Polo del Conocimiento

Pol. Con. (Edición núm. 41) Vol. 5, No 01
Enero 2019, pp. 581-607
ISSN: 2550 - 682X
DOI: 10.23857/pc.v5i01.1239

Evaluación de seguridad perimetral, aplicando normativa de la Súper Intendencia de Economías Populares y Solidarias, SEPS-IGT-IR-ISF-ITIC-IGJ-2017-103. Caso de estudio: Cooperativa del Sector 1

Perimeter security evaluation, applying regulations of the Super Intendancy of Popular and Solidarity Economies, SEPS-IGT-IR-ISF-ITIC-IGJ-2017-103. Case study: Sector 1 Cooperative

Avaliação de segurança de perímetro, aplicando os regulamentos da Super Intendência de Economias Populares e Solidárias, SEPS-IGT-IR-ISF-ITIC-IGJ-2017-103. Estudo de caso: Setor 1 Cooperativa

Christian Fernando Siavichay-Martínez [I]
christian.siavichay@cooperco.fin.ec
https://orcid.org/0000-0003-2648-5256

Jenny Karina Vizñay-Durán [II]
jviznay@ucacue.edu.ec
https://orcid.org/0000-0001-7557-5034

Correspondencia: christian.siavichay@cooperco.fin.ec

Ciencias de las ingenierías
Artículo de investigación

*Recibido: 10 de noviembre de 2019 *Aceptado: 23 diciembre de 2019 * Publicado: 17 de enero 2020

I. Ingeniero en Informática, Jefatura de Posgrados. Universidad Católica de Cuenca, Cuenca, Ecuador.

II. Ingeniero en Sistemas, Sub Decana de la Unidad Académica de Tecnologías de la Información, Jefatura de Posgrados, Universidad Católica de Cuenca, Cuenca, Ecuador.

Resumen

El presente trabajo de investigación expone una evaluación de la seguridad perimetral en la Cooperativa del caso de estudio la misma que se encuentra en el sistema financiero de economía popular y solidaria, dicho segmento está regulado por un ente perteneciente al estado, la Súper intendencia de Economía Popular y Solidaria SEPS; y, es quien impone los reglamentos y normativas que deben cumplir las Cooperativas en sus diferentes segmentos. Para cumplir con el objetivo se planteó un camino a seguir con un estado de situación inicial, generar una matriz de riesgos de a seguridad perimetral, evaluar las herramientas más idóneas para la remediación y elaborar un informe final con la propuesta de mejora en seguridad perimetral.

Con el estado de situación inicial se pudo determinar que a la institución debe realizar cambios para mejorar los procesos, infraestructura y herramientas de gestión, pues utilizando una observación participativa se logra identificar debilidades en la protección de perímetro de la red institucional, el equipo de seguridad perimetral tiene características distintas a las que necesita la institución, la creación de políticas, reglas, perfiles que permiten controlar el acceso de los usuarios y su tráfico están basados en un reglamento interno y siempre orientando a cumplir con la norma establecida; la política y controles para ejecutar transacciones por canales electrónicos está en desarrollo, debido a esto se implementan medidas correctivas temporales en cuanto a seguridad de accesos.

Gracias al análisis de riesgos se determinó los activos con una probabilidad e impacto muy alto de que su amenaza se cumpla, este servirá de base para el desarrollo de salvaguardas que protejan dichos bienes.

Las herramientas a evaluar se las selecciona de acuerdo a criterios como el tipo de institución al que se orienta, un dimensionamiento correcto permite una mejor selección de la solución, lógicamente se debe tomar en cuenta el presupuesto con el que cuenta la institución; entonces, con lo antes expuesto se debe determinar si la herramienta de seguridad perimetral (firewall) que actualmente está en producción es la idónea para la institución; y, cual es la mejor opción de software UEM para permitir el acceso de dispositivos móviles a la red LAN de la Cooperativa.

El porcentaje de efectividad de las herramientas o soluciones que se implementen dentro de una empresa depende de que tan maduros sean sus procesos, por lo que debe evaluarse una metodología internacionalmente reconocida que ayude a mejorar y crear procesos institucionales. La Cooperativa del caso de estudio tiene procesos creados para cubrir una necesidad de cumplimiento de normativa y fundamentados en reglamentos internos que les falta alinearse a una metodología que pueda ayudar a estandarizarlos, de fácil auditoria, a mantener el equilibrio entre obtener beneficios, optimizar los niveles de riesgo y el uso de recursos.

Es por esto que la propuesta se fundamenta en el uso de una metodología que ayude a la Cooperativa a cumplir sus objetivos de gobierno y gestión de TI; con la que se pueda desarrollar procesos de seguridad de la información y sean auditables; una vez que se los haya creado o actualizado, iniciar con el plan de mejora continua para el establecimiento de políticas de seguridad perimetral y su aplicación siempre adaptándolos a las nuevas necesidades de la Cooperativa sobre todo siempre buscando cumplir con la normativa SEPS-IGT-IR-ISF-ITIC-IGJ-2017-103 de la SEPS; estos ajustes deben implementarse dentro del departamento de TI así como el departamento de Seguridad de la Información, lo que agrega valor para los dos bloques y por consiguiente a la Cooperativa pues la sensación de seguridad que se ofrece a los Socios es muy importante para su crecimiento.

Palabras clave: Seguridad de la información; normativas de la SEPS; Unified Endpoint Management-, Cobit 5 for security professionals; firewall.

Abstract

The present research work intends to prepare an evaluation of the perimeter security in the Cooperativa of the case study that is found in the financial system of Economía popular y solidaria, said segment is regulated by an entity belonging to the state, the Súper intendencia de Economía Popular y Soludaria SEPS; and, it is the one who imposes the regulations and regulations that Cooperativas must comply with in their different segments. To meet the objective, a way forward with a state of initial situation was proposed, to generate a matrix of perimeter security risks, to evaluate the most suitable tools for remediation and to prepare a final report with the proposal to improve perimeter security.

With the initial situation, it was determined that the institution must make changes to improve the processes, infrastructure and management tools, since using a participatory observation it is possible to identify weaknesses in the perimeter protection of the institutional network, the security team perimeter has different characteristics to those that the institution needs, the creation of policies, rules, profiles that allow to control the access of the users and their traffic are based on an internal regulation and always oriented to comply with the established norm; The policy and controls for executing transactions through electronic channels are under development, due to this temporary corrective measures are implemented regarding access security.

Thanks to the risk analysis, the assets were determined with a very high probability and impact that their threat is met, this will serve as the basis for the development of safeguards that protect these assets.

The tools to be evaluated are selected according to criteria such as the type of institution to which it is oriented, a correct sizing allows a better selection of the solution, logically the budget that the institution has must be taken into account; then, with the above, it must be determined if the perimeter security tool (firewall) that is currently in production is ideal for the institution; and, what is the best UEM software option to allow mobile devices access to the Cooperative's LAN network.

The percentage of effectiveness of the tools or solutions that are implemented within a company depends on how mature its processes are, so an internationally recognized methodology that helps to improve and create institutional processes must be evaluated.

The proposal is based on the use of a methodology with which information security processes can be developed and auditable; once they have been created or updated, start with the continuous improvement plan for the establishment of perimeter security policies and their application always adapting them to the new needs of the Cooperative, especially always seeking to comply with SEPS-IGT-IR -ISF-ITIC-IGJ-2017-103 of the SEPS regulations These adjustments must be implemented within the IT department as well as the Information Security department, which adds value for the two blocks and therefore to the Cooperativa as the sense of security offered to the Partners is very important for their growth.

Keywords: Information security; normativas de la SEPS; Unified Endpoint Management; Cobit 5 for security professionals; firewall.

Resumo

O presente trabalho de pesquisa apresenta uma avaliação da segurança do perímetro na Cooperativa do estudo de caso, encontrado no sistema financeiro da economia popular e solidária, sendo esse segmento regulado por uma entidade pertencente ao Estado, a Super Administração de Economia SEPS Popular e Solidariedade; e é quem impõe os regulamentos e regulamentos que as cooperativas devem cumprir em seus diferentes segmentos. Para atingir o objetivo, foi proposto um caminho a seguir com um estado de situação inicial, para gerar uma matriz de risco de segurança de perímetro, avaliar as ferramentas mais adequadas para remediação e preparar um relatório final com a proposta de melhorar a segurança de perímetro.

Com o status inicial da situação, determinou-se que a instituição deve fazer alterações para aprimorar processos, infraestrutura e ferramentas de gerenciamento, pois, utilizando uma observação participativa, é possível identificar fragilidades na proteção do perímetro da rede institucional, a equipe de segurança o perímetro possui características diferentes daquelas de que a instituição precisa, a criação de políticas, regras, perfis que permitam controlar o acesso dos usuários e seu tráfego são baseados em um regulamento interno e sempre orientados para atender à norma estabelecida; A política e os controles para a execução de transações por meio de canais eletrônicos estão em desenvolvimento, devido a essas medidas corretivas temporárias, implementadas em relação à segurança de acesso.

Graças à análise de risco, os ativos foram determinados com uma probabilidade e impacto muito altos de que sua ameaça foi atendida, servindo de base para o desenvolvimento de salvaguardas que protegem esses ativos.

As ferramentas a serem avaliadas são selecionadas de acordo com critérios como o tipo de instituição para a qual estão orientadas, um dimensionamento correto permite uma melhor seleção da solução, logicamente o orçamento que a instituição possui deve ser levado em consideração; com o exposto, deve-se determinar se a ferramenta de segurança de perímetro (firewall) atualmente em produção é ideal para a instituição; e qual é a melhor opção de software UEM para permitir o acesso de dispositivos móveis à rede LAN da cooperativa.

O percentual de eficácia das ferramentas ou soluções implementadas em uma empresa depende da maturidade de seus processos; portanto, deve ser avaliada uma metodologia reconhecida internacionalmente que ajude a melhorar e criar processos institucionais. A Cooperativa de Estudo de Caso possui processos criados para cobrir a necessidade de conformidade regulamentar e com base em regulamentos internos que precisam se alinhar a uma metodologia que pode ajudar a padronizá-los, com auditoria fácil, para manter o equilíbrio entre obter benefícios e otimizar níveis risco e uso de recursos.

É por isso que a proposta se baseia no uso de uma metodologia que ajuda a Cooperativa a atingir seus objetivos de governança e gerenciamento de TI; com que processos de segurança da informação podem ser desenvolvidos e auditáveis; uma vez criados ou atualizados, inicie com o plano de melhoria contínua para o estabelecimento de políticas de segurança de perímetro e sua aplicação, adaptando-as sempre às novas necessidades da Cooperativa, buscando sempre cumprir com os regulamentos SEPS-IGT-IR -ISF-ITIC-IGJ-2017-103 do SEPS; Esses ajustes devem ser implementados no departamento de TI e no departamento de Segurança da Informação, que agrega valor aos dois blocos e, portanto, à Cooperativa, pois o senso de segurança oferecido aos Parceiros é muito importante para o seu crescimento. .

Palavras-chave: Segurança da informação, regulamentos SEPS, Unified Endpoint Management, Cobit 5 para profissionais de segurança, firewall.

Introducción

La Súper Intendencia de Economías Populares y Solidarias SEPS(GomezMiguel, 2012) dentro de su reglamentación y funciones tiene la obligación de controlar y auditar a las entidades financieras que pertenecen al sector en muchos aspectos. En esta investigación, interesa el control de como los socios y colaboradores pueden acceder mediante canales electrónicos a realizar transacciones con su dinero alojado en cuentas de ahorros, todo esto de una manera segura, para garantizar que dichas operaciones lleguen a su destino final y no sean interceptadas y modificadas para beneficios de terceros. Es así que la SEPS constantemente revisa los avances tecnológicos, y, en base a ellos emite nuevas normativas, con las cuales pretenden tener un sector homogéneo para que las comunicaciones inter cooperativas puedan reconocerse e interpretarse de la misma forma en todas

ellas; la normativa más reciente tiene que ver con la implementación de seguridades mínimas que debe tener un canal electrónico al momento de realizar una transacción, enfocando propiamente para el desarrollo del documento la *"sección III: Medidas tecnológicas de seguridad en el uso de transferencias electrónicas*", en donde detalla lo que debe contemplarse para realizar transacciones por cualquier tipo de canal electrónico permitido por el ente regulador. En el desglose de los requerimientos está la necesidad de autenticaciones seguras, precautelar integridad y privacidad de la información del socio, establecimiento de límites, etc., que para poderlos cumplir es necesaria la implementación de herramientas tecnologías de seguridad perimetral, la generación de procesos internos, etc., siendo aquí donde surge la necesidad de realizar el estudio, que plasma una evaluación del estado de situación actual de la Cooperativa y recomendaciones a las que deben ajustarse para cumplir con la norma.

El nivel de exigencia por parte de la SEPS para que una entidad regulada cumpla con estos requerimientos dependerá del segmento en el que se la clasifica, es así que la Cooperativa del caso de estudio, en el año 2019 fue ascendida al segmento 1, en donde los cumplimientos de todas las normativas deben ser absolutos y en caso de no tener implementada la infraestructura y procesos que soporten los requerimientos de las normativas, la institución será sancionada de acuerdo al reglamento. Es por esto que la institución debe preguntarse ¿Cuáles son las mejores prácticas que debe adoptar la institución para mejorar su seguridad perimetral e infraestructura tecnológica?, adicionalmente hay que tomar en cuenta que se hizo varias contrataciones en el año 2019 para poder cumplir con las exigencias del segmento 1 de la SEPS, entre las que se destaca la inclusión de un Oficial de Seguridad, que por ser un cargo nuevo en la institución, no existen procesos establecidos, al contrario se los están generando conjuntamente con los departamentos implicados y en forma bidireccional con el departamento de TI; a esto se suma la falta de infraestructura tecnológica con la que se pueda gestionar las redes de datos y accesos desde internet de una manera eficiente y se pueda permitir el acceso a la red LAN de manera segura desde cualquier lugar.

El objetivo de esta investigación se basó en "Evaluar el departamento de TI, en su seguridad perimetral, para elaborar una propuesta con la que permita el acceso seguro de dispositivos externos hacia la red LAN, tomando como referencia la normativa de la SEPS SEPS-IGT-IR-ISF-ITIC-IGJ-2017-103".

Para poder cumplir con el objetivo planteado se realizaron los siguientes pasos:

- ✓ Determinar el estado de situación inicial tanto técnico como de procesos en cuanto a la administración de las seguridades implementadas en su infraestructura tecnológica. Con esto lo que se pretende, es llegar a conocer las herramientas aplicadas en seguridad perimetral y end point, determinar si dichas herramientas están bien utilizadas y dimensionadas, si existen procesos y su debida aplicación.
- ✓ Generar una matriz de riesgo de la seguridad perimetral. En donde se realizará un levantamiento de activos de información: hardware, software, personas determinando los grados de criticidad y salvaguardas.
- ✓ Determinar herramientas de remediación idóneas, haciendo una evaluación de las que se ajusten a las necesidades existentes y futuras de la institución, con dimensionamientos realistas en base a su crecimiento anual.
- ✓ Elaborar un informe técnico que proponga la mejora de la seguridad perimetral y su gestión.

El plan propuesto está fundamentado en los marcos de referencia tales como Itil y Cobit, que se utilizan en el área de tecnología de la información y específicamente en la normativa SEPS SEPS-IGT-IR-ISF-ITIC-IGJ-2017-103 del ente de control.

Desarrollo

Estado de situación inicial de la Cooperativa del caso de estudio.

La Cooperativa es una institución financiera con más de 50 años de experiencia apoyando a los sectores productivos que no siempre son atendidos por la banca nacional; este arduo trabajo da como resultado un crecimiento importante de la institución en los 2 últimos años y la clasificación en el segmento número uno de la Súper Intendencia de Economías Populares y Solidarias SEPS, lo cual implica mucha más responsabilidad para la Cooperativa y por lo tanto el cumplimiento de reglamentos y normativas impuestas por los entes reguladores del sector, entre las cuales está la SEPS-IGT-IR-ISF-ITIC-IGJ-2017-103, la cual regula o establece los niveles mínimos de protección en las transferencias electrónicas realizadas mediante mensajes o instrucciones telefónicas, electrónicas o celulares desde un ordenador conectado a redes de comunicación propias o de terceros a otro ordenador, mediante el uso de cualquier terminal.

Para poder cumplir esta normativa es necesario contemplar cambios tanto en procedimientos como en infraestructura tecnológica, por lo que se debe primero realizar un análisis de la situación actual de la institución en estos dos puntos, ejecutando las siguientes actividades:

- Entrevista con el Oficial de Seguridad de la Información OSI de la Cooperativa.
- Solicitud de documentación, manuales, políticas y procesos a los departamentos pertinentes.
- Entrevista con el Jefe de Tecnologías de la Información para recopilar información.
- Inspección de las instalaciones y de su infraestructura tecnológica.

Entrevista con el Oficial de Seguridad.

De acuerdo a la entrevista, a inicios del año 2019 se realizó la contratación de un Oficial de Seguridad de la Información, quien ha desplegado un plan para conocer la verdadera situación de la Cooperativa, misma que se detalla a continuación:

En cuanto al antivirus de los equipos terminales, existía un 71% de los equipos sin uno instalado, en el resto las actualizaciones no estaban al día con las bases de datos, se detectaron más de dos mil virus en algunos de los equipos, el firewall no determina reglas de navegación específicas para los sectores críticos. Está en producción el Firewall PFSense, el cual no cumple con los requisitos mínimos de seguridad perimetral y que debe ser cambiado lo antes posible puesto que no pueden crearse reglas de firewall robustas, perfiles de navegación diferenciados, control de aplicaciones, no existe servicios de seguridad, tales como botnet, ATP, virus, IPS, etc. En cuanto a spam's el dominio de la Cooperativa ha pasado a ser parte de las listas negras, lo que ha traído inconvenientes al departamento de TI, pues todas las semanas existen reportes de los usuarios que llegan correos de phishing, spam y virus. Continuando con el tema de los correos, no existen políticas de contraseñas, se puede recibir correos adjuntos ejecutables (.exe), existen cuentas de correo que le pertenecían a exfuncionarios que todavía están activas.

La Cooperativa tiene 12 cajeros automáticos, de los cuales el 75% no cuenta con un antiskimming en óptimas condiciones, el 60% cuenta con antivirus, el sistema de grabaciones de video tiene una capacidad de almacenamiento de 30 días para grabaciones.

No se cuenta con una aplicación de seguridad para la página web institucional. Se detectó malware en dicho sitio, pues re direccionan a páginas ajenas a la de la Cooperativa.

A lo anterior se puede sumar la falta de políticas para bloqueos de los puertos USB de los equipos terminales, control en la navegación, etc. Esto ha provocado que se presenten amenazas, entre ellas: conexiones no autorizadas, ataques de phishing, pérdida de la confidencialidad y robo de la información; lo que representa un riesgo elevado para una institución financiera, por lo que se requiere de acciones inmediatas para mitigar estos hallazgos.

Solicitud de documentación.

Dentro de la institución el departamento de procesos es quien resguarda los manuales, reglamentos y políticas de la misma, también es quien debe dar mantenimiento y actualizarlas de acuerdo a las nuevas normativas externas, mediante solicitud formal vía correo electrónico se solicitó manuales y políticas que tengan que ver con la seguridad de la información, la documentación entregada fue:

- Manual de seguridad de la información.
- Normativa SEPS-IGT-IR-ISF-ITIC-IGJ-2017-103.

El manual de seguridad de la información detalla las responsabilidades de los actores que deben intervenir dentro de la Cooperativa y define la política de un control de acceso para el mantenimiento y creación de usuarios de los distintos sistemas que se manejan internamente; están definidos de manera general los controles físicos y la gestión de los incidentes de seguridad, adicionalmente se define buenas prácticas para el correcto uso de las herramientas tecnológicas asignadas. A pesar de la existencia del manual, en este no se observa que hayan sido abordados lineamientos cruciales en el ámbito de seguridad tales como:

- Lineamiento de seguridad para medios de almacenamiento extraíbles.
- Lineamiento de seguridad para Backup en servidores.
- Lineamiento de seguridad para repositorios institucionales.
- Lineamiento de seguridad para la clasificación, reciclaje y/o destrucción de la información.
- Lineamiento de seguridad para centro de datos.

- Lineamiento de seguridad para infraestructura tecnológica.
- Lineamiento de seguridad para proveedores.

Como ya se mencionó, la normativa SEPS-IGT-IR-ISF-ITIC-IGJ-2017-103, establece los niveles mínimos de protección en las transferencias electrónicas realizadas mediante mensajes o instrucciones telefónicas, electrónicas o celulares, desde un ordenador conectado a redes de comunicación propias o de terceros a otro ordenador, mediante el uso de cualquier terminal, a este documento deben referirse todas las instituciones financieras regidas por la SEPS debiendo adaptar sus procesos políticas e infraestructura tecnológica.

Entrevista con el Jefe de TI.

El jefe del departamento se encuentra en el cargo desde hace 3 años, tiempo en el cual ha visto como crece la Cooperativa y sus requerimientos en la parte tecnológica, haciendo énfasis en la siempre latente necesidad de seguir creciendo constantemente, tanto en personal como en infraestructura, lo cual implica que su administración también se complica, es por esto que se prioriza la adquisición de software con el que se pueda administrar de manera efectiva toda la infraestructura, contratos con proveedores que garanticen acuerdos de SLA convenientes para la Institución, optimizar al máximo los recursos adquiridos. En cuanto a la seguridad de la información, debido al crecimiento y a la exigencias del ente de control se ha iniciado cambios en la seguridad perimetral, servidores publicados y equipos terminales, esto es un proyecto que inició en el último trimestre del año 2018, en medio del proyecto se contrató un Oficial de Seguridad, por lo que se trasladó a ese departamento la mayor parte del mismo, manteniendo la administración de firewall excepto la parte de perfiles de accesos, la consola del antivirus Kaspersky, creación y mantenimiento de usuarios en los distintos sistemas, administración de antimalware para cajeros automáticos y demás procesos que son competencia del nuevo departamento de Seguridad de la Información. En este proceso de transición, se implementó un Firewall con sus licencias, un antispam para el correo institucional, adquisición de licencias de antivirus para los equipos restantes, creación de políticas para la administración de los recursos mencionados.

Inspección de instalaciones y revisión de infraestructura tecnológica.

Actualmente, la Cooperativa tiene un centro de datos principal y uno alterno, el cual está en proceso de puesta en producción, por el momento está funcionando con equipos y servidores virtuales que mantienen información de los sistemas que mantenía una cooperativa que fue absorbida en el año 2018 por la Cooperativa del caso de estudio, en cuanto a los equipos que lo componen, existe un chasis Flex Lenovo con capacidad para 14 blade's, hay 3 espacios ocupados; es decir, tres servidores que son los que sostienen la institución con aproximadamente 50 máquinas virtuales, de las cuales 30 son equipos de producción, los demás son parte de un ambiente de pruebas y desarrollo con los que se trabaja para certificar nuevos desarrollos y sistemas. Para la Base de datos existen servidores exclusivos (1 de producción y 2 de pruebas), pues de acuerdo a los licenciamientos que se tiene se debe hacer la instalación en Bare metal. En la parte de red LAN existen switchs de core y de acceso, todos administrables, con lo que se puede configurar VLAN's y segmentar la red, existe un contrato con la Empresas nacionales que proveen de los 30 enlaces hacia las agencias, tanto dentro como fuera de la ciudad y provincia, cada enlace tiene un ancho de banda de 2,5 Mb, una salida a internet de 18 Mb, un enlace L2 para unir los centros de datos principal y alterno, todos estos enlaces están creados dentro de una topología de estrella, en la Matriz está el concentrador y todo el tráfico pasa por el firewall SonicWall TZ 500, ya sea de manera interna como externa. También existen enlaces hacia distintas empresas con las cuales tiene convenios de cobro, los mismos que no van por la IP pública, son enlaces privados y cifrados.

En cuanto a las agencias, el Jefe de TI señala que para el mes mayo del 2019 el proveedor del enlace instala un router y la cooperativa instala un switch configurable y hace el tendido de red para los equipos terminales que se instalarán, el sistema de cámaras de vigilancia también es desplegado, el cual deberá mantener grabaciones de todas las cámaras durante 90 días, ajustándose a la normativa vigente.

Los equipos terminales nuevos son preparados con una imagen de sistema operativo que contiene instalado previamente los programas necesarios y básicos para cada uno de los funcionarios, y, con el antivirus instalado, antes de ser entregado se realiza la actualización de las bases de datos del mismo.

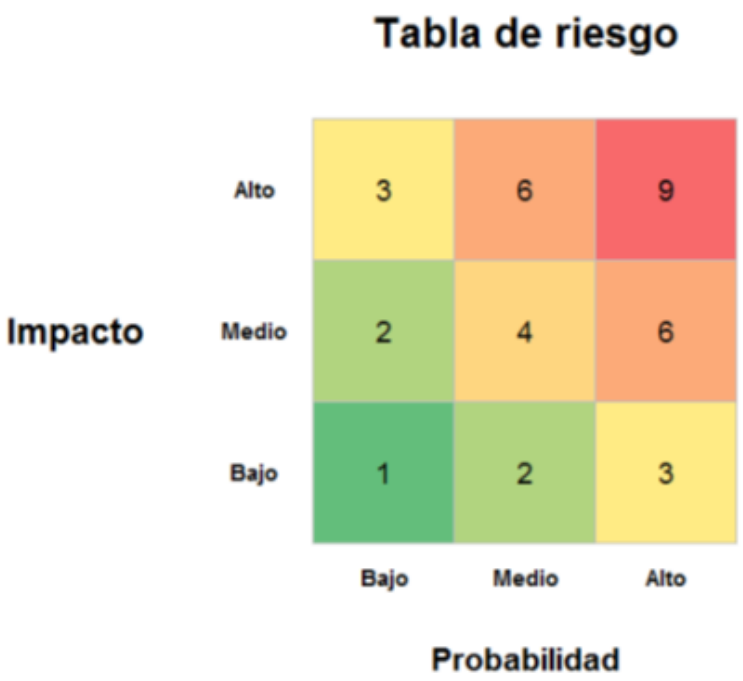
Análisis del estado de situación inicial.

Una vez que se ha recopilado la información de los departamentos involucrados, se puede evidenciar que se requiere de cambios urgentes en la parte de seguridad de la información, pues debido al crecimiento acelerado se han obviado procesos importantes, no se han creado políticas suficientes para cumplir con la normativa de la SEPS, no existen los requerimientos mínimos de seguridad, los equipos terminales son de fácil acceso, no se cuenta con un directorio activo que permita implementar políticas por grupos, se debe depurar los permisos de usuario por cada sistema interno que se maneja, centralizar la administración en un responsable. El proceso de cambio ya empezó a inicios del 2019 con algunos que favorecieron considerablemente a la institución y que han logrado cumplir con parte de las normativas vigentes, pero todavía queda trabajo por hacer en cuanto a la generación de procesos y un manual que contemple todo lo concerniente a mantener la información disponible, integra y siempre con la confidencialidad que necesita.

Análisis de riesgos.

Uno de los puntos más importantes, es conocer el estado de la institución en cuanto a sus riesgos, como los evalúa, su plan de mitigación, etc. Con la metodología Magerit(coordinación de contenidos et al., 2012) se ha logrado extraer una matriz de riesgos inicial en la que se puede observar los riesgos medidos por el impacto y la probabilidad de que se sucedan las amenazas planteadas sobre los activos detallados en la misma; entonces en base a la siguiente tabla se ha establecido la criticidad de los riesgos encontrados

Tabla 1 Tabla de riesgo



Fuente: Elaboración Propia

Este levantamiento de la información se la realizó con personal de TI, el departamento de Riesgos y de Seguridad de la Información, pues la responsabilidad de una buena administración de los activos declarados está en ellos.

Se han considerado los siguientes activos para este análisis:

Tabla 2 Identificación de Activos

Identificador	Activo	Aplicación
C1	Equipos de Almacenamiento	SI
C2	Servidores	SI
C3	Conexión a Internet con wifi y cableado	SI
C4	Red interna	SI
C5	Dispositivos móviles con datos	SI
C6	Core Financiero	SI
C7	Página web, sistema facturación electrónica y redes sociales que gestionan desde la empresa	SI
C8	Herramientas para empresas en la nube	SI
C9	Web Services (carga, descarga de datos)	SI

Fuente: Elaboración Propia

Tabla 3 Catálogos de Amenazas

Amenazas - Desastres Naturales
Fuego
Daños por agua
Desastres naturales

Amenazas- Errores, fallos no intencionales
Fuga de información
Introducción de falsa información
Alteración de la información (intencional, no intencionas)
Corrupción de la información
Destrucción de información
Interceptación de información (escucha)

Amenazas - De origen industrial
Corte del suministro eléctrico
Condiciones inadecuadas de temperatura o humedad
Fallo de servicios de comunicaciones
Interrupción de otros servicios y suministros esenciales
Desastres industriales

Amenazas Errores, fallos no intencionales
Degradación de los soportes de almacenamiento de la informaci
Difusión de software dañino
Errores de mantenimiento / actualización de programas (software
Errores de mantenimiento / actualización de equipos (hardware)
Caída del sistema por sobrecarga
Pérdida de equipos
Indisponibilidad del personal
Abuso de privilegios de acceso
Acceso no autorizado

Amenazas - Personas
Errores de los usuarios
Errores del administrador
Errores de configuración

Amenazas - Ataques intencionados
Denegación de servicio
Robo
Indisponibilidad del personal
Extorsión
Ingeniería social
Explotación de vulnerabilidades

Fuente: Elaboración Propia

Como resultado de la carga de esta matriz de riesgo se tiene como resultado que, 9 de los activos de acuerdo a su amenaza planteada con ponderación de riesgo alto, es decir de probabilidad alta y de impacto alto, sobre los cuales hay que trabajar en salvaguardas efectivas.

Existen 26 amenazas que tienen un riesgo con calificación 6, lo que significa una probabilidad alta y un impacto medio, las cuales deben ser atendidas lo antes posible para mitigar el riesgo existente.

Tabla 4 Análisis de Riesgos

ANÁLISIS DE RIESGOS					
Activo		**Amenaza**	**Probabilidad**	**Impacto**	**Riesgo**
Equipos de Almacenamiento	C1	Fuego	Alta (3)	Alto (3)	9
Equipos de Almacenamiento	C1	Corte del suministro eléctrico	Alta (3)	Alto (3)	9
Equipos de Almacenamiento	C1	Desastres industriales	Alta (3)	Alto (3)	9
Equipos de Almacenamiento	C1	Abuso de privilegios de acceso	Alta (3)	Alto (3)	9
Servidores	C2	Errores de mantenimiento / actualización de programas (software)	Alta (3)	Alto (3)	9

Servidores	C2	Errores de mantenimiento / actualización de equipos (hardware)	Alta (3)	Alto (3)	9
Core Financiero	C5	Fuego	Alta (3)	Alto (3)	9
Core Financiero	C5	Corte del suministro eléctrico	Alta (3)	Alto (3)	9
Herramientas para empresas en la nube	C7	Explotación de vulnerabilidades	Alta (3)	Alto (3)	9

Fuente: Elaboración Propia

Los planes para generar y actualizar las salvaguardas deben estar fundamentados en la normativa SEPS-IGT-IR-ISF-ITIC-IGJ-2017-103, el reglamento interno y marcos de referencia que actualmente utilice la institución.

A manera de complemento del análisis de riesgo, existe un análisis de vulnerabilidades realizado por uno de los proveedores de la institución, el cual refleja datos alarmantes en cuanto a la seguridad perimetral, como por ejemplo:

Ataque y vulnerabilidades de software explotadas, se puede encontrar un listado de más de 80 direcciones IP públicas de todas partes del mundo, que han atacado a la institución.

La fuga de datos demuestra que hay 36 aplicaciones que actualmente usan los empleados para poder enviar su información hacia el exterior de la Cooperativa.

El ancho de banda consumido por algunas de las aplicaciones es preocupante, pues se tratan de túneles que usan en los equipos terminales para poder saltarse las reglas de navegación, convirtiéndose en blancos fáciles para ser objetos de ataques e infectar toda la red LAN de la empresa.

En cuanto a las aplicaciones de acceso remoto para soporte está siendo utilizado por el departamento de TI exclusivamente, pero no dejan de ser un riesgo pues pueden pasar por alto la seguridad perimetral y esconder identidades, de lo revisado estos accesos están siendo muy utilizados.

Los detalles mencionados han sido los puntos más relevantes del análisis de vulnerabilidades realizado por el proveedor Coresolutions, y, con una de las herramientas que dispone la marca Check Point.

Como se puede observar el estado inicial de la Cooperativa en cuanto a su seguridad requiere de cambios sustanciales, por lo que se debe actuar de inmediato para ir solucionando todos estos hallazgos de manera ordenada y progresiva.

Evaluación de herramientas idóneas

En el mercado se ofertan soluciones propietario y open source con las que se pueden solventar los hallazgos detallados en la sección anterior, pero estos deben ser seleccionados de acuerdo a varios criterios:

- Tipo de institución.- al ser una entidad financiera, se requiere de una garantía en todos los activos que se puedan adquirir, ya sea hardware o software y más aún cuando se trata de proteger la información de los Socios, por lo que se recomienda considerar soluciones propietario como primera opción.
- Dimensionamiento.- todas las herramientas están diseñadas y elaboradas en base a una necesidad existente en las distintas empresas pero su rendimiento puede variar entre una y otra, por lo tanto se debe primero determinar los requerimientos de la institución y el alcance que debe tener la implementación de la solución seleccionada.
- Presupuesto.- los departamentos tienen asignados presupuestos anuales para poder trabajar, por lo que la solución que se busque debe ajustarse a este, tomando en cuenta que se deben desarrollar varios proyectos durante un año.

Con estos criterios se procede con la búsqueda de una solución de seguridad de perímetro que se ajuste a la necesidad institucional y que pueda soportar el crecimiento proyectado.

Las herramientas a evaluar deben ajustarse a los procesos que se deben desarrollar para proteger los accesos a la red LAN de la institución, ya que sin ellos serían una herramienta más y podría llegar a verse como un gasto innecesario. De acuerdo a lo antes expuesto lo que se requiere es de un software que permita el acceso de dispositivos a la red institucional, por lo que a más de un firewall de perímetro debidamente configurado es necesaria una herramienta que ayude a controlar dichos accesos de manera controlada y con perfiles establecidos para evitar intentos de acceso a lugares donde no está permitido; hoy en día existe la tecnología UEM (Unified Endpoint Management) que no solo ayuda con lo detallado, también hace administración de usuarios, revisión, actualización de dispositivos, administra recursos, provee seguridad, control de acceso y

entrega de apps. Este software libera al departamento de TI de una importante carga de trabajo y ofrece a los usuarios la flexibilidad que desean para ejecutar su trabajo.

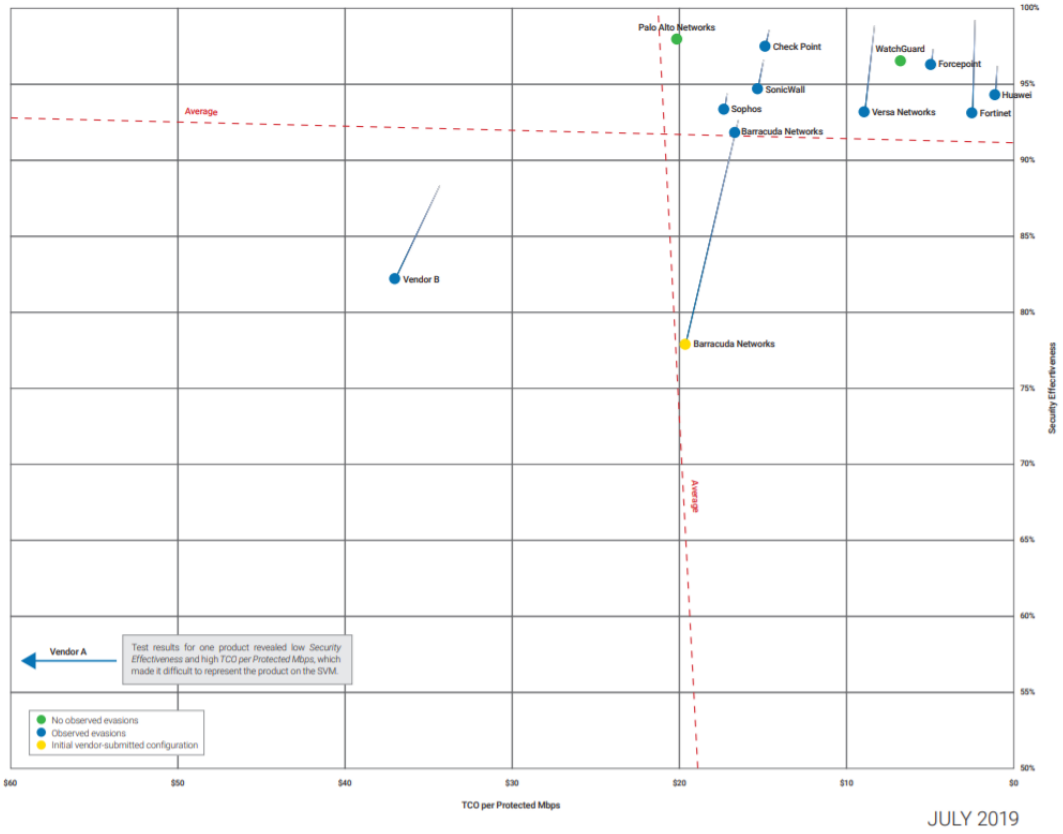
Como ya se mencionó la herramienta que debe ser evaluada con detenimiento es el firewall de perímetro cuyas funciones básicas son: filtrado de paquetes, proxy, sistemas de detección y prevención de intrusos, protección contra malware, control de aplicaciones, permisos de navegación, listas negras, etc; por el momento la institución ha implementado un firewall de la marca Dell modelo Sonicwall TZ500, capaz de soportar el troughtput de 300 usuarios y con un software capaz de realizar los controles que se detallan anteriormente. El equipo fue adquirido de manera atípica, pues era parte de la infraestructura de una cooperativa que fue absorbida, por lo que se aprovechó para mejorar el existente. Una de las comparativas que no deben faltar es el cuadrante mágico de Gartner. Gartner es una empresa con cuarenta años de experiencia y líder en investigación de tecnología y asesoramiento, que ha expandido sus líneas de investigación para ofrecer a sus clientes consejos, herramientas e ideas integrales con las que podrán alcanzar todas sus prioridades(*About Gartner*, n.d.). Uno de sus servicios es el Cuadrante Mágico en donde se puede apreciar claramente el performance del software que han evaluado, es así que para julio del 2019 Sonicwall está ubicado en el cuadrante de "niche players" y con un rendimiento medio como se puede observar en la siguiente gráfica.

Ilustración 1Cuadrante Mágico NGFW

Fuente 1 Gartnet Septiembre 2019

NSS Labs es una empresa que realiza pruebas de rendimiento en distintos aplicativos basados en la demanda existente en el mercado y lo que miden en cada test son: efectividad, evasión, rendimiento, estabilidad, usabilidad y costo de propiedad(Labs, n.d.). En el siguiente cuadro se podrá observar el costo de la seguridad perimetral que se puede tener por Mbps (Mega Bits Por Segundo), pudiendo determinar que para el firewall implementado el costo por Mbps es aproximadamente de $15,00 (quince dólares) y con una efectividad de menos del 95%

Ilustración 2 SVM para NGFW



Fuente: NSS Labs

De la misma manera se procede con el análisis de la herramienta que mejor puede adaptarse a las necesidades de la institución en cuanto a un UEM, primero el cuadrante de Gartner para tener una idea clara del rendimiento de las distintas opciones.

Ilustración 3 Cuadrante MágicoUEM

Fuente 2 Gartner Agosto 2019

Debido a que no hay implementado una herramienta similar, se tomarán en cuenta las herramientas que se ubican en el cuadrante de "Leaders", las cuales deben ser evaluadas en base a las siguientes características principales:

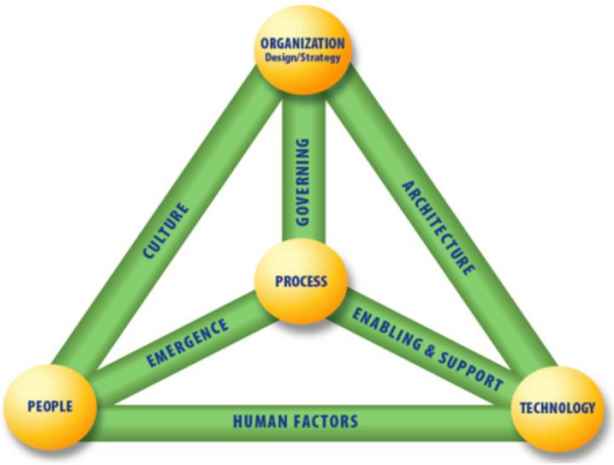
- Acceso a cualquier tipo de aplicaciones ya sean cloud, empresariales o de movilidad, organizadas en un catálogo único.
- Inicio de sesión único, que pueda integrarse a directorios LDAP.
- Acceso sin contraseñas desde dispositivos de confianza con autenticación biométrica o tiempos de espera para recibir un PIN.
- Su arquitectura debe funcionar con dispositivos existentes en el mercado y con los que dentro de un futuro cercano aparezcan.
- La gestión de dispositivos debe ser en conformidad con la tecnología Unified Endpoint Management UEM.

- El costo de la implementación es una característica en la que los administradores pondrán más atención.

La creación de procesos que indiquen el camino a seguir para mejorar la seguridad en los accesos a la red LAN deben estar alineados con marcos de referencia internacionales reconocidos que garanticen la buena práctica en los mismos y sean fáciles de auditar. Para esto existen dos marcos con los que se puede trabajar, ITIL v4 y Cobit 5.

En el año 2012 ISACA por medio de Cobit 5 lanzó la guía llamada "Cobit 5 for Security Professionals" en donde presenta un enfoque integral orientando al negocio la gestión de la seguridad de la información, estableciendo un lenguaje estándar para hacer alusiones a la protección de la información; son varios los componentes del Business Model for Information Security BMSI que se habilitan para interactuar y respaldar la gestión en la organización ayudando al cumplimiento de sus objetivos y creando valor. Utilizando este marco de referencia como guía para levantar y mejorar procesos se cumple con la normativa vigente y se obtiene proceso que pueden ser mapeables y de fácil auditoría.

Ilustración 4 Componentes de BMIS



Fuente: Cobit 5

Metodología

Para la elaboración del artículo se utilizó una investigación descriptiva, en virtud de que se realiza una descripción del estado actual de la institución en cuanto a su infraestructura tecnológica y procesos; para posteriormente generar la propuesta que se adapte a la realidad encontrada.

El método utilizado es el inductivo y las técnicas e instrumentos fueron la entrevista, la observación y recopilación de información

Resultados

La seguridad de la información de acuerdo al Computer Security Handbook de NIST (National Institute of Standards and Technology) está definida de la siguiente manera: "*La protección brindada a un sistema de información automatizado para lograr los objetivos aplicables de preservar la integridad, disponibilidad y confidencialidad de los recursos del sistema de información (incluye hardware, software, firmware, información / datos y telecomunicaciones)"*(Nieles et al., 2017), siendo estos tres últimos sus pilares con los cuales deben crearse las metodologías que ayudarán a proteger el activo más preciado para una empresa, su información. Para una institución financiera la seguridad de su información es una prioridad, pues esta trabaja con el dinero de las personas que lo han depositado confiando en que lo van a mantener seguro, que las transacciones monetarias que puedan realizar por medio de la institución sean seguras, que siempre tenga disponible su dinero, que su información no sea visible para el público; las instituciones financieras deben hacer grandes esfuerzos para mitigar los riesgos y mantener las debidas seguridades en toda su infraestructura. En el país fue creado un ente regulador llamado Súper intendencia de Economía Popular y Solidaria SEPS, al cual las cooperativas de ahorro y crédito deben rendir cuentas de manera periódica entregando documentación auditable de sus movimientos, estado de procesos, balances, cumplimiento de normativas, etc., que deben estar de acuerdo al reglamento y normativas vigentes de dicho ente regulador. Para el caso de la seguridad de la información existe una normativa que todas las cooperativas deben cumplir, caso contrario son sancionadas de acuerdo a la gravedad de la falta cometida.

La situación actual de la cooperativa de ahorro y crédito del caso de estudio demuestra que debido a un crecimiento acelerado en los últimos años, los procesos establecidos para ofrecer la seguridad que requiere la institución necesitan revisarse para mejorarlos y adaptarlos a las nuevas necesidades existentes.

La infraestructura central y en especial los equipos que ofrecen seguridad en el perímetro de la red LAN necesitan de actualizaciones inmediatas.

Desde inicios del año 2019 se realizaron adquisiciones y creaciones de nuevos departamentos, con el objetivo de mejorar los procesos y controles para el cumplimiento de las normativas vigentes, sin embargo, a pesar del progreso evidente, se necesita que continúen con el proceso de mejora continua.

La propuesta para mejorar la seguridad perimetral de la cooperativa está basada en el uso de un marco de referencia internacional reconocido para levantamiento y mejora de procesos, ya que al ser una metodología estandarizada y comprobada, se puede obtener las herramientas para la creación, implementación, control y auditoria de los proceso que se necesiten. La guía "Cobit 5 for Security Professionals"(*COBIT 5 Spanish*, n.d.), esta guía es la indicada para la gestión de la seguridad de la información y su gobierno; todo esto basado en los procesos de negocios de la organización, creando valor para los interesados por medio de actividades, recomendaciones, explicaciones y procesos; al final propondrá una visión de gobierno y de gestión de la seguridad de la información por medio de la creación de una guía que debe contener su establecimiento, implementación y mantenimiento. La implementación de la nueva metodología dentro de la institución iniciará con una campaña agresiva de capacitaciones a todo el personal involucrado quienes deben hacer la transferencia de conocimientos al resto del personal, una vez que se lo ha socializado la segunda etapa inicia con la implementación de manera progresiva de dicha metodología, adaptando los procesos existentes a esta.

Una vez establecidos la metodología para creación y actualización de procesos, establecer un plan de mejora continua para la creación de políticas de seguridad perimetral y aplicarlas a los equipos que se adquieran para que cumplan con este cometido, incluyendo el monitoreo y posterior análisis de las herramientas que mediante el Comité de Tecnología determinar si el dimensionamiento del equipo todavía soporta el tráfico de información que se genera desde la red LAN hacia internet y viceversa, haciendo énfasis en el cumplimiento de la normativa. Como recomendación adicional, debe realizarse análisis de vulnerabilidades en toda la red LAN al menos 2 veces al año, lo cual también es parte de cumplimiento de normativas y servirá de insumo para el plan de mejora continua.

Para mejorar el control de accesos desde la WAN hacia la red institucional y su administración, se recomienda implementar una herramienta de software que utilice la nueva metodología UEM, es la última generación de software que gestiona y monitorea cada dispositivo del usuario a través de

todo el ciclo de vida (device deployment, configuración, seguridad, monitoreo y soporte)(Reyes, 2013). Así los usuarios disfrutan la libertad de utilizar sus dispositivos y las empresas saben que sus empleados ingresan de manera segura su información por lo tanto el rendimiento en sus actividades laborales tendrá una clara tendencia de incremento. Se recomienda utilizar Workpace One de VMware(VMware, n.d.), es una herramienta que cumple con las características deseadas y plasmadas en la evaluación de las herramientas idóneas y adicional a esto la institución ya cuenta con experiencia con el manejo de software de la misma marca en la virtualización de servidores, por lo que la integración no implica un rango de tiempo mayor a 3 meses debido al conocimiento previo que tienen los colaboradores responsables del área de infraestructura central.

Conclusiones

Con la contratación de un oficial de seguridad de la información OSI debe continuar con el proceso de cambio en este departamento para cumplir con lo establecido en la norma

Los cambios e incorporaciones en cuanto a las herramientas de software que ayuden a mejorar el control de accesos requiere de la creación de procesos con los que se pueda soportar toda su gestión

La existencia de documentación, manuales, procesos existentes fueron creados en base a reglamentos internos y normativas vigentes del ente de control pueden ser mejoradas con la incorporación de una metodología internacional y reconocida en este caso Cobit 5.

El plan de adquisiciones no se adapta a los requerimientos del área provocando que no se pueda contar con las debidas herramientas para la gestión y administración del departamento de TI, a esto se suma la inexistencia de un plan de capacitaciones continuo que debe ser el complemento de todas las adquisiciones que se realicen.

La infraestructura tecnológica de la Cooperativa ha mejorado en el último año con la incorporación de nuevos equipos y software de gestión que ayudan a la administración del departamento, sin embargo, todavía existe una brecha que debe cubrirse para el cumplimiento de la normativa de la SEPS.

El plan de mejora continua debe fundamentarse en el análisis de riesgos presentado pues existen nueve amenazas que pueden afectar gravemente a los activos de la Cooperativa, por lo que todo plan, proceso, adquisición que se realice debe orientarse a mitigar estos hallazgos.

La selección de nuevo software o hardware debe seguir un proceso que garantice la idoneidad del activo frente a la necesidad de la Cooperativa, evitando la compra innecesaria o mal dimensionada.

Referencias

1. About Gartner. (n.d.). Retrieved January 21, 2020, from https://www.gartner.com/en/about
2. COBIT 5 Spanish. (n.d.). Retrieved January 19, 2020, from http://www.isaca.org/COBIT/Pages/COBIT-5-spanish.aspx
3. coordinación de contenidos, E., General de Modernización Administrativa, D., & Impulso de la Administración Electrónica, P. (2012). Magerit versión 3.0: Metodología de análisis y gestión de riesgos de los Sistemas de Información. Libro I: Método (version 3.). http://administracionelectronica.gob.es/
4. GomezMiguel, A. (2012). Bienvenidos a la Superintendencia de Economía Popular y Solidaria - SEPS - SEPS (M. de H. y A. Públicas (Ed.); version 3.). https://www.seps.gob.ec/
5. Labs, N. (n.d.). NGFW 2019: Security Value Map – NSS Labs, Inc. Retrieved January 21, 2020, from https://www.nsslabs.com/reports/14202/
6. Nieles, M., Dempsey, K., & Pillitteri, V. Y. (2017). NIST Special Publication 800-12 Revision 1 An Introduction to Information Security. https://doi.org/10.6028/NIST.SP.800-12r1
7. Reyes, V. (2013). BYOD y la movilidad corporativa. http://www.redicces.org.sv/jspui/bitstream/10972/1985/1/BYOD y la mobilidad.pdf
8. VMware. (n.d.). VMWARE WORKSPACE ONE Sencillez para el usuario, seguridad para la empresa.

References

1. About Gartner (n.d.). Retrieved January 21, 2020, from https://www.gartner.com/en/about
2. COBIT 5 Spanish. (n.d.). Retrieved January 19, 2020, from http://www.isaca.org/COBIT/Pages/COBIT-5-spanish.aspx

3. content coordination, E., General of Administrative Modernization, D., & Impulse of Electronic Administration, P. (2012). Magerit version 3.0: Methodology of analysis and risk management of Information Systems. Book I: Method (version 3.). http://administracionelectronica.gob.es/
4. Gomez Miguel, A. (2012). Welcome to the Superintendence of Popular and Solidarity Economy - SEPS - SEPS (M. de H. y A. Públicas (Ed.); Version 3.). https://www.seps.gob.ec/
5. Labs, N. (n.d.). NGFW 2019: Security Value Map - NSS Labs, Inc. Retrieved January 21, 2020, from https://www.nsslabs.com/reports/14202/
6. Nieles, M., Dempsey, K., & Pillitteri, V. Y. (2017). NIST Special Publication 800-12 Revision 1 An Introduction to Information Security. https://doi.org/10.6028/NIST.SP.800-12r1
7. Reyes, V. (2013). BYOD and corporate mobility. http://www.redicces.org.sv/jspui/bitstream/10972/1985/1/BYOD and the mobility.pdf
8. VMware (n.d.). VMWARE WORKSPACE ONE Simplicity for the user, security for the company.

Referências

1. Sobre o Gartner (n.d.). Recuperado em 21 de janeiro de 2020, em https://www.gartner.com/en/about
2. COBIT 5 Espanhol. (n.d.). Recuperado em 19 de janeiro de 2020, de http://www.isaca.org/COBIT/Pages/COBIT-5-spanish.aspx
3. coordenação de conteúdo, E., Geral de Modernização Administrativa, D., & Impulse of Electronic Administration, P. (2012). Magerit versão 3.0: Metodologia de análise e gerenciamento de riscos de Sistemas de Informação. Livro I: Método (versão 3.). http://administracionelectronica.gob.es/
4. Gomez Miguel, A. (2012). Bem-vindo à Superintendência de Economia Popular e Solidária - SEPS - SEPS (M. de H. e A. Públicas (Ed.); Versão 3.). https://www.seps.gob.ec/
5. Labs, N. (n.d.). NGFW 2019: Mapa de valores de segurança - NSS Labs, Inc. Recuperado em 21 de janeiro de 2020, em https://www.nsslabs.com/reports/14202/

6. Nieles, M., Dempsey, K., & Pillitteri, V.Y. (2017). Publicação Especial NIST 800-12 Revisão 1 Uma Introdução à Segurança da Informação. https://doi.org/10.6028/NIST.SP.800-12r1
7. Reyes, V. (2013). BYOD e mobilidade corporativa. http://www.redicces.org.sv/jspui/bitstream/10972/1985/1/BYOD e a mobilidade.pdf
8. VMware (n.d.). VMWARE WORKSPACE ONE Simplicidade para o usuário, segurança para a empresa.