las herramientas de seguridad.

- Es importante que las organizaciones estén en continuo mejoramiento y actualización de sus herramientas de seguridad ya que las amenazas cada vez son diferentes.

9. CONCLUSIONES

El desarrollo de esta monografía, ha permitido identificar la gestión de las plataformas de seguridad en varias organizaciones, que si bien pertenecen a diferentes sectores, todas cuentan con factores en común, en general se tratan de los mismos profesionales velando por un mismo fin, proteger la información sensible de la compañía y su infraestructura tecnológica, por lo tanto, es posible tener en cuenta los hallazgos encontrados a nivel general, para cualquier tipo de organización y en cualquier tamaño, dado que siempre tendrán los mismos desafíos solo que puede ser en diferentes magnitudes.

Por medio de cada uno de los resultados analizados fue posible identificar aspectos importantes para tener presentes en cuestión de aseguramiento de la infraestructura tecnológica y de la información sensible, se logró evidenciar la adquisición de plataformas de seguridad en todas las organizaciones que demuestran interés en proteger su información, sin embargo, existen aún varias necesidades para mejorar la gestión de las mismas.

De nada sirve mucha seguridad si no existen procesos claros para ejercer los controles necesarios para que se cumplan, asa como una contraseña débil puede permitir vulnerar cualquier protección, faltas en los controles pueden dejar en riesgo la seguridad sin importar las plataformas o herramientas de seguridad que se tengan, procedimientos o controles escasos pueden generar fallas en la protección, poniendo en riesgo la infraestructura y la información.

En diferentes momentos las empresas solicitan asesoría de organizaciones externas, donde se realiza la identificación de debilidades, estos proveedores externos procede a señalar una serie de recomendaciones dependiendo los hallazgos de seguridad y el enfoque que se le da a la consultoría; las empresas solicitantes ahorrarían costos si tuvieran en cuenta normas y buenas prácticas para la planificación de distintas tareas como backups, actualizaciones y vencimiento de configuraciones, entre otras; por otra parte es clave la definición de políticas, protocolos y tareas internas, ya que las diferentes áreas tendrían que regirse a esta normatividad, es importante contar con un grupo interdisciplinar que haga seguimiento a todos estas políticas definidas para así, no solo evitar gastos adicionales en consultorías sino evitar una pago de multas por parte de la organización, lo cual se puede presentar por desconocimiento o descuido a los controles de seguridad importantes dependiendo su arquitectura y soluciones.

Es común que en cualquier tipo de organización, sin tener en cuenta la cantidad de empleados, usuarios o tipo de negocio hayan deficiencias en temas de

administración y gestión de la seguridad informática, a veces se tienen implementadas diferentes herramientas pero no se parametrizan de la manera ideal, estos errores son comunes no solo en la parametrización de las herramientas sino también al momento de establecer protocolos de comunicación entre dispositivos bien sea para temas de monitoreo, logs o administración; al realizar la revisión de otros aspectos se pueden encontrar deficiencias en las tareas de gestión como vulnerabilidades, muchas veces no se tienen definidos periodos o roles para la ejecución de esto, lo cual es importante para tener un patrón y realizar un seguimiento.

El análisis desarrollado, en ningún momento pretendía descifrar o responder grandes interrogantes que quizá no tengan solución, al contrario, es posible que toda la información recolectada en el documento ya sea conocida por las organizaciones, sin embargo, siguen presente, por lo tanto, es posible que el análisis apoye la toma de decisiones o la realización de acciones que puedan ser a corto, mediano y largo plazo.

El mundo de seguridad informática es muy amplio y se puede considerar un campo de batalla en donde se encuentran atacantes que buscan nuevas técnicas o vulnerabilidades que les permitan cumplir con sus objetivos ideológicos o lucrativos, generando incidentes de seguridad para las organizaciones en donde pueden reflejarse con pérdidas financieras o afectación de su imagen por ser víctimas de cualquier incidente de seguridad. Por lo anterior, los profesionales de seguridad informática requieren mejorar a diario su seguridad, verificar el estado de su infraestructura tecnológica, resolver los incidentes que se presenten y analizar su estado de seguridad permanentemente, mejorando las configuraciones que se tengan y cerrando nuevas brechas que se presenten.

10. RECOMENDACIONES

Realizar un análisis de riesgos de las aplicaciones de acuerdo con los procesos que realiza el cliente final abordando como un único conjunto todos los sistemas que intervienen en esta labor, al implementar un análisis de riesgos permitirá agilidad en el proceso y facilidad en la asignación de valores de impacto o riesgo, se puede decir que al momento de realizar un análisis de este tipo se logrará identificar diferentes amenazas, vulnerabilidades sobre la plataforma tecnológica de una organización esto puede dar paso a generar un plan de implementación de controles que aseguren un ambiente informático seguro, bajo los criterios de disponibilidad, confidencialidad e integridad de la información.

Diseñar un plan de auditoria que brinde mayor seguridad a la organización seleccionada y a la protección de la información para ser más competitiva y así identificar diferentes falencias que pueden afectar los procedimientos de las áreas de trabajo, es importante que las organizaciones cuenten con una constante evaluación y así tendrán un mayor control en caso de que se materialice una amenaza e impida la continuidad del negocio.

Implementar una solución de seguridad enfocada a la protección de los datos personales de los usuarios de aplicaciones públicas que brinden servicios de su empresa de acuerdo con la ley 1581 de 2012, es indispensable para todas las organizaciones custodiar los datos de los usuarios, ya sea de personal interno como externo, así mismo garantizar que el uso que se le esté dando a la información sea únicamente la autorizada, algunas brindan servicios publicados en la nube y no se da el tratamiento adecuado a la información personal de los usuarios.

11. BIBLIOGRAFÍA

ÁLVAREZ, L. J., (2005) “Seguridad en informática (auditoria de sistemas)”

BORGHELLO, C. (2010). Vulnerar para Proteger. Obtenido de http://www.seguinfo.com.ar/proteccion/vulnerar.htm

CARDONA, S. F., (1999) “Diseño de una red “LAN” para la Secretaria de Salud de Santafé de Bogotá”, Universidad Javeriana, Bogotá, Colombia.

CASTRO, L. (2010). About.com. Obtenido de ¿Qué es spyware?: http://aprenderinternet.about.com/od/SeguridadPrivacidad/a/Que-Es-Spyware.htm

CORTES, E. (2009). Blog La columna lítica y otros escritos. Obtenido de http://ernestocortes.blogspot.com/2009_01_01_archive.html

FEREVER, R. (2011). SITESEG. Recuperado el 2012, de Metodología recomendad para el análisis de vulnerabilidad: www.siteseg.com

GUTIERREZ, C. (2012). AUDITORIA INFORMATICA ISO/IEC 27000. (s.f.). Obtenido de ISO 27000: http://www.iso27000.es/download/doc_iso27000_all.pdf

IBARRA, D. (1980). Diccionario de la lengua Castellana compuesta por la Real Academia Española. Impresor de Cámara de S.M y de la real academia Española.

LÓPEZ GARCÍA, J. (2011). EDUTEKA. Obtenido de RECOMENDACIONES PARA CREAR CONTRASEÑAS ROBUSTAS.

MARKUS, E. (2009). Gestión de Riesgo en la seguridad informática. Obtenido de Blog de WordPress.com: http://protejete.wordpress.com/gdr_principal/retos_seguridad/

MELÍAN, M. (2011). Introducción a la Seguridad Informática. Obtenido de UNED: https://www.uned.es/ 413042/material/IntroSefInformatic

MURIEL, P. J., (2010)" Desarrollo de una red LAN para campus universitario a partir de las exigencias tecnológicas y comparaciones económicas"

VERGARA, K. (2011). Blog Informático. Obtenido de software, aplicaciones web, seguridad informática y muchos más.: http://www.bloginformatico.com/amenazas-informaticas-mas-comunes.php.

_____ Blog Informático. Obtenido de Virus informático: Bombas lógicas o de tiempo: http://formacion15.wordpress.com/2010/04/30/virus-informatico-bombas-logicas-o-de-tiempo/

WULFFERT W. A., Wulffert B. K., (2003) "Estructura de una red LAN/WAN", Universidad Javeriana, Bogotá, Colombia.

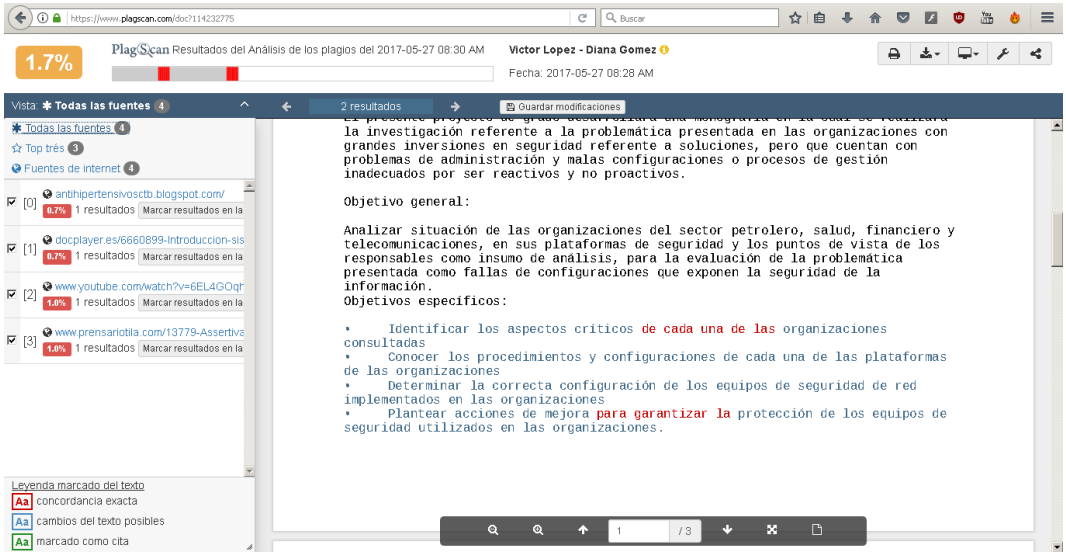
XIMO, as. (2012). ¿Qué son los troyanos? ¿y los virus? ¿y los gusanos? Obtenido de http://ximoas.blogspot.com/2012/04/que-son-los-troyanos-y-los-virus-y-los.html

12. ANEXOS

12.1 ANEXO A

Para garantizar el trabajo desarrollado, se ha ejecutado la revisión antiplagio por medio de las aplicaciones PlagScan y Turnitin, de estas se obtienen los siguientes resultados

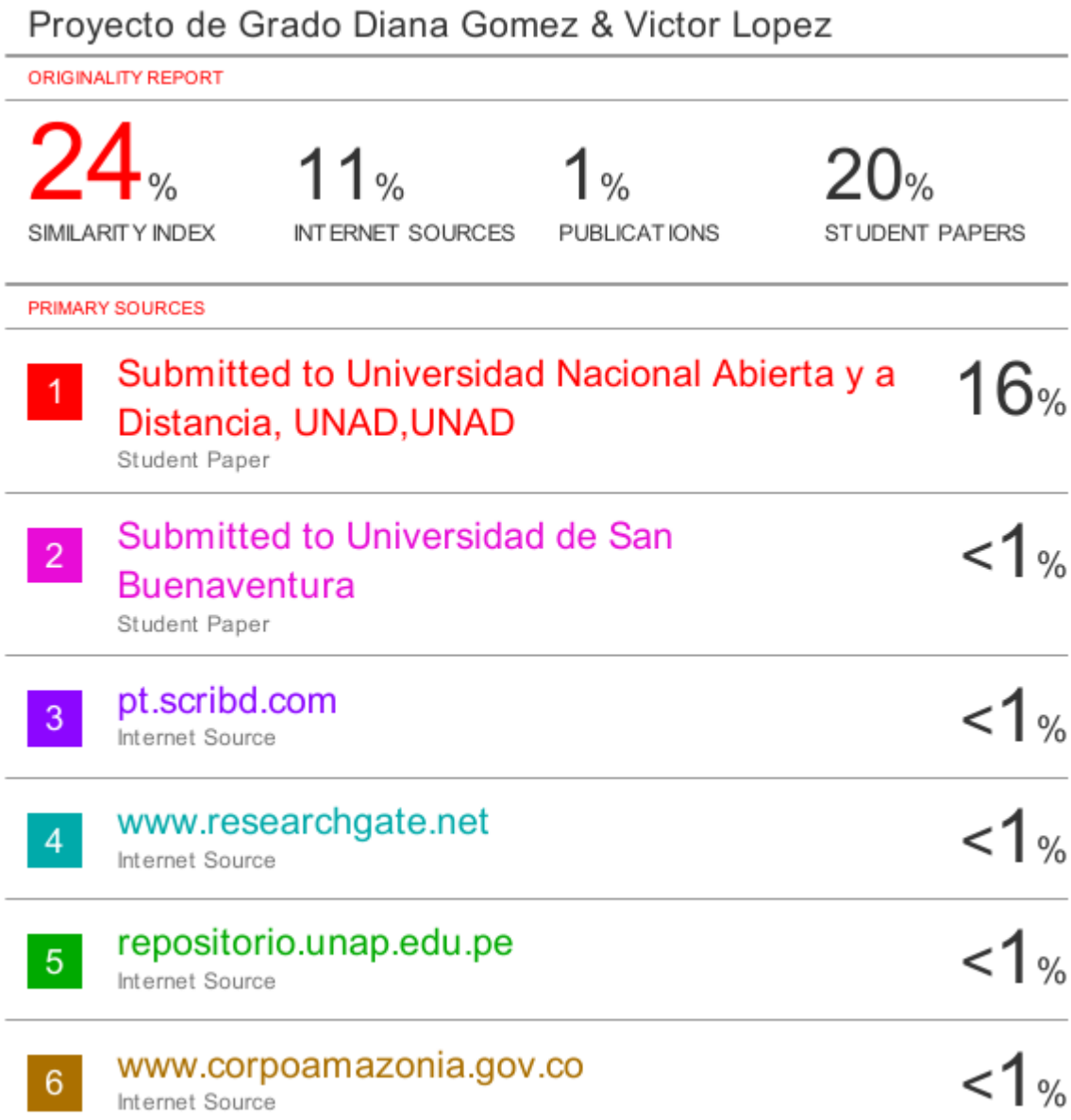
Figura 20. Revisión antiplagio página PlagScan



Fuente: https://www.plagscan.com/doc?114232775

Al realizar la revisión a través de Turnitin, se arroja un resultado del 24% similar, se aclara que esto se origina dada la referencia al documento de anteproyecto de la presente monografía, correspondiente al 16% de la revisión, por lo anterior esta evaluación se omite para el análisis. A continuación, se relaciona el resultado de la herramienta.

Figura 21. Resultado revisión antiplagio Turnitin



Fuente:https://ev.turnitin.com/app/carta/en_us/?lang=en_us&o=966013653&u=1069664871&s=&student_user=1

12.2 ANEXO B

Encuesta realizada para levantamiento de información

1. Indique el sector de la compañía donde trabaja *

- [ ] Financiero
- [ ] Gobierno
- [ ] Petrolero
- [ ] Salud
- [ ] Telecomunicaciones

2. ¿Cuál es su cargo o rol en la organización? *

_____

3. ¿Cuánto tiempo lleva en la compañía? *

- [ ] Menos de 1 año
- [ ] 1 a 2 años
- [ ] 2 a 3 años
- [ ] 3 a 5 años
- [ ] más de 5 años

4. ¿Cuál es el número de empleados de la compañía? *

- [ ] 0-50
- [ ] 51-100
- [ ] 100-200
- [ ] 200-500
- [ ] más de 500

5. ¿Qué tipo de información maneja la compañía? *

- [ ] Sensible (Requiere controles de acceso)
- [ ] Secreta (Ningún empleado o personal externo debe acceder a la información, está reservada para unos pocos)
- [ ] Confidencial (Se requiere pertenecer a un grupo determinado para acceder a la información)
- [ ] Pública (Cualquier empleado o personal externo puede tener acceso a la información)

6. Teniendo en cuenta que la integridad de la información es la propiedad que busca mantener los datos libres de modificaciones no autorizadas, ¿Considera que las soluciones actuales en la compañía ayudan a cumplir esta propiedad de la información? *

- [ ] SI
- [ ] NO
- [ ] Otro:

7. Teniendo en cuenta que la confidencialidad es la garantía de que la información personal sea protegida para que no sea divulgada sin consentimiento de su propietario ¿Considera que las soluciones actuales en la compañía ayudan a cumplir esta garantía? *

- [ ] SI
- [ ] NO
- [ ] Otro:

8. Teniendo en cuenta que la disponibilidad es un servicio que garantiza que los usuarios autorizados tengan acceso a la información ¿Considera que las soluciones actuales en la compañía ayudan a cumplir esta garantía? *

- [ ] SI
- [ ] NO
- [ ] Otro:

9. Conoce usted si la compañía cuenta con políticas establecidas para configuración de dispositivos de seguridad. *

- [ ] Si
- [ ] No
- [ ] Desconozco si existe el procedimiento.

10. Conoce usted si la compañía ha sufrido últimamente de algún incidente de seguridad de la información: *

- [ ] Si, hace menos de 1 mes
- [ ] Si, hace menos de 6 meses
- [ ] Si, en el último año
- [ ] Si, en los últimos 3 años
- [ ] No, al menos en los últimos 3 años

11. Considera que las políticas y controles que se tienen implementadas son *

- [ ] Suficientes
- [ ] Escasos
- [ ] Limitados
- [ ] Insuficientes

12. Cuáles dispositivos o soluciones de seguridad tienen en la compañía (Seleccione todas las que corresponde) *

- [ ] Antivirus
- [ ] Firewall Perimetral
- [ ] Firewall interno
- [ ] IPS / IDS
- [ ] Control y protección de navegación
- [ ] Protección de correo o AntiSpam
- [ ] Web Application Firewall
- [ ] Database Firewall
- [ ] Data Loss Prevention
- [ ] SIEM
- [ ] Protección de amenazas avanzadas
- [ ] Protección de portales
- [ ] Network Access Control
- [ ] Gestión de Vulnerabilidades o Virtual Patch
- [ ] Otro:

13. En su mayoría, ¿Quién administra las soluciones de Seguridad? *

- [ ] Personal interno de la organización
- [ ] Terceros - Personal Outsourcing

14. Conoce si el personal encargado de la seguridad informática de la organización es: *

- [ ] Suficiente, Se cuenta con personal idóneo y altamente capacitado que administra cada solución con las mejores prácticas y aprovechando todas las funcionalidades de cada una de estas.
- [ ] Es suficiente, con conocimientos intermedios que permiten atender los requerimientos del dia a dia
- [ ] Está bien, se administra por personal interno o tercerizado con conocimientos básicos de acuerdo a los requerimientos actuales, aunque no se logran aplicar todas las funcionalidades de las soluciones.
- [ ] Resulta escasa la gestión, generalmente se atienden los requerimientos urgentes y otros tardan mucho tiempo en aplicarse y no hay manera de aplicar nuevas funcionalidades.
- [ ] Las soluciones no cuentan con un administrador especifico, todo el equipo del área sin mucho conocimiento genera las configuraciones según los requerimientos de la compañía.

15. Teniendo en cuenta la solución de Antivirus que actualmente tienen en la compañía donde trabaja, considera que *

- [ ] Es buena y está siendo bien utilizada
- [ ] Es buena pero no se usa adecuadamente
- [ ] Es regular, brinda la protección mínima necesaria
- [ ] Es mala, no posee las capacidades que actualmente requieren este tipo de soluciones
- [ ] No se tiene protección antivirus.

16. Teniendo en cuenta la solución de Antivirus que actualmente tienen en la compañía, sabe si cuenta con los siguientes módulos activos (seleccione todos los que aplique): *

- [ ] Firewall
- [ ] Data Loss Prevention
- [ ] Cifrado
- [ ] Control de Navegación
- [ ] Control de Aplicaciones
- [ ] HIPS
- [ ] Ninguna - Solo Antivirus
- [ ] Otro:

17. Teniendo en cuenta la solución de Firewall que actualmente tienen en la empresa donde trabaja, considera que: *

- [ ] Es buena y está siendo bien utilizada
- [ ] Es buena pero no se usa adecuadamente
- [ ] Es regular, brinda la protección mínima necesaria
- [ ] Es mala, no posee las capacidades que actualmente requieren este tipo de soluciones

18. Teniendo en cuenta la solución de Firewall que actualmente tienen en la empresa donde trabaja y sus funcionalidades, sabe si cuenta con los siguientes módulos activos (seleccione todos los que aplique): *

- [ ] IPS / IDS
- [ ] Antivirus
- [ ] Control de Navegación
- [ ] Control de Aplicaciones
- [ ] Control de Malware y amenazas avanzadas
- [ ] Ninguna - Solo firewall
- [ ] Otro:

19. Existe en la empresa plan de actualización de versiones de los Sistemas Operados (Seleccione el más aproximado). *

- [ ] Mensual

- [ ] Trimestral
- [ ] Semestral
- [ ] Anual
- [ ] No existe un plan periódico de actualizaciones.

20. Cada cuanto se debe realizar el cambio de credenciales en los dispositivos que son administrados por usted: *

- [ ] Entre 1 y 3 meses después del último cambio.
- [ ] Entre 3 y 6 meses después del último cambio.
- [ ] Entre 6 y 9 meses después del último cambio.
- [ ] Cada año después del último cambio.
- [ ] No se tiene una política establecida.

21. Es permitido el acceso a los dispositivos que están bajo su administración desde cualquier punto de la red: *

- [ ] Si
- [ ] No

22. Se realiza periódicamente auditorías de seguridad: *

- [ ] Si, entre cada 1 y 3 meses.
- [ ] Si, entre cada 3 y 6 meses.
- [ ] Si, entre cada 6 y 9 meses.
- [ ] Si, entre cada 9 y 12 meses.
- [ ] No se realiza análisis de efectividad.

23. De acuerdo con su precepción, la seguridad informática en la empresa donde trabaja es: *

- [ ] Excelente
- [ ] Buena
- [ ] Regular
- [ ] Mala

24. En su mayoría, ¿Qué tipo de incidentes de seguridad de la información se presentan? *

_____

25. ¿Cuáles son los mayores obstáculos que se presentan para mejorar la seguridad de la información? *

_____

26. ¿Se cuenta con inversión suficiente para mejorar la seguridad de la información? *

- [ ] Si
- [ ] NO
- [ ] Otro:

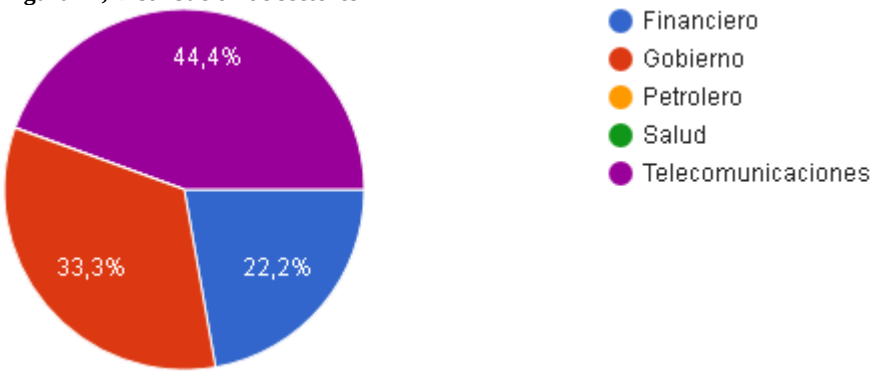
12.3 ANEXO C

Resultados obtenidos de la encuesta

A continuación, se presenta el detalle de las respuestas obtenidas

1. Sector de la compañía

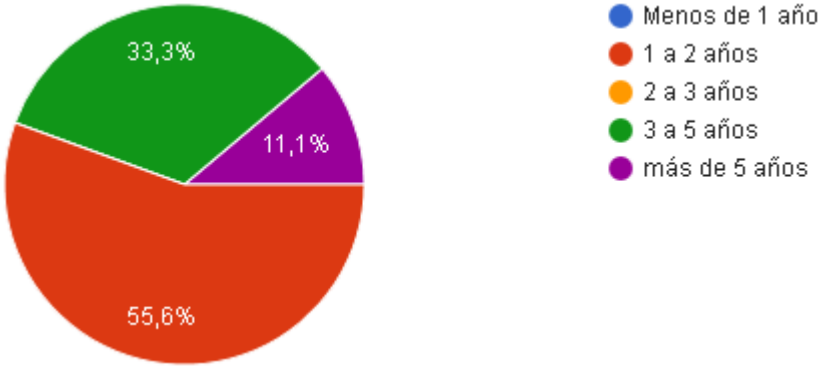
Figura 22, Distribución de sectores



Fuente: Resultados encuesta de Monografía

2. Tiempo trabajando en la compañía

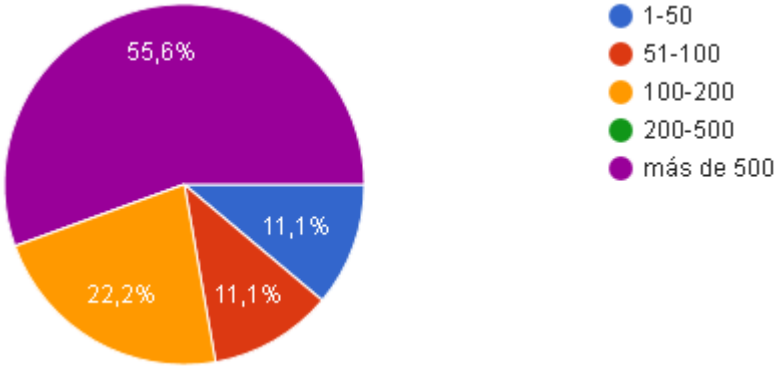
Figura 23, Distribución por antigüedad



Fuente: Resultados encuesta de Monografía

3. Número de empleados en la compañía

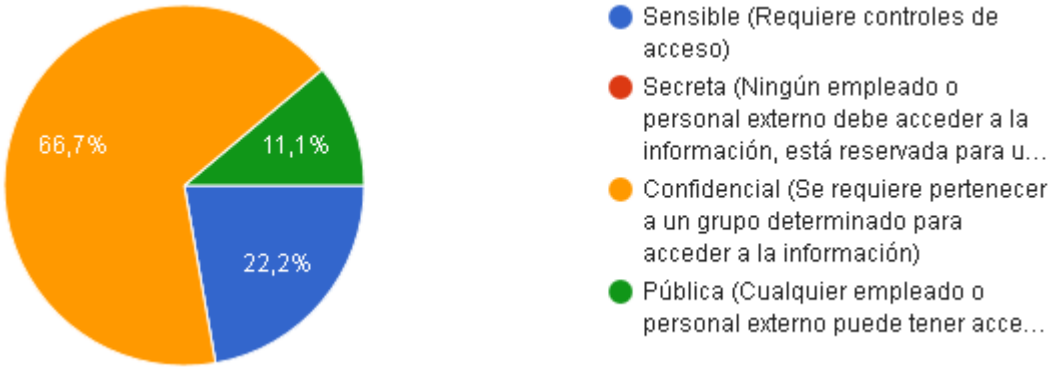
Figura 24, Distribución por número de empleados



Fuente: Resultados encuesta de Monografía

4. Tipo de información de la compañía

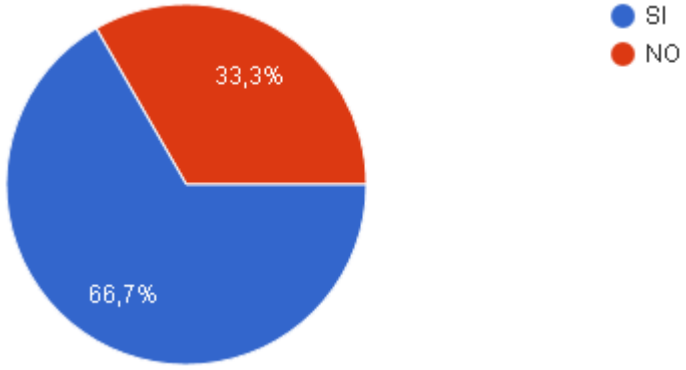
Figura 25, Distribución por tipo de información



Fuente: Resultados encuesta de Monografía

5. Cumplimiento de Disponibilidad de la información en la compañía

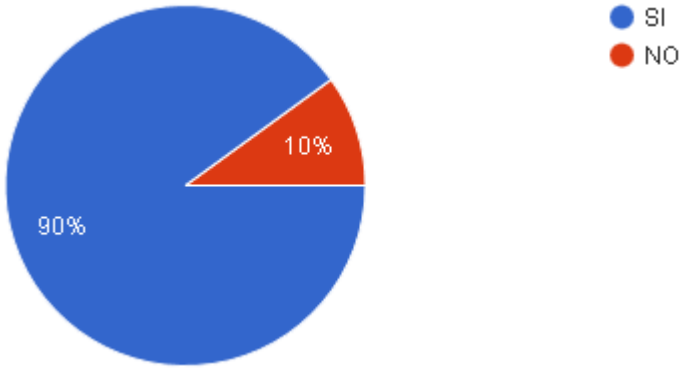
Figura 26, Distribución de cumplimiento de Disponibilidad



Fuente: Resultados encuesta de Monografía

6. Cumplimiento de Integridad de la información en la compañía

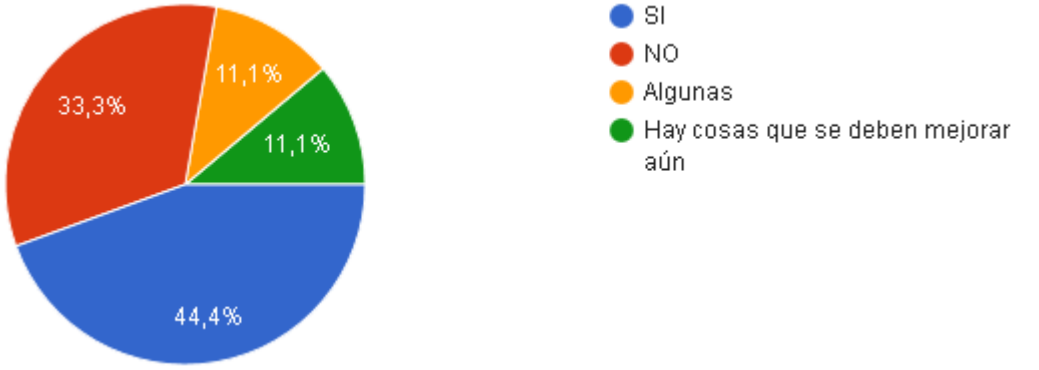
Figura 27, Distribución de cumplimiento de Integridad



Fuente: Resultados encuesta de Monografía

7. Cumplimiento de Confidencialidad de la información en la compañía

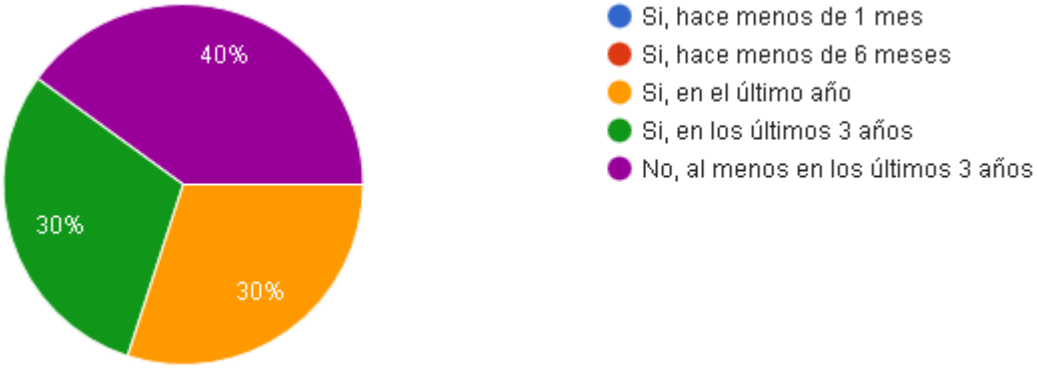
Figura 28, Distribución por cumplimiento de confidencialidad



Fuente: Resultados encuesta de Monografía

8. Registro de último incidente

Figura 29, Distribución de registro de incidentes



Fuente: Resultados encuesta de Monografía

9. Tipos de Incidentes más comunes

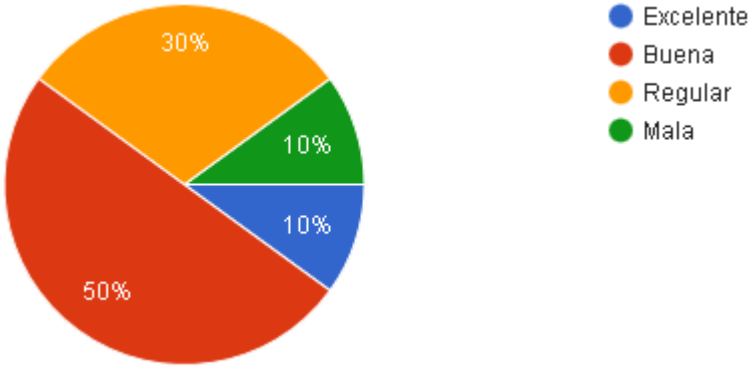
Figura 30, Listado de incidentes comunes

robo
Phishing
Denegación de Servicio
fuga de informacion
Ddos
No hay controles
navegacion a sitios inseguros
perdida de información
Amenazas de virus
Ninguno

Fuente: Resultados encuesta de Monografía

10. Percepción de seguridad de la información

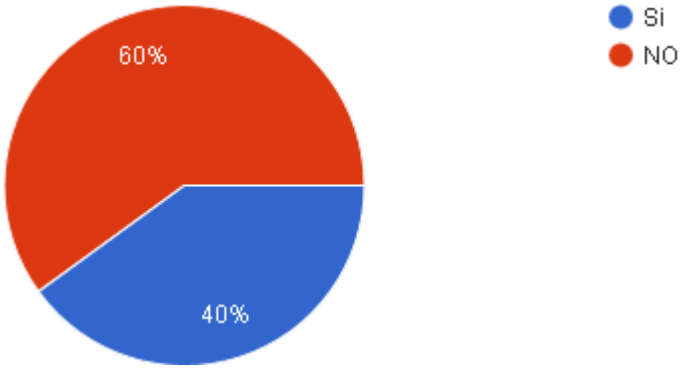
Figura 31, Distribución de percepción de seguridad



Fuente: Resultados encuesta de Monografía

11. Optima Inversión en seguridad de la información

Figura 32, Distribución de percepción en inversión



Fuente: Resultados encuesta de Monografía

12. Inconvenientes para mejorar la seguridad de la información

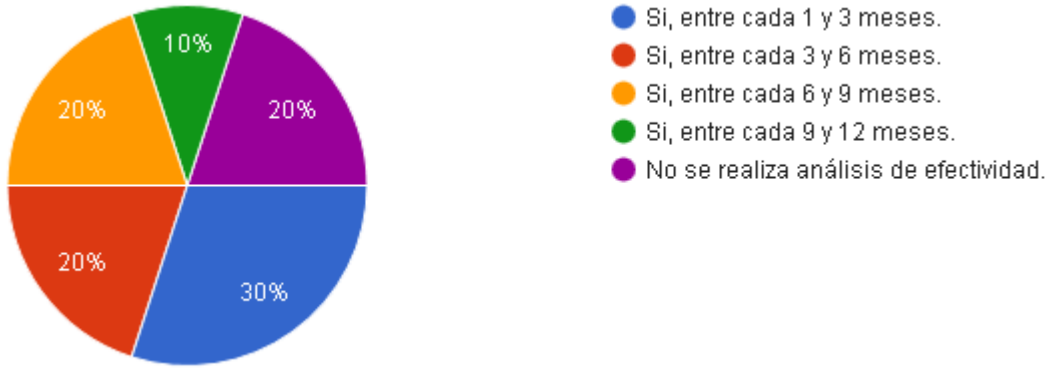
Figura 33, Listado de inconvenientes de mejora

cultura
La escases de personal, y la falta de recursos para implementar nuevas herramientas.
Roles y responsabilidades mal definidos
divulgcion de politicas
Economico
Miedo al cambio
Presupuesto
tiempo
Falta de presupuesto para conseguir equipos que brinden mejor cobertura
No aplica

Fuente: Resultados encuesta de Monografía

13. Ejecución de auditorías de seguridad

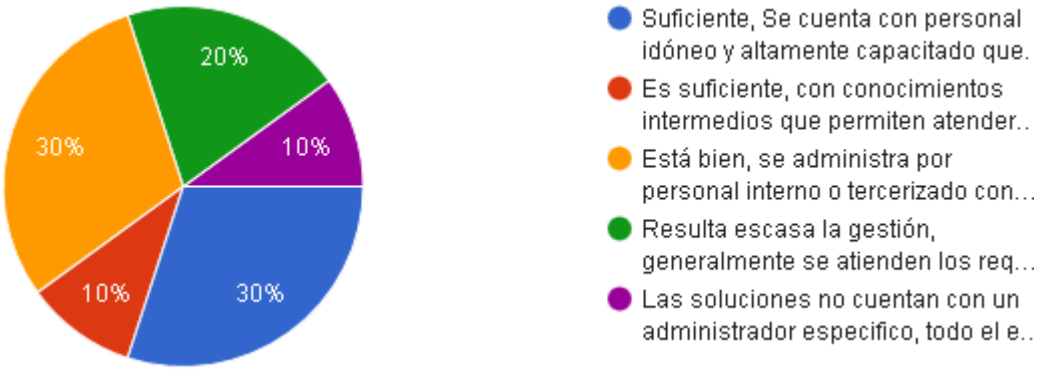
Figura 34, Distribución de periodicidad de auditorías de seguridad



Fuente: Resultados encuesta de Monografía

14. Madurez de nivel de personal encargado de las soluciones de seguridad

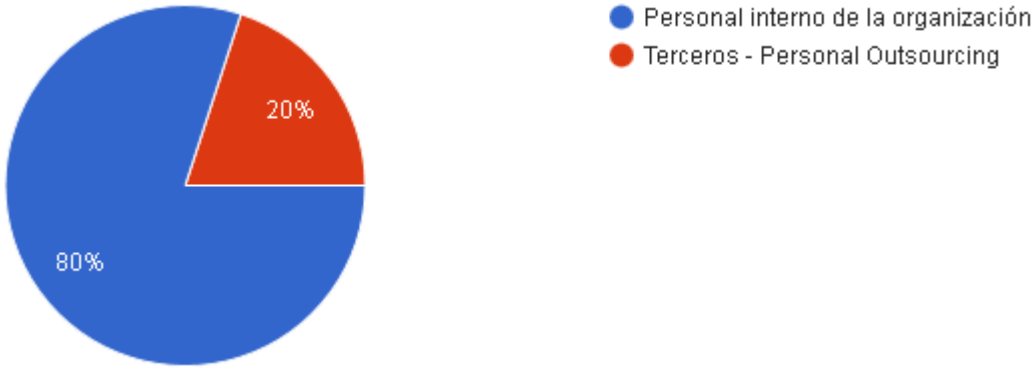
Figura 35, Distribución por madurez de administradores



Fuente: Resultados encuesta de Monografía

15. Composición del personal administrador de plataformas

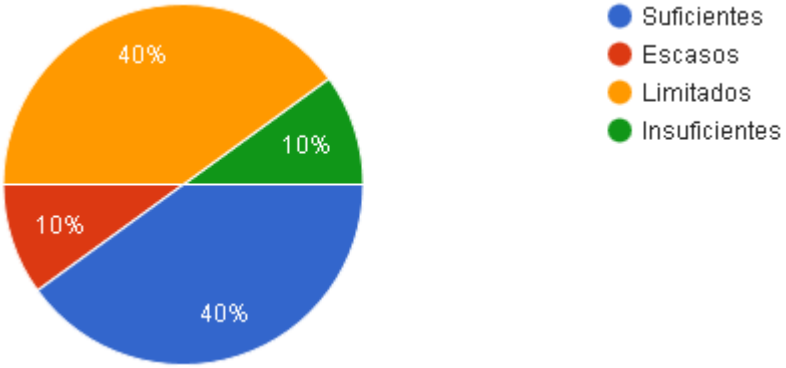
Figura 36, Distribución por personal administrador



Fuente: Resultados encuesta de Monografía

16. Estado de políticas y controles aplicados

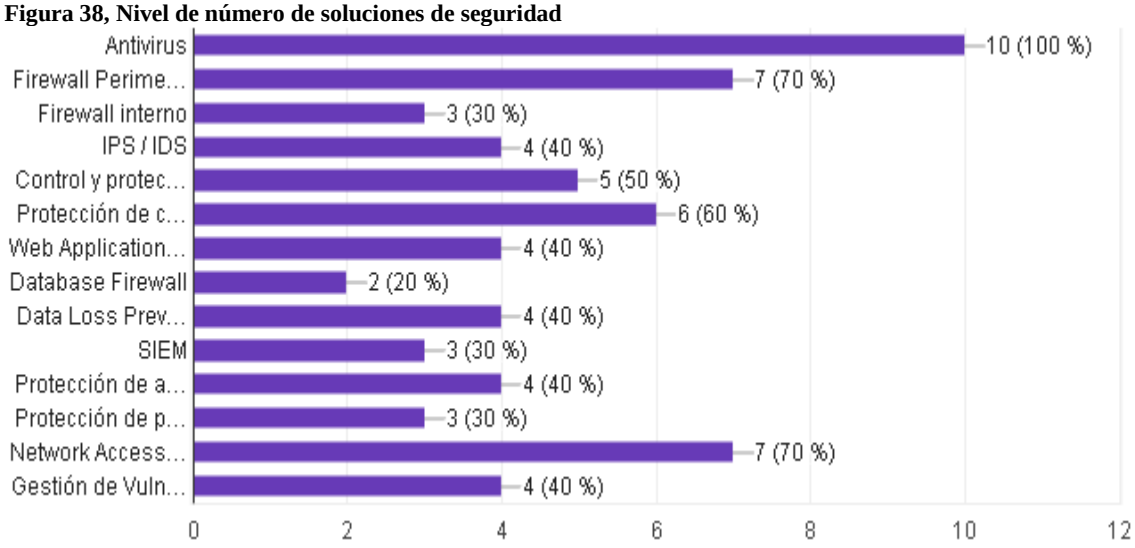
Figura 37, Distribución por estado de controles y políticas



Fuente: Resultados encuesta de Monografía

17. Soluciones de seguridad implementadas

Figura 38, Nivel de número de soluciones de seguridad



Fuente: Resultados encuesta de Monografía

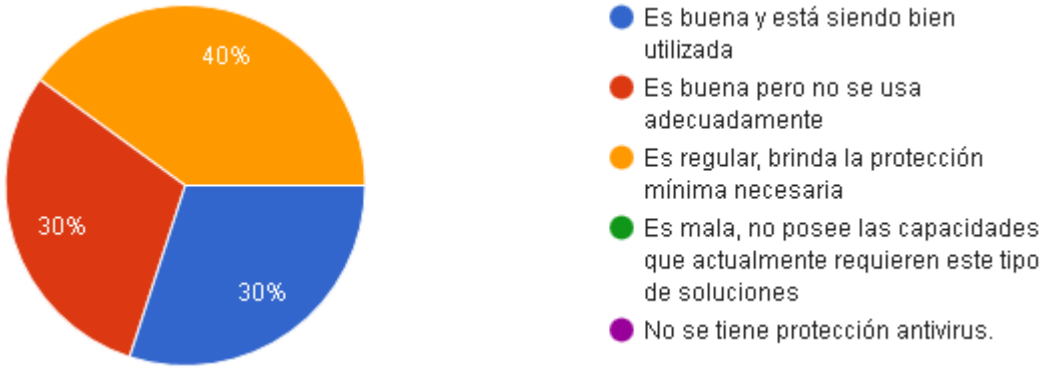
18. Percepción de la configuración del Firewall

Figura 39, Distribución por percepción de configuración del firewall

Fuente: Resultados encuesta de Monografía

19. Percepción de la configuración del Antivirus

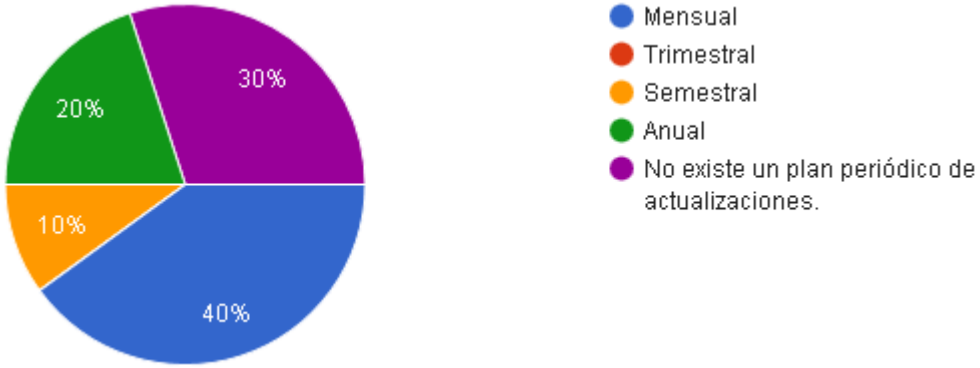
Figura 40, Distribución por percepción de configuración del Antivirus



Fuente: Resultados encuesta de Monografía

20. Ejecución de actualizaciones de los dispositivos y servicios

Figura 41, Distribución por percepción de actualizaciones



Fuente: Resultados encuesta de Monografía