Polo del Conocimiento

Pol. Con. (Edición núm. 42) Vol. 5, No 02
Febrero 2020, pp. 674-696
ISSN: 2550 - 682X
DOI: 10.23857/pc.v5i2.1305

Acceso y seguridad a la red wifi mediante la tecnología CISCO identity services engine (ise) para los usuarios de la Empresa Indurama de Cuenca, Ecuador

Access and security to the wifi network through CISCO identity services engine (ise) technology for users of the Indurama Company of Cuenca, Ecuador

Acesso e segurança à rede wifi através da tecnologia do motor de serviços de identidade CISCO (ise) para usuários da Empresa Indurama de Cuenca, Equador

Diego Sebastián Ñauta-Tapia [I]
sebasnauta87@hotmail.com.
https://orcid.org/0000-0002-9124-5497

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

Correspondencia: sebasnauta87@hotmail.com

Ciencias de las ingenierías
Artículo de investigación

*__Recibido:__ 18 de diciembre de 2019 *__Aceptado:__ 25 de enero de 2020 * __Publicado:__ 03 de febrero de 2020

I. Universidad Católica de Cuenca, Maestría en Tecnologías de la Información, Cuenca, Ecuador.
II. Universidad Católica de Cuenca, Unidad Académica de Tecnologías de la Información y la Comunicación, Cuenca, Ecuador.

Resumen

El objetivo de esta investigación fue realizar una propuesta de mejora en el acceso y seguridad de los usuarios a la red wifi en la empresa Indurama de Cuenca, Ecuador, mediante la tecnología CISCO Identity Services Engine (ISE). Como metodología se realizó un diagnóstico del programa informático instalado en las redes de la empresa, el ISE de Cisco y, se llevó a cabo un autodiagnóstico, tomando como base la norma ISO 27001. En cuanto a los resultados se encontró que tanto la red wifi de empleados Wifi-ConsensoCorp y la red wifi de invitados Wifi-Invitados, presentan fallas de seguridad. Se concluyó que el sistema de seguridad de la empresa requiere de mejora de la herramienta ISE y se propone corregir esta situación a través de la reinstalación del ISE a fin de proteger los datos de la empresa de cualquier violación a sus protocolos de seguridad.

Palabras claves: Tecnología; programas de seguridad; protocolos.

Abstract

The objective of this research was to make a proposal to improve the access and security of users to the Wi-Fi network in the Indurama Company of Cuenca, Ecuador, by means of the CISCO Identity Services Engine (ISE) technology. Computer program installed in the company's networks, the Cisco ISE and, a self-diagnosis was carried out, based on the ISO 27001 standard. Regarding the results, it was found that both the Wi-Fi network of Wifi-ConsensoCorp employees and the Wifi network of guests Wifi-Guests have security flaws. It was concluded that the company's security system requires improvement of the ISE tool and it is proposed to correct this situation through the reinstallation of the ISE in order to protect the company's data from any breach of its security protocols.

Keywords: Technology; security programs; protocols.

Resumo

O objetivo desta pesquisa foi fazer uma proposta para melhorar o acesso e a segurança dos usuários da rede Wi-Fi na empresa Indurama de Cuenca, Equador, utilizando a tecnologia CISCO Identity Services Engine (ISE). Programa de computador instalado nas redes da empresa, o Cisco ISE e, foi realizado um autodiagnostico, com base na norma ISO 27001. Quanto aos resultados,

verificou-se que tanto a rede Wi-Fi dos funcionários da Wifi-ConsensoCorp quanto os Rede Wifi de convidados Wifi-Hóspedes, possuem falhas de segurança. Concluiu-se que o sistema de segurança da empresa requer aprimoramento da ferramenta ISE e propõe-se corrigir essa situação através da reinstalação do ISE, a fim de proteger os dados da empresa de qualquer violação de seus protocolos de segurança.

Palavras-chave: Tecnologia; programas de segurança; protocolos.

Introducción

Las telecomunicaciones constituyen hoy en día una herramienta fundamental para la sociedad moderna, están presentes en todos los ámbitos de la vida del ser humano desde el social hasta el económico y empresarial, se encuentran en todos los tipos de dispositivos móviles, GPS, internet, entre otros. En este sentido, el internet junto a las redes sociales, la banda ancha, las redes inalámbricas, son el mejor ejemplo de lo que significan las telecomunicaciones en la actualidad, en cuanto a las múltiples posibilidades que ofrecen: disponibilidad de contenido, comunicación bidireccional e instantánea, comercio en línea, estudiar en línea, trabajar en línea, transferencias bancarias, entre muchas otras necesarias e importantes actividades en un mundo globalizado y digital. Según, Dordoigne (2018)

> Las telecomunicaciones, mediante las redes inalámbricas, son la nueva tendencia tecnológica que se utiliza en todos los mercados comerciales y de servicios, fomentando la eficiencia, ahorro de tiempo entre las personas y trabajo, además de la disminución de costos para las organizaciones.

Sobre este particular, en el mundo de hoy, ya sea para una persona, empresa u organización, las telecomunicaciones se han convertido en un requisito importante para participar de una sociedad cada vez más dependiente de la tecnología. Así, en el ámbito empresarial se han convertido en un recurso clave para mejorar el intercambio de información entre empresas y con los clientes, para aumentar la rentabilidad, la competitividad y optimizar los costos. En este contexto, el carácter mundial de las plataformas de las telecomunicaciones permite una mayor integración de la economía mundial. Según el informe de GlobalWebIndex (2016: p.2). “El comercio a través de redes sociales ha tenido un incremento de 80%.”

Por otra parte, de acuerdo al informe elaborado por la International Telecomunication Union (ITU, 2015: p. 3):

> "Los usuarios que se conectan de dispositivos móviles también han incrementado de 2.2 a 7.1 mil millones en los últimos diez años y la contratación de anchos de banda para estos mismos dispositivos creció de 0.8 a 3.5 mil millones en los pasados cinco años."

En un sentido similar de acuerdo con la página internet World Stats "ya son aproximadamente 3 mil millones de personas conectadas a la red de redes, internet" es por ello que, muchos autores consideran que el sector de las telecomunicaciones es decisivo y esencial para el desarrollo global, así como para fomentar la competitividad en las regiones.

En este contexto, la competitividad en las empresas se relaciona con la eficiencia y eficacia de todos los recursos de la organización. Con base en esta premisa y con la finalidad de lograr mayores márgenes de ganancia, los empresarios buscan mejorar continuamente los procesos por medio de la integración de nuevas tecnologías para simplificar, y mejorar los procedimientos que se llevan a cabo en la organización.

Sin embargo, a pesar de que las telecomunicaciones ofrecen un mundo de oportunidades, de acuerdo con Méndez, Mosquera y Rivas (2015) "existe la contra parte que opera en el robo de información ocasionando pérdidas económicas para la empresa." Por tanto, las redes corporativas desde donde se transfiere o publica toda la información de los usuarios cuando se utiliza internet desde diversos dispositivos ya sean, servidores, hubs, routers, firewalls, servidores DNS, entre otros, deben ofrecer un nivel óptimo de seguridad.

A este respecto, la Organización Internacional de Estandarización (ISO) emitió una norma conocida como la ISO 27001:2013 (también conocida como BS EN 27001:2017) que proporciona un marco para que "los sistemas de gestión de seguridad de la información puedan mantener la confidencialidad, integridad y disponibilidad de la información y cumplan los requisitos legales. Esta norma es esencial para proteger su activo más importante, la información."

Cabe apuntar que la confidencialidad, integridad y disponibilidad constituyen la base sobre la cual se sostiene la seguridad de la información de amenazas como: el crimen cibernético; fugas de datos personales; vandalismo/terrorismo; incendio/daños; uso indebido; robo; ataque viral, entre otros.

De acuerdo con el Sistema de Gestión de Seguridad de la Información (SGSI: 2019), en referencia a la confidencialidad: "la información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados" De manera similar, este organismo señala que: "la integridad es el mantenimiento de la exactitud y completitud de la información y sus métodos de proceso." Y la disponibilidad es entendida como el acceso y utilización de la información y los sistemas de tratamiento de esta por parte de los individuos, entidades o procesos autorizados cuando lo requieran.

En la misma línea, en la actualidad la tecnología es considerada un activo de las empresas y, al momento de implementarlas o renovarlas es necesario tener en cuenta la seguridad de la información. Al momento presente, la red de una empresa se extiende donde se encuentran sus clientes, empleados y sus datos. En muchas ocasiones, los empleados necesitan acceso a los recursos de la empresa desde distintos dispositivos y a través de redes públicas, por lo que la organización debe estar asegurada y protegida ante la diversidad de dispositivos habilitados para la red y ante la amenaza que representan los ataques y violaciones cibernéticos para evitar comprometer el acceso a la confidencialidad del gran número de datos que generalmente manejan las organizaciones empresariales.

Es así como en el mercado existen algunas alternativas para mejorar la seguridad de las empresas y de los usuarios de las redes locales Wireless (WLAN) como: Cisco Identity Services Engine (CISCO ISE) que según Cruz (2016) "hace las funciones análogas a las de un vigilante de seguridad de la empresa, que está a la entrada de la organización y revisa la autorización del personal o visitante que quiere entrar dentro de la empresa." Entre algunas de sus características están: "centralizar y unificar el control de acceso seguro basado en el rol de cada usuario para proporcionar una política de acceso a la red coherente independientemente de que se conecten a través de cable, red inalámbrica." Partner, (2016). Así como también: "obtener una mayor visibilidad y una capacidad de identificación más precisa de los dispositivos con el sistema de visualización de perfiles de Cisco ISE, que reduce el número de endpoints desconocidos. (Datacom.global, 2017)."

De acuerdo con el glosario de terminología informática, endpoints o punto final son el puerto de comunicaciones empleado para realizar llamadas a procedimientos remotos. Sobre este particular, Vásquez (2016) señala que:

> Los endpoints son los equipos de escritorio, laptops, teléfonos inteligentes, impresoras, cajeros automáticos (ATM) y equipos de punto de venta que forman parte de su Red de Área Local (LAN, por sus siglas en inglés) que pese a estar protegidos por las capas de seguridad de Gateway y de red, requieren contar con funciones básicas de seguridad para bloquear el malware avanzado que podría infiltrarse en su empresa; evitar las pérdidas de datos valiosos, e inclusive que algún miembro de su equipo no cumpla con las normas que rigen el uso de soportes capaces de ser extraídos (como las llamadas memorias USB o pendrives), además de dar acceso seguro al correo electrónico y aplicaciones web (aquellas que funcionan en la nube).

De igual forma, otra de las características resaltantes de este sistema de protección digital es la de: "simplificar la incorporación y gestión de los usuarios mediante la creación de portales cliente 100% personalizables en minutos que permiten gestionar fácilmente la experiencia de usuario. (Datacom.global, 2017)." Igualmente, de acuerdo con los señalamientos de Ciberseguridad Industrial, (2020) otra de sus características es:

> Compartir los datos de usuario y dispositivo con la red de partners y soluciones de seguridad para aumentar la eficacia de éstas y acelerar el tiempo de contención de amenazas. Contener amenazas automáticamente a través de la integración con Cisco FirePower Management Center y otros partners tecnológicos.

Según informe de expertos en el área "La solución ISE 2.0 se ha rediseñado para facilitar aún más un control de acceso seguro uniforme a través de redes por cable o inalámbricas de varios proveedores y las conexiones VPN remotas. Cisco ISE profundiza en la red para ofrecer una visibilidad superior acerca de quién y qué accede a los recursos." (CISCO, 2015).

Es importante acotar que básicamente, la función que cumple CISCO ISE es la de facilitar las conexiones VPN remotas, que es una red privada virtual en la que todos los datos son prácticamente anónimos mientras se navega por internet, y un punto importante es también la definición de perfiles y sensores inteligentes, que quiere decir, a través de ciertos filtros, se puede detectar información peligrosa provenientes de ataques cibernéticos.

En el caso de la empresa Indurama, ubicada en Cuenca, Ecuador, se ha realizado un autodiagnóstico en base a la norma ISO 27001, la misma que se basa en Cisco ISE que es una solución de control de políticas centralizadas. Los resultados de la entrevista efectuada al personal administrativo permitieron avizorar de manera general la necesidad de gestión en las

áreas políticas de seguridad, clasificación y control de activos, seguridad física y del entorno, control de accesos, mismas que se veían reflejadas en situaciones tales como: los usuarios se conectan a sus diferentes dispositivos provocando que las descargas y tareas, fuera del ámbito laboral, afecten el rendimiento de navegación de la red y a la gestión del sistema interno, además que los invitados puedan acceder a información importante de la empresa.

Con relación a la herramienta ISE, esta se encuentra actualmente funcionando en la empresa, pero, no está configurada totalmente, tiene problemas para la revisión de los logs, no muestra el consumo de las licencias base que se está usando, no tiene aplicado políticas para el acceso de los usuarios al wifi.

Por lo antes expuesto esta investigación se planteó como objetivo realizar una propuesta de mejora en el acceso y seguridad de los usuarios a la red wifi en la empresa Indurama de Cuenca, Ecuador, mediante la tecnología CISCO Identity Services Engine (ISE).

Metodología

Para el desarrollo de la investigación se tomaron en cuenta los siguientes aspectos:

Primera parte

- **Diagnóstico**

Se efectuó una revisión del programa informático instalado en las redes de la empresa, el cual corresponde al sistema ISE de Cisco. Posteriormente se llevó a cabo un autodiagnóstico, tomando como base lo establecido en la norma ISO 27001. Los resultados arrojados del diagnóstico fueron los siguientes:

En primer lugar, no permite conocer toda la información (Dashboard), es decir, no se aprecia el momento cuando otros usuarios tienen acceso a la red a través de los dispositivos, por lo tanto, la información que se refleja en la pantalla está incompleta. (Ver ilustración 1)

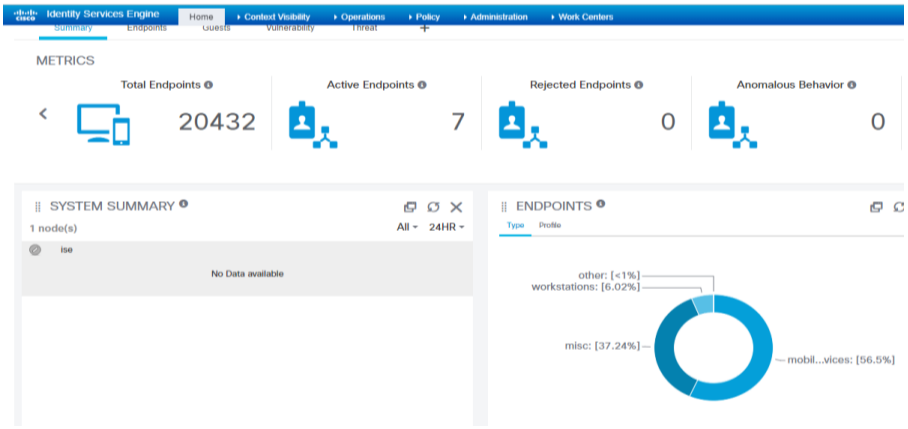

Ilustración 1: Errores de ISE en la empresa. **Fuente:** Empresa Indurama

Elaborado por: El autor

En segundo lugar, no se observa todo lo que acontece en las conexiones con relación al consumo de logs y dirección IP, también constituyen en un error de la herramienta ISE las licencias, que impide monitorear cuando se conecta un usuario, el nombre del usuario, detalle del IP o datos como por qué no se puede conectar al servidor de la empresa un usuario. Es decir, los logs no se visualizan, aparecen con datos cero, lo que constituye un error del ISE. (Ver ilustración 2)

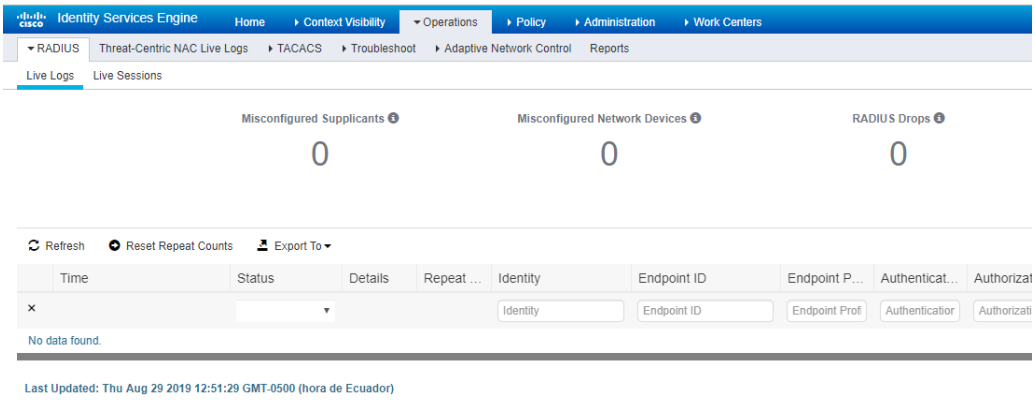

Ilustración 2: Problemas en los logs. **Fuente:** Empresa Indurama

Elaborado por: El autor

En tercer lugar, no se observa el consumo de las licencias, es decir, no se tiene acceso a la cantidad de licencias utilizadas o excedidas, lo que constituye un error de la herramienta ISE. (Ver ilustración 3)

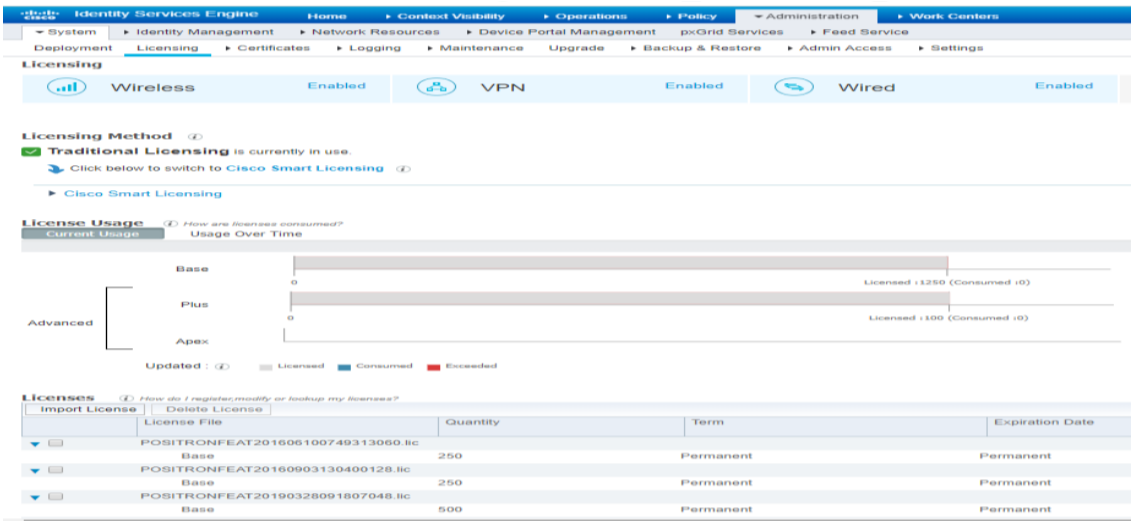

Ilustración 3: Falta de observancia en consumo de licencias. **Fuente:** Empresa Indurama

Elaborado por: El autor

En cuarto lugar, se encontró que el estado actual de funcionamiento del sistema de protección seguridad, permite a cualquier persona conectarse fácilmente a la red wifi de la empresa. (Ver ilustración 4)

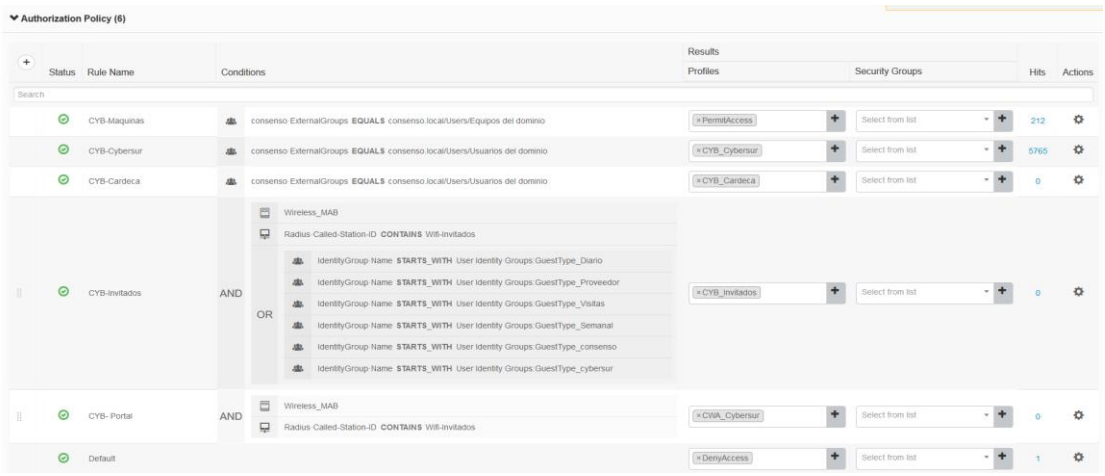

Ilustración 4: Control de errores de conexión. **Fuente:** Empresa Indurama

Elaborado por: El autor

- **Autodiagnóstico. Norma ISO 27001**

En la empresa Indurama, existen dos redes SSID, la primera red es para la conexión al wifi para los empleados, esta red se ha denominado Wifi-ConsensoCorp y la segunda es para invitados o

personas externas a la empresa se llama Wifi-Invitados. La primera red Wifi-ConsensoCorp funciona mediante conexión a active directory y se valida si el usuario tiene una cuenta hace una conexión con el ISE para autenticar y asignar el perfil que tiene 133 controles distribuidas en once secciones principales y da paso a tener la conexión (Arias, M. y Carrillo, C., 2017). Y la segunda red Wifi-Invitados es un portal cautivo que permite mediante un usuario y contraseña loguearse y tener conexión a internet.

El formulario de autodiagnóstico que se utilizó tiene como base los dominios de la ISO 27001 pero adaptados con un lenguaje más sencillo para ser interpretados tanto en usuarios finales como para la parte técnica ya que en situaciones particulares ni siquiera los técnicos pueden interpretar estás temáticas.

Las variables que se evaluaron en el autodiagnóstico fueron, políticas de seguridad, organización de la seguridad, administración de activos, seguridad de los recursos humanos, seguridad física y del ambiente, gestión de comunicación y operaciones, control de accesos, desarrollo y mantenimiento de los sistemas, administración de incidentes, gestión de la continuidad del negocio y cumplimiento. Cada tema evaluado contiene subtemas relacionados al tema principal que fueron seleccionados de acuerdo con los requerimientos de la empresa en estudio. El formato del formulario del autodiagnóstico se encuentra en el anexo 1. Los resultados del autodiagnóstico fueron los siguientes:

Autodiagnóstico: Políticas de seguridad

Con relación a las políticas de seguridad, cuenta con documentos de políticas de seguridad, a su vez hay una persona responsable de las mismas, sin embargo, no todos los documentos se encuentran con respaldo de procedimientos relativos a la seguridad de SI, los mecanismos para la comunicación a los usuarios de las normas no poseen al igual que controles regulares para verificar la efectividad de las políticas ISE.

Autodiagnóstico: Organización de la seguridad

Posee roles y asignación de responsabilidad a empelados con relación a la seguridad, las cuales son distribuidas según los departamentos de la empresa, además manejan condiciones contractuales de seguridad para con terceros y outsourcing. La información se maneja según acuerdos de confidencialidad y periódicamente se controla la seguridad de la información por una empresa independiente. Sin embargo, no hay programas de formación en seguridad para los

empleados, clientes y terceros, por otra parte, no se utilizan criterios de seguridad para el manejo de terceras partes.

Autodiagnóstico: Administración de activos

Poseen una actualización de los inventarios de activos, donde se observa activos de datos, software, equipos y servicios, esta información es llevada por un responsable, pero no disponen de una clasificación de la información según la criticidad de esta. No existe clasificación de la información según la criticidad de esta, de igual carecen de procedimientos para clasificar y etiquetar la información.

Autodiagnóstico: Seguridad de los RRHH

Esta información posee seguridad con relación a selección y baja de personal de la empresa, en caso de existir inconvenientes en la seguridad de la información, poseen un canal y procedimientos protocolizados que permiten reparar el problema además el proceso disciplinario de la seguridad de la información se cumple. Por otra parte, las responsabilidades y roles de seguridad no se encuentran definidos, los datos de incidentes no se recogen de forma detallada. Las vulnerabilidades observadas o sospechadas no son reportadas por los usuarios.

Autodiagnóstico: Seguridad física y del ambiente

La seguridad física en la empresa si existe, además de controles de entrada para restringir el acceso a personal no autorizado, además en las áreas de mayor seguridad si poseen controles adicionales que garanticen la seguridad del ambiente al igual que las áreas de carga, expedición y equipos poseen el aislamiento adecuado, pero no hay un área segura, cerrada, aislada y protegida de eventos naturales conforme el protocolo ISO 27001, no existen protecciones frente a fallos en la alimentación eléctrica, igualmente carecen de protecciones para la seguridad en el cableado frente a daños e intercepciones.

Autodiagnóstico: Gestión de comunicaciones y operaciones

Para controlar los cambios en equipos existen responsabilidades concretas, con relación a las áreas de desarrollo y producción se cumple con los protocolos de separación de estas dos áreas, además se lleva a cabo la actualización de sistemas informáticos de acuerdo con las nuevas versiones y realizan el monitoreo de software malignos previniendo daños por estas causas, los logs de fallos son detectados a tiempo, además manejan los logs para las tareas que ejecutan los operadores y existen controles para almacenar los datos informáticos como cintas discos, etc., por otra parte, se mantienen medidas de seguridad para las transacciones que se efectúan en línea. Sin

embargo, carecen de procedimientos operativos identificados según la política de seguridad ISO 27001 que indica la documentación de la información. No poseen un método para reducir el mal uso accidental o deliberado de los sistemas, no poseen contratistas externos para la gestión de los Sistemas de Información y las actividades relacionadas a la seguridad no son monitoreadas.

Autodiagnóstico: Control de accesos

Manejan el control y restricción para el acceso, poseen uso y control de password de usuarios, además de autenticación de usuarios para conexiones externas y control de routing en redes, Por otra parte, la política de control de accesos no se está aplicando, al igual que los derechos de acceso de los usuarios no se está utilizando, por otra parte, no se protege el acceso de los equipos desatendidos, no se aplica una política de uso de los servicios de red, no hay procedimientos de log-on al terminal.

Autodiagnóstico: Desarrollo y mantenimiento de los sistemas

La seguridad para desarrollo y mantenimientos de los sistemas si se aplica, pero, al no poseer una infraestructura de red con equipos Cisco ISE instalada correctamente, no se puede aseverar que la seguridad está implantada en los sistemas de información, además faltan controles criptográficos y seguridad en los ficheros de los sistemas. Por otra parte, la seguridad en los procesos de desarrollo, testing y soporte no se aplican.

Autodiagnóstico: Administración de incidentes

Cuando se producen imprevistos, estos se comunican oportunamente, además existe la gestión de incidentes, es decir, existe definidas las responsabilidades antes un incidente. No existe un diseño, redacción e implantación de planes de continuidad y no se aplica pruebas, mantenimiento y reevaluación de los planes de continuidad del negocio.

Autodiagnóstico: Gestión de la continuidad del negocio

En el sistema si se utilizan procesos para la gestión de la continuidad, además existe un marco de planificación para la continuidad del negocio. El análisis de impacto no se ha evaluado y no se han efectuado pruebas, mantenimiento y reevaluación de los planes de continuidad del negocio.

Autodiagnóstico: Cumplimiento

Con relación al cumplimiento en la empresa si cumplen con la legislación de los sistemas, además existe el resguardo de los datos de la empresa, como también consideraciones sobre las auditorías de los sistemas. Sin embargo, carece del resguardo de la propiedad intelectual y de una revisión de la política de seguridad y de la conformidad técnica.

A continuación, se presenta de forma gráfica los resultados obtenidos en el autodiagnóstico del sistema de seguridad de la empresa Indurama de Cuenca, Ecuador. (Ver ilustración 5)

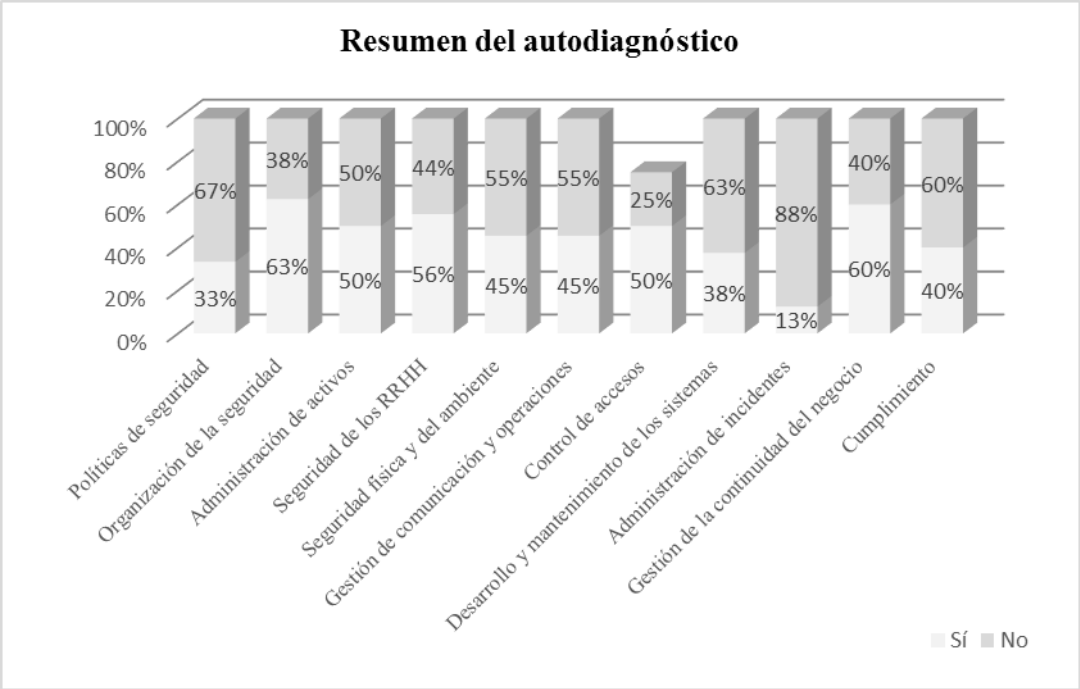

Ilustración 5: Resumen de autodiagnóstico. **Fuente:** Diagnóstico ISO 27001 a usuarios Indurama

Elaborado por: El autor

Finalmente, las observaciones se fundamentan en que la primera red tiene falencia por que mediante la herramienta ISE no existe un perfilamiento que indique si el gerente como bodeguero puedan acceder a la red wifi en la misma red ejemplo 192.168.168.0 /24, actualmente todos pueden conectarse y se debería mejorar.

La segunda red tiene la falencia que si el invitado una vez conectado con las credenciales si tiene conocimientos en informática puede tener acceso a base de datos o equipos x que tiene acceso a toda la red no hay alguna restricción.

Por lo expuesto, se propone corregir a través de la reinstalación del ISE, posteriormente, los empleados pueden conectar sus dispositivos móviles o tablets este es otro problema que se puede solucionar. Con el mismo usuario una persona que se loguee con celular o portátil tiene las mismas configuraciones.

Segunda parte

- **Recolección de datos**

Número total de usuarios que ingresan diariamente a la red wifi de Indurama

El número total de usuarios son de 340, comprende 300 empleados y 40 visitantes.

Universo de estudio y tratamiento muestral

Fórmula

$$n=(z^2.N.P.Q)/((〚e)〛^2.(N-1)+z^2.P.Q)$$

Donde:

"n = el tamaño de la muestra, N = tamaño de la población (Universo), P= Probabilidad de ocurrencia del evento, Q= Probabilidad de no ocurrencia del evento, Z = Valor obtenido mediante niveles de confianza. Es un valor constante que, si no se tiene su valor, se lo toma en relación con el 95 % de confianza equivale a 1,96 (como más usual) o en relación con el 99 % de confianza equivale 2,58, valor que queda a criterio del investigador, e = Límite aceptable de error de muestra que, generalmente cuando no se tiene su valor, suele utilizarse un valor que varía entre el 1 % (0,01) y 9 % (0,09), valor que queda a criterio del encuestador". (Pág. 15)

Desarrollo de la fórmula

(Z)	Nivel de confianza	=	95%
E	Error	=	5%
(P)	Probabilidad Ocurrencia	=	50%
(Q)	Probabilidad No Ocurrencia	=	50%
N	Universo	=	340

$$n = (1,96)2 \times (340) \times (0,5) \times (0,5)$$
$$(0,05)2 \times (340 - 1) + (1,96)2 \times (0,5) \times (0,5)$$

$$n = (3,8025) \times (340) \times (0,5) \times (0,5)$$
$$(0,0025) \times (339) + (3,8025) \times (0,5) \times (0,5)$$
$$n = 326,54$$
$$1,80$$
$$n = 181 \text{ registros de usuários}$$

Para la aplicación de los diagnósticos se consideró el total de usuarios 340, clasificados de la siguiente manera: (Ver tabla 1)

Tabla 1: Resultados de la información del número de usuarios que acceden a la red wifi de la empresa Indurama de Cuenca, Ecuador

Usuarios	Datos muestra	Muestra %	N° de diagnósticos muestra	Muestra %
Personal administrativo	300	88%	172	88%
Visitantes	40	12%	23	12%
Total	340	100%	195	100%

Fuente: Usuarios Indurama **Elaborado por:** El autor

Resultados

Luego de la aplicación del instrumento se logró obtener los siguientes resultados.

Propuesta de mejora de la herramienta ISE

Esta imagen describe la forma como debería mostrar el Dashboard de ISE. (Ver ilustración 6)

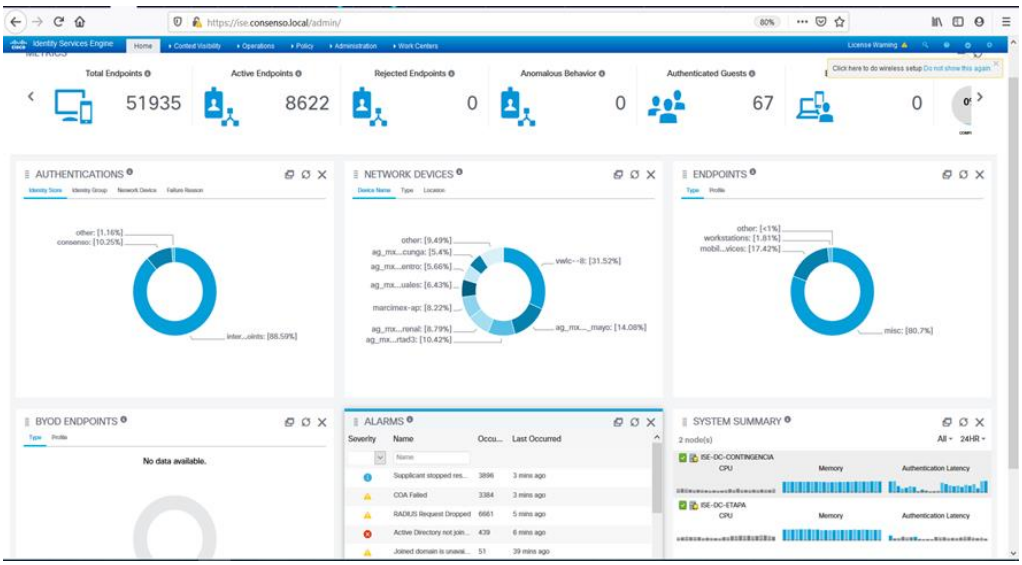

Ilustración 6: Dashboard de ISE **Elaborado por:** El autor

En relación a la segunda imagen, se puede apreciar los logs con información es útil este menú. (Ver ilustración 7)

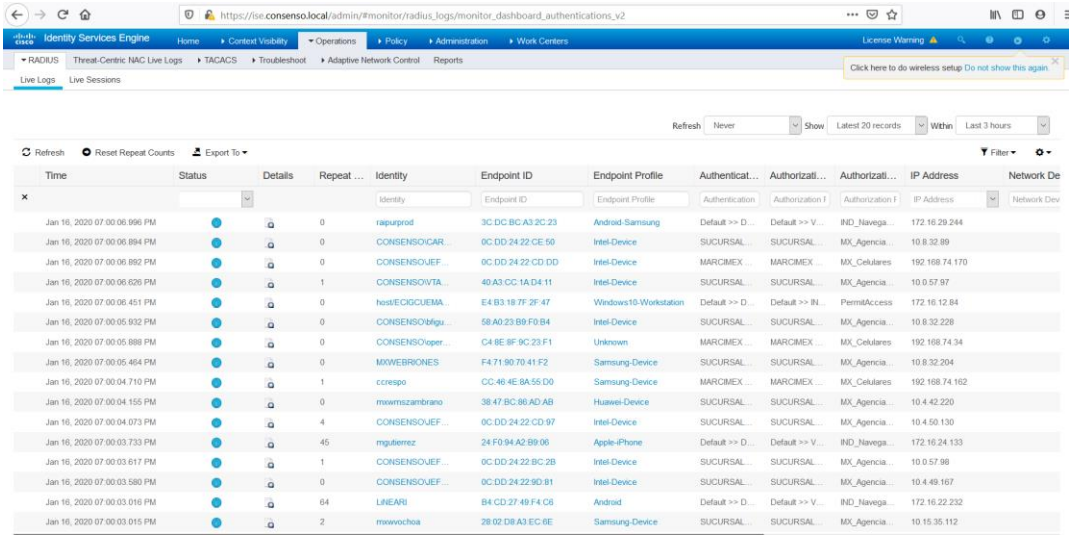

Ilustración 7: Logs **Elaborado por:** El autor

A continuación, se puede apreciar el consumo de las licencias por la barra de color azul, este momento está de 1250 licencias disponibles 821 licencias consumidas. (Ver ilustración 8)

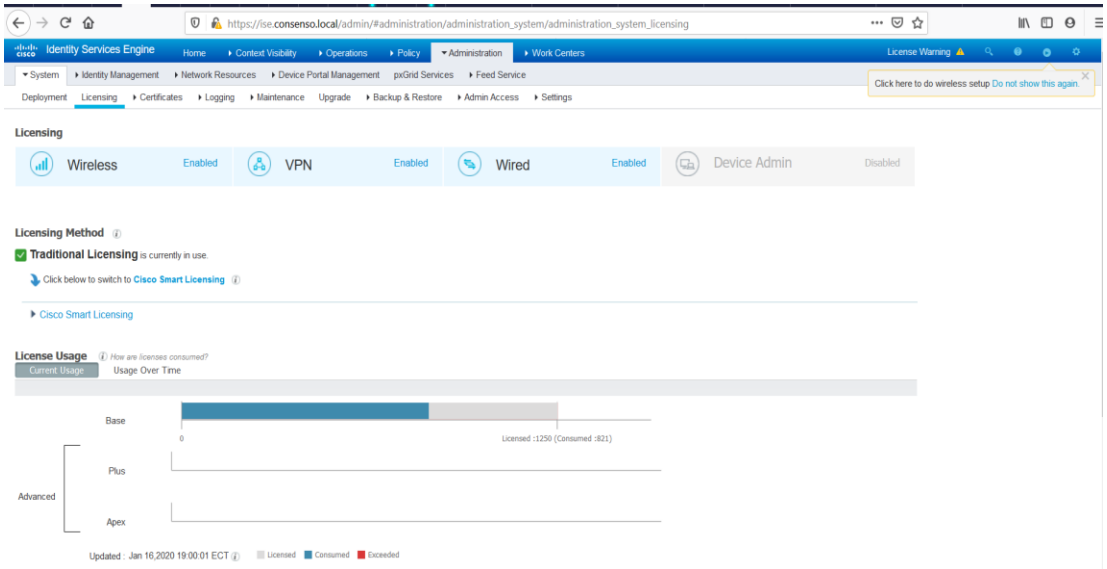

Ilustración 8: Registro consumo de licencias **Elaborado por:** El autor

Con respecto a las políticas sugeridas el sistema de seguridad quedaría configurado, de tal forma que cada persona debe tener asignado diferente ip. (Ver ilustración 9)

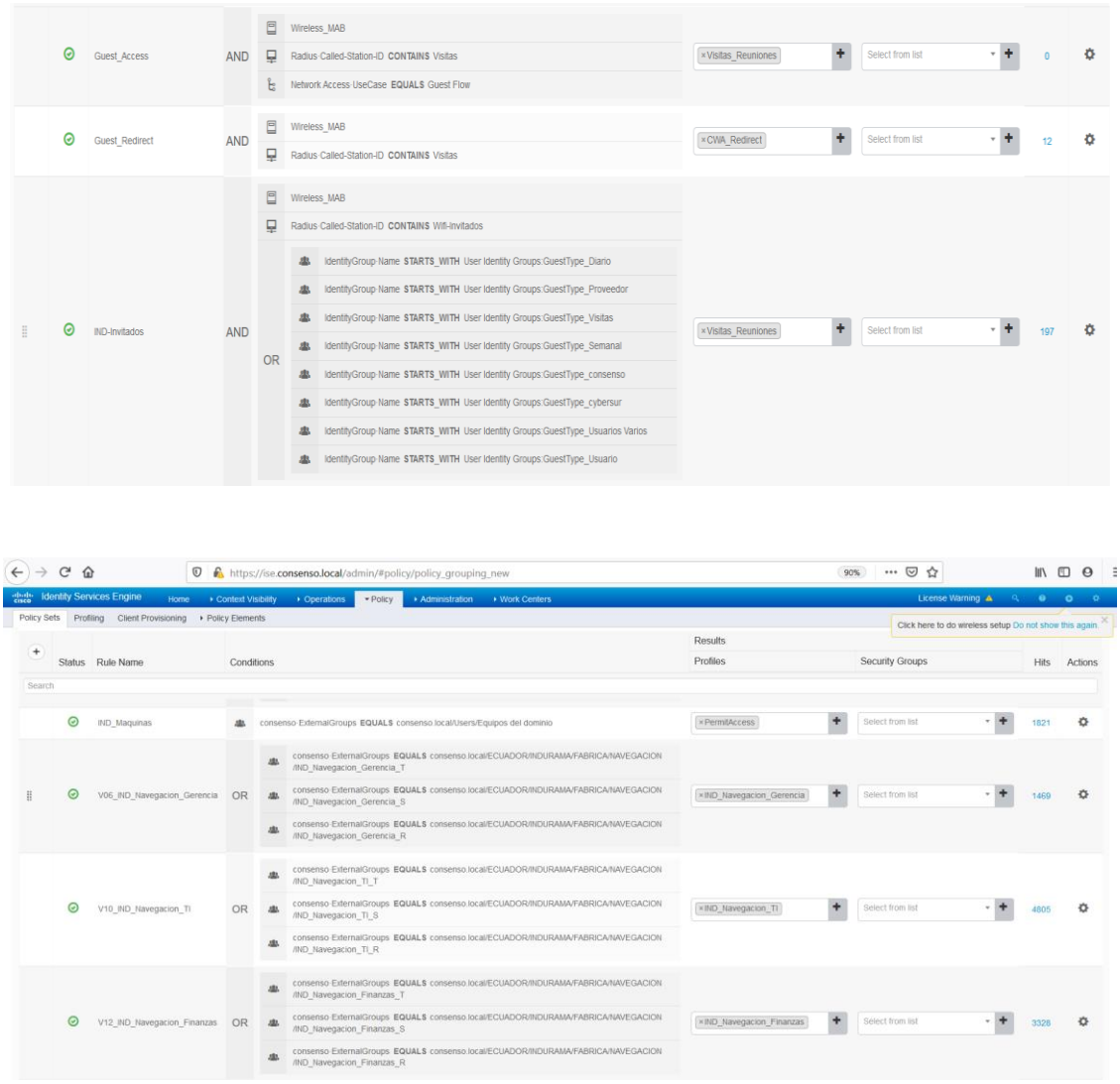

Ilustración 9: Asignación para ingreso a IP **Elaborado por:** El autor

Estructura de contenidos

Para la primera red se pretende que ISE gestione mediante perfilamientos de usuarios las conexiones por ejemplo el gerente se conectará a una red 172.16.6.0 /24 mientras que el bodeguero a otra red 172.16.27.0 /24 y también para los dispositivos como celulares o tablets asignar otra red con un ancho de banda limitada ejemplo 192.168.30.0/24. La manera como gestiona que el usuario se esté conectando con su equipo portátil o dispositivo móvil lo hará

mediante la licencia de ISE PLUS. Para la red de invitados se pretende que ISE gestione un canal solamente hacia internet evitando así el tráfico interno hacia la red de la empresa. Con la debida corrección en la base de datos o reinstalación de ISE se corrige el problema de que no se ven los logs y el consumo de licencia.

Instrumentos de evaluación

El instrumento de evaluación que se propone como mejora para el acceso y seguridad a la red wifi mediante la tecnología CISCO Identity Services Engine (ISE) para los usuarios de la empresa Indurama

Valoración de la propuesta

Una vez que se realicen las actualizaciones y modificaciones a la base de datos de ISE se podrá corregir el problema relacionado a la falta de apreciación de los logs y el consumo de licencia, parámetros que ofrece la tecnología CISCO Identity Services Engine (ISE) con la finalidad de que el acceso a la red wifi sea seguro para los usuarios.

Resultado general

Luego de que se efectúen las correcciones a la herramienta ISE, se ofrecerá un producto de calidad, cuya seguridad con relación a la información de la base de datos y usuarios restringirá el ataque cibernético, garantizado la eficiencia empresarial de Indurama

Resultados parciales

- Solución para acceder y conocer toda la información (Dashboard),
- Las conexiones con relación al consumo de logs y dirección IP.
- Control en consumo de licencias.

Conclusión

Una vez realizado el autodiagnóstico ISO 27001 se concluye que el nivel global de seguridad es del 53%, existiendo un faltante de seguridad del 47% que puede ser corregido a través de la reinstalación de esta herramienta de información aprovechando las ventajas que ofrece esta herramienta tecnológica de autenticación CISCO Identity Services Engine (ISE), al contar con políticas de actualización de datos y selección de aplicativos por su amplia gama que contribuyen al mejoramiento del servidor empresarial.

Con relación a las licencias, se evidenció un total de 1250 licencias disponibles, y en base a la propuesta planteada se observó el consumo por parte de la empresa de 821 licencias. De esta

manera se evidencia que la empresa tiene capacidad de permitir que más usuarios puedan conectarse.

En la propuesta una vez corregido el log, permite identificar al usuario y el tipo de dispositivo que utilizó para conectarse, si es portátil, (Windows o macOS), celular Apple, o Android (Samsung, LG, Huawei, etc.), identifica la dirección ip y la Mac address del equipo, como también fecha y hora que se conecta el dispositivo.

Según la configuración del perfil del usuario se establece lineamientos para determinar los permisos de navegación y de esta manera garantizar la seguridad en la información.

Referencias

1. Ciberseguridad Industrial. (2020). https://www.cci-es.org/documents/10694/148873/Catalogo-serv-sol-CiberSeguridad+Industrial.pdf.
2. CISCO. (2015). https://www.cisco.com/c/dam/assets/global/pdfs/november-security/es/c45-654884-13_ise_aag_v2a_es-eu.pdf. Recuperado el 16 de 06 de 201, de https://www.cisco.com/c/dam/assets/global/pdfs/november-security/es/c45-654884-13_ise_aag_v2a_es-eu.pdf
3. Cruz, M. (2016). Administración de políticas de seguridad de la red. CISCO ISE. [Documento en línea] Disponible en: https://www.solutel.com/administracion-de-politicas-de-seguridad-cisco-ise/
4. Dordoigne, J. (2018). Redes Informáticas: Nociones Fundamentales. Séptima Edición. Málaga, España: ENI Ediciones. Obtenido de https://www.abebooks.com/book-search/title/redes-informaticas-nociones-fundamentales/author/dordoigne/
5. GlobalwebIndex. (2016). GlobalWebIndex bi-annual report on the latest trends in online commerce.[Documento en linea] Disponible en: http://cdn2.hubspot.net/hubfs/304927/GWI_Commerce__Q1_2016_Summary.p
6. González, A, Beltrán, D y Fuentes, E. (2016). Proposal of security protocols for the local wireless network of the Cienfuegos University. Revista Universidad y Sociedad, 8(4).[Documento en linea] Disponible en: http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S2218-36202016000400017
7. http://www.internetworldstats.com/stats.htm

8. ITU (2015). International Telecomunication Union. Measuring the information society report 2015.[Documento en linea] Disponible en: https://www.itu.int/en/ITU-D/Statistics/Documents/events/wtis2015/MISR2015_Magpantay.pdf
9. Méndez, W, Mosquera, D y Rivas, T. (2015). Vulnerabilidad de protocolos de encriptación WEP, WPA y WPA2 en redes inalámbricas con plataforma Linux. Revista Tecnura, 19, 79-87. [Documento en linea] Disponible en: http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S0123-921X2015000500007
10. Partner, Ch. (2017). (Channel, Editor) [Documento en linea] Disponible en: https://www.channelpartner.es/fabricantes/noticias/1102512001102/cisco-simplifica-esquema-de-certificaciones.1.html
11. SGSI (2019). Sistema de Gestión de la Seguridad de la Información. ISO 27001. [Documento en línea] Disponible en: http://www.iso27000.es/download/doc_sgsi_all.pdf
12. Tp Link. (2013). https://www.tp-link.com/ar/support/faq/500/. Recuperado el 15 de 06 de 2019, de https://www.tp-link.com/ar/support/faq/500/
13. Vásquez, E. (2016). La seguridad de los endpoints, la fortaleza en su empresa. [Documento en línea] Disponible en: https://www.edgarvasquez.com/endpoints-seguridad-informatica/

References

1. Industrial Cybersecurity. (2020). https://www.cci-es.org/documents/10694/148873/Catalogo-serv-sol-CiberSeguridad+Industrial.pdf.
2. CISCO. (2015). https://www.cisco.com/c/dam/assets/global/pdfs/november-security/es/c45-654884-13_ise_aag_v2a_es-eu.pdf. Retrieved on June 16, 201, from https://www.cisco.com/c/dam/assets/global/pdfs/november-security/es/c45-654884-13_ise_aag_v2a_es-eu.pdf
3. Cruz, M. (2016). Administration of network security policies. CISCO ISE. [Online document] Available at: https://www.solutel.com/administracion-de-politicas-de-seguridad-cisco-ise/
4. Dordoigne, J. (2018). Computer Networks: Fundamental Notions. Seventh edition. Malaga, Spain: ENI Editions. Retrieved from https://www.abebooks.com/book-search/title/redes-informaticas-nociones-fundamentales/author/dordoigne/

5. GlobalwebIndex. (2016). GlobalWebIndex bi-annual report on the latest trends in online commerce. [Online document] Available at: http://cdn2.hubspot.net/hubfs/304927/GWI_Commerce__Q1_2016_Summary.p
6. González, A, Beltrán, D y Fuentes, E. (2016). Proposal of security protocols for the local wireless network of the Cienfuegos University. Universidad y Sociedad Magazine, 8 (4). [Online document] Available at: http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S2218-36202016000400017
7. http://www.internetworldstats.com/stats.htm
8. ITU (2015). International Telecommunication Union. Measuring the information society report 2015. [Online document] Available at: https://www.itu.int/en/ITU-D/Statistics/Documents/events/wtis2015/MISR2015_Magpantay.pdf
9. Méndez, W, Mosquera, D y Rivas, T. (2015). Vulnerability of WEP, WPA and WPA2 encryption protocols in wireless networks with Linux platform. Tecnura Magazine, 19, 79-87. [Online document] Available at: http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S0123-921X2015000500007
10. Partner, Ch. (2017). (Channel, Editor) [Online document] Available at: https://www.channelpartner.es/fabricantes/noticias/1102512001102/cisco-simplifica-esquema-de-certificados.1.html
11. ISMS (2019). Information Security Management System. ISO 27001. [Online document] Available at: http://www.iso27000.es/download/doc_sgsi_all.pdf
12. Tp Link. (2013). https://www.tp-link.com/ar/support/faq/500/. Retrieved on June 15, 2019, from https://www.tp-link.com/ar/support/faq/500/
13. Vásquez, E. (2016). The security of endpoints, the strength in your company. [Online document] Available at: https://www.edgarvasquez.com/endpoints-seguridad-informatica/

Referências

1. Cibersegurança industrial. (2020). https://www.cci-es.org/documents/10694/148873/Catalogo-serv-sol-CiberSeguridad+Industrial.pdf.
2. CISCO. (2015). https://www.cisco.com/c/dam/assets/global/pdfs/november-security/es/c45-654884-13_ise_aag_v2a_es-eu.pdf. Recuperado em 16 de junho de 201,

em https://www.cisco.com/c/dam/assets/global/pdfs/november-security/es/c45-654884-13_ise_aag_v2a_es-eu.pdf

3. Cruz, M. (2016). Administração de políticas de segurança de rede. CISCO ISE. [Documento online]. Disponível em: https://www.solutel.com/administracion-de-politicas-de-seguridad-cisco-ise/
4. Dordoigne, J. (2018). Redes de computadores: noções fundamentais. Sétima edição. Málaga, Espanha: Edições ENI. Recuperado em https://www.abebooks.com/book-search/title/redes-informaticas-nociones-fundamentales/author/dordoigne/
5. GlobalwebIndex. (2016). Relatório semestral da GlobalWebIndex sobre as últimas tendências do comércio on-line. [Documento on-line] Disponível em: http://cdn2.hubspot.net/hubfs/304927/GWI_Commerce__Q1_2016_Summary.p
6. González, A, Beltrán, D. Fuentes, E. (2016). Proposta de protocolos de segurança para a rede local sem fio da Universidade de Cienfuegos. Revista Universidad y Sociedad, 8 (4). [Documento online]. Disponível em: http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S2218-36202016000400017
7. http://www.internetworldstats.com/stats.htm
8. UIT (2015). União Internacional de Telecomunicações. Medindo o relatório da sociedade da informação de 2015. [Documento online]. Disponível em: https://www.itu.int/en/ITU-D/Statistics/Documents/events/wtis2015/MISR2015_Magpantay.pdf
9. Méndez, W. Mosquera, D. Rivas, T. (2015). Vulnerabilidade dos protocolos de criptografia WEP, WPA e WPA2 em redes sem fio com a plataforma Linux. Revista Tecnura, 19, 79-87. [Documento online]. Disponível em: http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S0123-921X2015000500007
10. Partner, Ch. (2017). (Canal, Editor) [Documento online]. Disponível em: https://www.channelpartner.es/fabricantes/noticias/1102512001102/cisco-simplifica-esquema-de-certificados.1.html
11. ISMS (2019). Sistema de Gerenciamento de Segurança da Informação. ISO 27001. [Documento online]. Disponível em: http://www.iso27000.es/download/doc_sgsi_all.pdf
12. Link Tp. (2013). https://www.tp-link.com/ar/support/faq/500/. Recuperado em 15 de junho de 2019, de https://www.tp-link.com/ar/support/faq/500/

13. Vásquez, E. (2016). A segurança dos terminais, a força da sua empresa. [Documento online]. Disponível em: https://www.edgarvasquez.com/endpoints-seguridad-informatica/