Propuesta de Análisis de Política de Ciberseguridad de la empresa PEI AM

German David Arias Garzón, Lizbeth Vanesa Ávila González, Jahan Andrey Cárdenas Cortez, Cristian David Saavedra Pardo

Especialista en Seguridad informática, Fundación Universitaria Compensar

Proyecto fin de grado

Docente

Miguel Pérez Pereira

22 de noviembre de 2023

Esta obra está bajo una Licencia Creative Commons Atribución-NoComercial-Compartir Igual 4.0 Internacional.

Propuesta de Análisis de Política de Ciberseguridad de la empresa PEI AM

German David Arias Garzón, Lizbeth Vanesa Ávila González, Jahan Andrey Cárdenas Cortez, Cristian David Saavedra Pardo

Trabajo de grado presentado como requisito parcial para optar al título de:

Especialista en Seguridad informática

Director:

Jairo Gómez

Docente:

Miguel Pérez Pereira

Fundación Universitaria Compensar

Facultad de Ingeniería

Especialización en Seguridad Informática

Bogotá, Colombia

2023

Resumen

El objetivo de este documento es analizar la Política de ciberseguridad implementada por la empresa Pei Asset Management (PEI AM), Para proponer una reestructuración y actualización de esta política según los estándares establecidos por los Controles CIS en su versión 8. El análisis detallado de la política abarca las directrices aplicadas para la seguridad cibernética de la compañía, da descripción y funcionalidad de los Controles CIS.

Una parte crucial de este documento es el análisis comparativo entre la política de ciberseguridad de PEI AM y los Controles CIS. Este análisis permitirá identificar puntos de convergencia, verificando el nivel de alineación de la política actual con el conjunto de buenas prácticas establecido por la CIS. Así mismo, se resaltarán posibles áreas de mejora donde la política interna de la compañía podría reforzarse para cumplir de manera más efectiva.

Palabras clave: Ciberseguridad, seguridad, infraestructura y vulnerabilidad

Abstract

The purpose of this paper is to analyze the Cybersecurity Policy implemented by Pei Asset Management (PEI AM), to propose a restructuring and updating of this policy according to the standards set by the CIS Controls in its version 8. The detailed analysis of the policy covers the guidelines applied for the company's cybersecurity, gives description and functionality of the CIS Controls.

A crucial part of this document is the comparative analysis between PEI AM's cybersecurity policy and the CIS Controls. This analysis will allow identifying points of convergence, verifying the level of alignment of the current policy with the set of best practices established by the CIS. It will also highlight possible areas of improvement where the company's internal policy could be strengthened to comply more effectively.

Keywords: Cybersecurity, security, infrastructure and vulnerability.

Contenido

PÁG.

RESUMEN **3**

INTRODUCCIÓN **6**

ANTECEDENTES Y JUSTIFICACIÓN 6
FORMULACIÓN DEL PROBLEMA 7
OBJETIVO GENERAL 8
Objetivos Específicos *8*
ALCANCES Y LIMITACIONES 8

1. MARCO TEÓRICO **9**

1.1 CONCEPTOS BÁSICOS 9
1.1.1 Ciberseguridad *9*
1.1.2 Vulnerabilidades *9*
1.1.3 Ataques Informáticos *9*
1.1.4 Política de Ciberseguridad *10*
1.2 CENTRO DE SEGURIDAD EN INTERNET [CIS] 11
1.2.1 Controles CIS *11*

2. DISEÑO METODOLÓGICO **14**

2.1 ANÁLISIS DE LA POLÍTICA DE CIBERSEGURIDAD 14
2.2 EVIDENCIA DE LAS CARACTERÍSTICAS FALTANTES 15
2.3 PROPUESTA 17

3. RESULTADOS **18**

4. CONCLUSIONES Y RECOMENDACIONES **19**

BIBLIOGRAFÍA **20**

Introducción

Actualmente, los sistemas informáticos son un tema importante para las organizaciones, ya que estos activos manejan información de procesos sensibles, donde evidencian el funcionamiento y las áreas de mayor impacto. La empresa PEI AM, se dedica al sector inmobiliario desde 2006 y administra activos a nivel nacional, tiene una sede única en Bogotá donde se realiza la operación principal de sus servicios, la empresa cuenta con sistemas informáticos vitales para su funcionamiento, por eso los ataques cibernéticos se han convertido en un foco de preocupación constante, pues pueden generar pérdidas monetarias o de información generando problemas de seguridad.

PEI AM, toma la iniciativa de implementar una política de ciberseguridad que permita mitigar ataques, ya que, por ser una empresa del sector inmobiliario, almacena datos de clientes e inversionistas, todos estos datos se encuentran en sistemas de información utilizados para consultar según su necesidad y el estado de los activos. Es por esto, que la ciberseguridad debe ser su prioridad para garantizar la integridad de los activos informáticos y de los datos tratados, y así mitigar la explotación de vulnerabilidades.

Antecedentes y Justificación

La ciberseguridad se ha convertido en un aspecto crítico para la sostenibilidad y la confianza en las organizaciones para la era digital. PEI AM, en aras de su potencial crecimiento ha optado por seguir un modelo de transformación digital, que permite administrar información los de inversionistas y clientes, mejorando y optimizando múltiples procesos organizacionales.

Gestionar la información financiera y los datos sensibles de los clientes, enfrenta riesgos sustanciales de ciberataques y brechas de seguridad, de ahí la importancia de analizar y sugerir actualizar la Política que permita establecer acciones de mejora y un mayor control en la administración de herramientas informáticas de la organización, dicha política debe enmarcar procedimientos e ítems para mitigar futuras vulnerabilidades que puedan provocar daños de mayor impacto para sistemas informáticos de la organización.

La implementación por parte de la empresa de una política de ciberseguridad basada en la ISO 27001:2013 en el año 2022 evidencia su compromiso inicial con la protección de la información, dicha política se empezó a documentar durante el segundo semestre del año 2022, sin embargo, en un panorama en constante cambio, esta política debe evolucionar para abordar las últimas amenazas y desafíos, lo cual justifica este proyecto, ya que siempre existirá la necesidad imperante de garantizar que los controles de seguridad estén actualizados y sean eficaces, en línea con los estándares actuales representados por los Controles del Center for Internet Security [CIS].

Formulación del Problema

Pei Asset Management, es una empresa privada creada en el año 2006, enfocada en la estructuración y administración de portafolios de inversión inmobiliaria en Colombia, actualmente cuenta con alrededor de 8 billones de pesos en activos inmobiliarios, su sede principal se encuentra ubicada en la ciudad Bogotá, donde se desarrolla toda su operación, estos procesos se realizan por medio de herramientas informáticas que apoyan y facilitan la ejecución de las actividades.

Como parte de su proceso de crecimiento, la compañía realiza la implementación de una Política de Ciberseguridad, para mitigar riesgos de intrusión o afectaciones a los activos informáticos de la compañía, en la actualidad se conocen nuevos métodos de ataques para extraer información poniendo en riesgo la integridad del sistema.

El problema principal de la política de ciberseguridad de la empresa PEI AM está en su diseño e implementación, adicional a que esta se encuentra basada en la ISO 27001 del 2013, actualmente existe una organización sin ánimo de lucro llamado Center for Internet Security (CIS) que genera un listado de controles específicos orientados a la ciberseguridad, en donde se genera un número mayor de controles a ejecutar para así mitigar vulnerabilidades que lleguen a presentarse en un futuro.

Objetivo General

Proponer una evaluación de las políticas de Ciberseguridad de la empresa PEI AM basados en los Controles CIS en su versión 8, con el fin de identificar las falencias y vulnerabilidades en sus sistemas informáticos.

Objetivos Específicos

- Analizar la Política actual de Ciberseguridad implementada en PEI AM, con el fin de valorar y evaluar los procedimientos y controles establecidos.
- Evidenciar las características faltantes de la política de Ciberseguridad actual de la empresa, alineados a los 18 controles CIS Versión 8.
- Proponer recomendaciones que permita actualizar la política de ciberseguridad de la empresa.

Alcances y Limitaciones

Se propone un análisis detallado de la Política de Ciberseguridad de PEI AM para alinearlo a los controles establecidos por las CIS versión 8, cuyo análisis pretende sugerir modificaciones que mejoren el cumplimiento y control en esta política, elevando el nivel de seguridad. Este análisis servirá como base para que la empresa pueda ajustar su política de ciberseguridad, y así robustecer su infraestructura tecnológica.

Es claro que en esta investigación se hace una propuesta y depende de los directivos de la empresa para su implementación, por otro lado, se sabe que el éxito de cualquier política está en su correcta divulgación, ya que los usuarios internos y externos la encargan de poner en práctica.

1. Marco teórico

1.1 Conceptos Básicos

1.1.1 Ciberseguridad

La Ciberseguridad hace referencia a los procedimientos y herramientas utilizadas para proteger el activo más importante de las organizaciones, como la información y todos los mecanismos de comunicación utilizados, ya que las organizaciones pueden ser blanco de los ciberdelincuentes, que aprovechan cualquier momento y brecha de seguridad para introducirse en la red.

Por el avance exponencial de internet y los sistemas informáticos, ha crecido la información digital resguardada por las empresas, por lo que esto ocasionó una normalización de nuevos modelos de servicio en múltiples sectores, generando mayor responsabilidad para las entidades. (*¿Qué Es La Ciberseguridad? - Explicación de La Ciberseguridad - AWS*, n.d.)

1.1.2 Vulnerabilidades

Una vulnerabilidad es cualquier debilidad o alteración en un sistema informático, que pueden generarse tanto a nivel de hardware como de software, que representa un potencial riesgo a nivel personal y de las organizaciones, ya que los ciberdelincuentes las usan para acceder a los sistemas robar, alterar o secuestrar la información, para cometer actos delictivos que afectan a las víctimas. (Quiroz-Zambrano I Universidad Laica Eloy Alfaro de Manabí & Macías-Valencia, 2017)

1.1.3 Ataques Informáticos

Un ataque informático es conocido como la intención organizada de afectar la confidencialidad, integridad y disponibilidad de la información, aprovechando las debilidades o puntos frágiles que puedan presentar a nivel de hardware o software, los atacantes pueden acceder o realizar alteraciones en el funcionamiento de un sistema, para extraer, alterar o secuestrar información almacenada en los dispositivos. (Mieres, n.d.) Actualmente podemos encontrar múltiples tipos de ataques informáticos, pero dentro de los más comunes están:

Malware: Es un software informático con fines maliciosos e interceptar la información para afectar equipos informáticos clasificado como Virus, Gusanos o Troyanos, habitualmente es distribuido mediante correo electrónico, dispositivos de almacenamiento, descargas, etc. (*Malware*, n.d.)

Spyware: Software malicioso, su función principal es tomar la mayor cantidad de información relacionada a datos confidenciales como cuentas bancarias etc., la manera más común de ser instalado en un equipo es mediante la infiltración de software licenciado. (Castillo-Pérez et al., n.d.)

Ransomware: Malware que busca cifrar la información almacenada en los sistemas de información, solicitando pagos para entregar a la víctima una clave de descifrado y restaurar los sistemas, en varias ocasiones la clave suministrada luego del pago no funciona. (Castañaga et al., n.d.)

Phishing: Técnica que busca engañar para obtener datos personales, claves, números de cuenta, etc., suplantando organizaciones legitimas, llamadas, mensajes de texto, correos electrónicos o sitios web fraudulentos. (Guaña-Moya et al., n.d.)

Denegación de servicio (DOS): El objetivo de este es sobrecargar un sistema informático, realizando múltiples y constantes peticiones hacia un recurso bloqueando el acceso a este, volviéndolo inaccesible. (Edgar Fabricio Rivera Osorio. et al., 2020)

1.1.4 Política de Ciberseguridad

Una política de ciberseguridad es un conjunto de procedimientos informáticos establecidos por las organizaciones, para proteger la información y evitar ciberataques o brechas de seguridad que afecten sus sistemas. Una Política es implementada en las organizaciones para establecer directrices, el manejo de la información y el acceso a los sistemas, se definen pautas para el uso de los dispositivos y activos dentro de la red de la empresa, donde todos los usuarios deben estar alineamientos y conocer su nivel de responsabilidad ante los procedimientos establecidos. (Fonfría, n.d.)

1.2 Centro de Seguridad en internet [CIS]

El Centro de Seguridad en internet [CIS] es una organización sin ánimo de lucro fundada en el año 2000, enfoca en establecer la ciberseguridad orientada al desarrollo de empresas u organizaciones que buscan proteger y mantener su negocio. Los CIS permiten encaminar la implementación de políticas o procedimientos de seguridad informática orientada al modelo de negocio, factores económicos, talento humano y tecnológico que posean las organizaciones. (*Blog de Internet Security Auditors: Controles Del CIS: Novedades de La Versión 7.1*, n.d.)

1.2.1 Controles CIS

Conjunto de buenas prácticas creadas por el Centro de seguridad en internet, consideradas fundamentales para que las organizaciones mitiguen ataques cibernéticos y protejan su información almacenada en sus sistemas de datos y de telecomunicaciones, estos controles son actualizados periódicamente para abarcar las amenazas cibernéticas más actuales. El primer conjunto de controles CIS es publicado en el año 2008 con el nombre de **"Controles de Seguridad Críticos"**, de esta manera los controles han sido implementados por las compañías a nivel global, logrando un reconocimiento que posiciona a los controles CIS como referencia para la ciberseguridad de las organizaciones. (*CIS Controls: Todo Lo Que Necesitas Saber | CalCom*, n.d.)

Para el año 2022 se genera una nueva actualización que agrupa 18 controles específicos, descritos a continuación:

Tabla 1. Controles CIS

No	*Control*	*Descripción*
1	***Inventario y Control de Activos Empresariales***	Realizar inventario, monitoreo y verificación de los dispositivos informáticos enlazados a la red de la compañía tanto de manera física como virtual o remota.
2	***Inventario y Control de Activos de Software***	Documentar el inventario de software que se utiliza en la gestión empresarial, este debe ser licenciado y debe ser actualizado constantemente para salvaguardar los procesos internos y la información almacenada.

3	***Protección de los Datos***	Elaborar procesos de gestión de datos que permitan la clasificación, identificación, manejo, tiempo de preservación y eliminación de los datos almacenados.
4	***Configuración Segura de Activos y Software Empresarial***	Determinar protocolos que permitan una correcta configuración y mantener actualizado todo el hardware y software que pertenece a la organización.
5	***Administración de Cuentas***	Mantener documentada cada asignación de cuentas o cambios de permisos de los usuarios, esto garantizará dar seguimiento a cada actividad.
6	***Gestión de Control de Accesos***	Tener procesos definidos que permitan una administración funcional y actualización de los privilegios de cada usuario en los componentes empresariales.
7	***Gestión Continua de Vulnerabilidades***	Realizar procesos de revisión y seguimiento de vulnerabilidades, que permitan proteger todos los activos de la empresa.
8	***Gestión de Registros de Auditoría***	Mantener documentación que permita actuar y generar bases de conocimiento sobre auditorio o eventos de ataques registrados con anterioridad.
9	***Protección del Correo Electrónico y Navegador Web***	Establecer las prácticas de uso que mejoren la protección de cuentas de correo electrónico, garantizando lo que puede compartirse y lo que no por este medio.
10	***Defensas contra Malware***	Prevenir y controlar que, a través de las aplicaciones y herramientas de la organización, se distribuyan o propaguen virus de acciones maliciosas.
11	***Recuperación de Datos***	Establecer un plan de recuperación y restablecimiento de los sistemas de información, que permitan mantener el nivel de confianza ante cualquier evento de ataque.
12	***Gestión de la Infraestructura de Red***	Tener una correcta gestión y administración de los recursos de la red, esto permite tener el control de todos los procesos, servicios, minimizando la intención de intrusión.

13	***Monitoreo y Defensa de la red***	Implementar el control y monitoreo de la red, permitirá generar herramientas de defensa en la red y la detección temprana de intrusos o metodologías de ataque cibernético.
14	***Concientización en Seguridad y Formación de Habilidades***	Generar planes en seguridad como capacitaciones que fortalezcan los mecanismos de prevención, para que la comunidad esté informada.
15	***Gestión de Proveedores de Servicios***	Determinar perfiles para cada proveedor, prestador de servicios o tercero en la empresa, para dar responsabilidades determinadas dentro de las herramientas.
16	***Seguridad en el Software de Aplicación***	Se establece que todas las herramientas hardware y software utilizadas dentro de la empresa, estén dentro de los lineamientos del ciclo de vida, si se encuentran desactualizadas u obsoletas pueden ser vulnerables.
17	***Gestión de Respuesta a Incidentes***	Fortalece los procedimientos de respuesta ante incidentes, permite contemplar métodos que proporcionen las herramientas necesarias para prevenir, controlar y actuar en corto tiempo ante cualquier Ataque.
18	***Pruebas de Penetración***	Realizar pruebas de intrusión en los sistemas les da a conocer a las organizaciones dónde y cuáles de estos presentan vulnerabilidades, esto generando indicadores sobre la eficacia de sus mecanismos de defensa y mitigación del riesgo para salvaguardar su integridad.

(*Controles CIS*, n.d.)

2. Diseño Metodológico

Para el desarrollo del análisis de la política de ciberseguridad en la empresa PEI AM, se llevará a cabo en tres etapas fundamentales, las cuales corresponden a los objetivos específicos propuestos.

2.1 Análisis de la Política de Ciberseguridad

Actualmente la empresa cuenta con un documento denominado **"Política de ciberseguridad de la empresa PEI AM"**, dicho documento está dividido en 12 ejes principales los cuales se resumirán en la tabla 2.

Tabla 2. 12 ítems de la política en la empresa PEI AM

No	*Control*	*Descripción*
1	***Manejo de credenciales y gestión de contraseñas***	Establece parámetros a considerar para la administración de contraseñas de los sistemas informáticos dentro de la compañía, además aclara el uso exclusivo por parte del Área de TI de credenciales de administración.
2	***Uso del correo electrónico corporativo***	Determina la normativa de uso del correo electrónico corporativo para los trabajadores de la compañía, también da una serie de características que se deben tener presentes a la hora de recibir un correo electrónico de procedencia, contendido extraño o desconocido para evitar la descarga o ejecución de archivos maliciosos.
3	***Manejo del servicio de internet, redes de datos y Comunicaciones***	Decreta las prohibiciones establecidas para usar las redes de la compañía PEI AM, y específica que pueden existir excepciones según las actividades de cada usuario autorizado.
4	***Manejo adecuado de equipos de cómputo***	En general, el ciclo de vida de un equipo de cómputo, el software y su licenciamiento, además de los cuidados que deben seguir los empleados que los usarán, así como la disposición y administración de estos.
5	***Inactivación y/o bloqueo de usuarios***	Determina el control y los tiempos de respuesta para activar o inactivar un usuario en los diferentes sistemas de administración de software de la compañía ante una situación que lo ocasione (despido, cambio de cargo- área, licencia de maternidad etc.).
6	***Seguridad física y Datacenter***	Limita el acceso de los empleados y/o personal externo a los espacios de la empresa respecto a su cargo y/o responsabilidades mediante lineamientos administrativos sobre los sistemas de seguridad de acceso, además de establecer métodos de monitoreo.

7	***Administración de dispositivos y sistemas de Seguridad Perimetral***	Esta política está basada en la protección de los activos informáticos de la compañía, delegando al área de TI como encargada de realizar constantes trabajos de control sobre la información.
8	***Administración de servidores***	Enfatiza la administración de los servidores de la compañía, donde se deben tener los dispositivos actualizados y a su vez cumplir con los roles determinados para obtener acceso a los dispositivos garantizando el control de estos
9	***Respaldo de Información***	Establece criterios para la protección de datos de la compañía mediante copias de seguridad, en un tiempo considerado por la organización.
10	***Manejo de Software y licencias suministradas por PEI AM***	Establece garantías para el uso y asignación de software legal y licenciamiento con el fin de mantener en cumplimiento las obligaciones legales fortaleciendo el uso responsable de las plataformas.
11	***Manejo de la información y datos de PEI AM***	Busca garantizar siempre el tratamiento de datos administrados por PEI AM, para mantener la integridad, confidencialidad y disponibilidad de la información, limitando su circulación y disposición.
12	***Notificación de incidentes de ciberseguridad***	Determina la responsabilidad de colaboradores, trabajadores y/o terceros de notificar a la Dirección de ciberseguridad cualquier acto fuera de lo normal dentro de los sistemas de información y gestión de PEI AM.

2.2 Evidencia de las Características Faltantes

En la siguiente tabla se evidencia la comparativa de la política de ciberseguridad de PEI AM respecto a los Controles CIS, donde se relacionan diferentes puntos de la política con los mecanismos establecidos por la CIS, resaltando las deficiencias actuales.

Tabla 3. Comparativa de los controles CIS y los establecidos en la Política de PEI AM		
CONTROLES CIS	***POLITICA PEI AM***	***COMPARATIVA***
Administración de cuentas	*-Manejo de credenciales* *-Inactivación usuarios*	La Política se establece el procedimiento sobre la asignación de credenciales y responsabilidades, sin embargo, dentro de los CIS detalla la necesidad de adicionar procesos de inventario, control, monitoreo y el histórico.
Inventario y control de activos Empresariales	*-Manejo de equipos de cómputo* *-Administración de servidores*	La Política determina la responsabilidad del usuario, la gestión que realiza el mismo mediante un correcto cuidado de los equipos de cómputo y estándares de seguridad, sin embargo, la CIS establece como objetivo mantener un control de inventario de activos y monitorear los activos en la red.
Gestión de control de acceso	*-Seguridad física y Datacenter*	La Política establece control de accesos físico a la infraestructura, la tecnológica y adicional el ingreso a dispositivos de administración, sin embargo, los CIS complementan el acceso físico con procesos de Autenticación en herramientas y dispositivos expuestos externamente que permiten controlar el acceso.
Monitoreo y defensa de la red	*-Administración de dispositivos y sistemas de Seguridad Perimetral Informática*	La Política está basada en la administración, dispositivos y seguridad perimetral para la red, sin embargo, no se tiene en cuenta procedimientos que establezcan el correcto monitoreo de flujo de tráfico, la detección y prevención de intrusiones, los CIS complementarían este control en pro de defender y salvaguardar la red.
Inventario y control de activos de software	*-Manejo adecuado del Software y licencias suministradas por PEI AM*	El control de la Política hace referencia a la gestión adecuada del software de la compañía, describe como debería funcionar el proceso de inventario, sin embargo, no establece los mecanismos para realizarlo algo que si se encuentra especificado y alineado en los controles CIS.
Recuperación de los datos	*-Manejo de la información y datos de PEI AM* *-Respaldo de información*	El control establece el proceso de conservación y manejo de datos, adicionalmente precisa la responsabilidad de todo aquel que interactúe con la información de la empresa, este punto comparado con la CIS no especifica la importancia de un proceso de conservación, que se mantenga un inventario de tiempos de consecución, eliminación controlada de información para prevenir perdida de datos.
Gestión de respuesta de incidentes	*-Notificación de incidentes de ciberseguridad*	La Política únicamente abarca la responsabilidad del usuario y quienes tengan una relación con PEI AM a notificar, de eventos adversos de seguridad, los CIS buscan que solo la notificación de estos eventos no es suficiente se debe determinar el procedimiento que se ejecutara una vez exista la primera alerta.
Protección del Correo Electrónico y	*-Uso del correo electrónico corporativo* *-Manejo del servicio de*	La política establece responsabilidad y normas para el correcto uso de sus medios de comunicación como el correo corporativo y navegación en las redes de PEI AM, orientados correctamente con los controles CIS logrando un completo cumplimiento con respecto a este control.

La Política actualmente implementada por PEI AM muestra el cumplimiento de 8 parámetros establecidos frente a los 18 controles estandarizados por la CIS de acuerdo con la **tabla 3,** de esta manera se podrá sugerir acciones de mejora en los ítems que se encuentran en ejecución actualmente, que permitan encaminar la Política al modelo de negocio de PEI AM.

Los controles faltantes por ser aplicados dentro de la Política son:

Tabla 4. Controles no aplicados dentro de la Política			
1	Protección de Datos	**6**	Gestión de Infraestructura de Red
2	Configuración Segura de Activos y Software	**7**	Concientización en Seguridad y Formación de Habilidades
3	Gestión Continua de Vulnerabilidades	**8**	Gestión de Proveedores de Servicios
4	Gestión de Registros de Auditoria	**9**	Seguridad en el Software de Aplicación
5	Defensa contra Malware	**10**	Pruebas de Penetración

2.3 Propuesta

Según el análisis y las evidencias generadas, se sugiere realizar un ajuste en la política considerando las buenas prácticas establecidas en el CIS, actualmente la mayoría de los puntos de esta política no cumplen con dichas prácticas y se hace evidente la ausencia de controles fundamentales, que contribuyen a la orientación de la política y el objetivo general de la misma. Para lograr implementar de manera efectiva las buenas prácticas y controles, se sugiere a PEI AM:

- Iniciar un proceso de Análisis de la Política considerando las recomendaciones de los controles CIS, para aplicarse en cada área de la organización donde se puedan generar vulnerabilidades.

- Establecer un proceso de mejora que permita complementar los puntos establecidos dentro de la política, basándose en las buenas prácticas de la CIS y así garantizar el cumplimiento de su objetivo específico.

- Realizar un plan de trabajo con diferentes fases a corto, mediano y largo plazo, para la implementación de los diez controles CIS que no se encuentran establecidos dentro de la política.

3.Resultados

De acuerdo con el desarrollo del análisis de la Política de ciberseguridad de PEI AM frente a los Controles CIS y con base en las recomendaciones se evidencio que existen nuevos procedimientos que pueden ser implementados para mejorar la aplicabilidad, a su vez también, se identifican un conjunto de controles que no están siendo aplicados y que son de vital importancia ya que contribuirán al desarrollo del proceso de ciberseguridad, adicional a que es relevante tener en cuenta que los diez ítems de los controles CIS mencionados en la tabla 4, hablan de la importancia del tratamiento de datos personales y fundamentalmente del proceso de defensa y gestión ante vulnerabilidades, haciendo énfasis en la importancia de generar planes de concientización que involucren a las diferentes áreas que hacer parte de la operación, debido a que este es el principal método para reducir la brecha y fortalecer la preparación de la organización ante posibles hechos de amenazas y vulnerabilidades.

4. Conclusiones y recomendaciones

Conclusiones

Al comparar los Controles CIS y la Política de Ciberseguridad de la compañía, se evidencia que los 12 controles estipulados pueden presentar brechas de seguridad en un futuro, ya que algunos temas importantes no se consideran y no abarcan todos los procedimientos para lograr una óptima seguridad informática de los dispositivos, redes y servicios utilizados por PEI AM.

Al ser la ISO27001 el estándar más reconocido en seguridad informática, las compañías suelen elaborar sus Políticas de ciberseguridad basadas en ella, pero la norma 27001 abarca procedimientos y controles aplicables en distintas áreas de acción, generando que así se diseñen las Políticas, lo que ocasiona que las organizaciones hablen de las generalidades del proceso, sin llegar a las especificaciones necesarias en pro de su negocio, por eso los controles CIS buscan enfocarse en un conjunto de buenas prácticas de ciberseguridad orientado a sus objetivos específicos.

Recomendaciones

Basándonos en los resultados anteriores, se recomienda una vez reestructurada la política en base a los Controles CIS, se mantengan en constante estudio y actualización de acuerdo a las futuras Versiones que sean publicadas, con el objetivo de mejora continua frente a nuevas vulnerabilidades o métodos de ataque, adicional a que implementar estas recomendaciones dan mejora en la política y es fundamental darle el grado de importancia necesario, debido a que con la política actual no se observan los resultados esperados, en cuanto a gestión de procedimientos y aplicabilidad dentro de PEI AM, de allí la importancia necesaria de culturizar, capacitar y orientar todo aquel que maneje algún vínculo y que dentro de sus funciones, realice manejo o manipulación de información, omitir este proceso de transformación de la Política continuara aumentando el riesgo de vulneración dentro de PEI AM, aunque no se registran ataques exitosos por algún método, el ideal es mantener integridad de todo el modelo de negocio.

Bibliografía

1) *Blog de Internet Security Auditors: Controles del CIS: novedades de la versión 7.1*. (n.d.). Retrieved November 17, 2023, from https://blog.isecauditors.com/2019/11/novedades-version-7-1-controles-cis.html
2) Castañaga, I., Gibellini, F., Frias, P., Ruhl, L., Ciceri, L., Parisi, G., Zea, M., Bertola, F., & Olmedo, P. (n.d.). *Estrategias de detección de ransomware de cifrado*.
3) Castillo-Pérez, S., Alfredo, J., Andrés, M., & Garcia-Alfaro, J. (n.d.). *El Spyware como amenaza contra navegadores web*.
4) *CIS Controls: Todo lo que necesitas saber | CalCom*. (n.d.). Retrieved November 17, 2023, from https://www.calcomsoftware.com/cis-controls-todo-lo-que-necesitas-saber/
5) *Controles CIS*. (n.d.). http://www.cisecurity.org/controls/
6) Edgar Fabricio Rivera Osorio., Miriam Patricia Cárdenas Zea., & Washington Alberto Chiriboga Casanova. (2020, April). *Evaluación de ataques DDoS y fuerza bruta utilizando entorno virtual Kali Linux como plataforma experimental.*
7) Fonfría, A. (n.d.). *Elementos para una política de ciberseguridad efectiva*. https://www.sciencedirect.com/science/article/pii/S0167404813000801.
8) Guaña-Moya, J., del Carmen Jaramillo-Flores, P., Rafael Mora-Zambrano, E., Chiluisa-Chiluisa, M., Naranjo-Villota, D., & Gerardo Larrea-Torres, L. (n.d.). *Ataques de phishing y cómo prevenirlos Phishing attacks and how to prevent them*.
9) *Malware*. (n.d.). Retrieved November 17, 2023, from https://www.mintic.gov.co/portal/inicio/18744:Malware
10) Mieres, J. (n.d.). *Ataques informáticos Debilidades de seguridad comúnmente explotadas*. www.evilfingers.com
11) *¿Qué es la ciberseguridad? - Explicación de la ciberseguridad - AWS*. (n.d.). Retrieved November 17, 2023, from https://aws.amazon.com/es/what-is/cybersecurity/
12) Quiroz-Zambrano I Universidad Laica Eloy Alfaro de Manabí, S. M., & Macías-Valencia, D. G. (2017). *Seguridad en informática: consideraciones Computer security: considerations*. *3*(5), 676–688. https://doi.org/10.23857/dom.cien.pocaip.2017.3.5.agos.676-688