Universidad Continental

FACULTAD DE INGENIERÍA

Escuela Académico Profesional de Ingeniería de Sistemas e Informática

Tesis

Propuesta de implementación de políticas de seguridad basado en CISCO ISE (identity services engine) en la red LAN de Caja Huancayo

Gabriel Gregorio Huaman Mauricio
Geanlee Ronald Rojas Marcelo
John Kennedy Rojas Marcelo

Para optar el Título Profesional de
Ingeniero de Sistemas e Informática

Lima, 2022

04-05-2023 TESIS ISE

INFORME DE ORIGINALIDAD

20%	19%	7%	6%
INDICE DE SIMILITUD	FUENTES DE INTERNET	PUBLICACIONES	TRABAJOS DEL ESTUDIANTE

FUENTES PRIMARIAS

1	repositorio.continental.edu.pe Fuente de Internet	1%
2	extranet.sbs.gob.pe Fuente de Internet	1%
3	repositorio.ucv.edu.pe Fuente de Internet	1%
4	inba.info Fuente de Internet	1%
5	www.coursehero.com Fuente de Internet	1%
6	www.htc-bol.com Fuente de Internet	1%
7	www.slideshare.net Fuente de Internet	1%
8	repositorio.espe.edu.ec Fuente de Internet	1%
9	librosnetworking.blogspot.com Fuente de Internet	1%

10	dspace.ups.edu.ec Fuente de Internet	<1 %
11	docplayer.es Fuente de Internet	<1 %
12	www.solutel.com Fuente de Internet	<1 %
13	marasauceda.blogspot.com Fuente de Internet	<1 %
14	repositorio.unapiquitos.edu.pe Fuente de Internet	<1 %
15	es.slideshare.net Fuente de Internet	<1 %
16	repositorio.upn.edu.pe Fuente de Internet	<1 %
17	repository.unab.edu.co Fuente de Internet	<1 %
18	Submitted to Escuela Politecnica Nacional Trabajo del estudiante	<1 %
19	www.scribd.com Fuente de Internet	<1 %
20	Submitted to Universidad San Ignacio de Loyola Trabajo del estudiante	<1 %
21	repositorio.uwiener.edu.pe	

	Fuente de Internet	<1 %
22	repositorio.udh.edu.pe Fuente de Internet	<1 %
23	www.unir.net Fuente de Internet	<1 %
24	repositorio.utp.edu.pe Fuente de Internet	<1 %
25	rraae.cedia.edu.ec Fuente de Internet	<1 %
26	www.cisco.com Fuente de Internet	<1 %
27	pt.scribd.com Fuente de Internet	<1 %
28	repositorio.bicu.edu.ni Fuente de Internet	<1 %
29	repositorio.unheval.edu.pe Fuente de Internet	<1 %
30	repositorio.uap.edu.pe Fuente de Internet	<1 %
31	1library.co Fuente de Internet	<1 %
32	Submitted to Universidad Tecnologica del Peru	<1 %

Trabajo del estudiante

33	www.ccn-cert.cni.es Fuente de Internet	<1 %
34	www.repositorio.usanpedro.edu.pe Fuente de Internet	<1 %
35	cifradoypoliticasdeseguridad.blogspot.com Fuente de Internet	<1 %
36	repositorio.uandina.edu.pe Fuente de Internet	<1 %
37	www.netinkst.com Fuente de Internet	<1 %
38	repositorio.uach.mx Fuente de Internet	<1 %
39	repositorio.unh.edu.pe Fuente de Internet	<1 %
40	www.dspace.espol.edu.ec Fuente de Internet	<1 %
41	Submitted to Universidad Andina Nestor Caceres Velasquez Trabajo del estudiante	<1 %
42	repositorio.unac.edu.pe Fuente de Internet	<1 %
43	fr.slideshare.net Fuente de Internet	<1 %

44	repositorio.uladech.edu.pe Fuente de Internet	<1 %
45	tic4eso20.blogspot.com Fuente de Internet	<1 %
46	documentop.com Fuente de Internet	<1 %
47	repositorio.udl.edu.pe Fuente de Internet	<1 %
48	robertoelectiva1.wordpress.com Fuente de Internet	<1 %
49	Submitted to Universidad Cesar Vallejo Trabajo del estudiante	<1 %
50	repositorio.ug.edu.ec Fuente de Internet	<1 %
51	www.femp.es Fuente de Internet	<1 %
52	Castillo Corona Dulce Mónica,Flores Loza Maribel. "Sistema de gestión de seguridad de la información para la Escuela Nacional Preparatoria No. 5 José Vasconcelos", TESIUNAM, 2008 Publicación	<1 %
53	repository.usta.edu.co Fuente de Internet	<1 %

54	vsip.info Fuente de Internet	<1 %
55	Submitted to Pontificia Universidad Catolica del Peru Trabajo del estudiante	<1 %
56	repositorio.unu.edu.pe Fuente de Internet	<1 %
57	repositorio.utn.edu.ec Fuente de Internet	<1 %
58	López Rosales Andrés Osvaldo,Romero Garcia Mario Alejandro. "Servicios outsourcing en seguridad informatica", TESIUNAM, 2007 Publicación	<1 %
59	institutojubones.edu.ec Fuente de Internet	<1 %
60	iscseguridad.blogspot.com Fuente de Internet	<1 %
61	repositorio.upeu.edu.pe Fuente de Internet	<1 %
62	kupdf.net Fuente de Internet	<1 %
63	Submitted to University of La Guajira Trabajo del estudiante	<1 %
64	docs.bvsalud.org Fuente de Internet	<1 %

65	dspace.unach.edu.ec Fuente de Internet	<1 %
66	fmc.axarnet.es Fuente de Internet	<1 %
67	prezi.com Fuente de Internet	<1 %
68	repositorio.uta.edu.ec Fuente de Internet	<1 %
69	support.microsoft.com Fuente de Internet	<1 %
70	tesis.ipn.mx Fuente de Internet	<1 %
71	Hidalgo Caballero Juan Carlos. "Una metodologia para la formulacion de politicas en seguridad informatica", TESIUNAM, 2004 Publicación	<1 %
72	www.acis.org.co Fuente de Internet	<1 %
73	Alvarado Hermida Moisés,Díaz Contreras Gibrán Toríz. "Actualización y difusión de las políticas de seguridad de cómputo de la Facultad de Ingeniería", TESIUNAM, 2011 Publicación	<1 %
74	repositorio.unesum.edu.ec Fuente de Internet	<1 %

75	www.buenastareas.com Fuente de Internet	<1 %
76	www.youtube.com Fuente de Internet	<1 %
77	Rendon Cataño José Uriel. "Diseño y desarrollo de una metodologia para la determinacion y el establecimiento de normas de seguridad informatica", TESIUNAM, 2004 Publicación	<1 %
78	Submitted to Universidad EAN Trabajo del estudiante	<1 %
79	reini.utcv.edu.mx Fuente de Internet	<1 %
80	repositorio.unap.edu.pe Fuente de Internet	<1 %
81	Submitted to Corporación Universitaria Minuto de Dios, UNIMINUTO Trabajo del estudiante	<1 %
82	González Robles Yuri Adrián,Martínez Olivares César Antonio. "Metodología para establecer un plan de seguridad de la información", TESIUNAM, 2008 Publicación	<1 %
83	Submitted to Universidad Internacional de la Rioja	<1 %

Trabajo del estudiante

84	Submitted to Universidad Nacional de Colombia Trabajo del estudiante	<1 %
85	repositoriodemo.continental.edu.pe Fuente de Internet	<1 %
86	repositoriosdigitales.mincyt.gob.ar Fuente de Internet	<1 %
87	vbn.aau.dk Fuente de Internet	<1 %
88	Lizarraga Toledo Gerardo. "Diseño y configuracion del sistema de comunicaciones para la transmision de datos del complejo petroquimico independencia", TESIUNAM, 1996 Publicación	<1 %
89	aleph.org.mx Fuente de Internet	<1 %
90	repositorio.escuelaing.edu.co Fuente de Internet	<1 %
91	repositorio.unp.edu.pe Fuente de Internet	<1 %
92	repositorio.unsaac.edu.pe Fuente de Internet	<1 %
93	www.jotmi.org Fuente de Internet	

		<1 %
94	www.pinterest.com Fuente de Internet	<1 %
95	Alvarez Chávez José Alfredo. "Fabricacion y caracterizacion de acopladores de fibra optica unimodo", TESIUNAM, 1994 Publicación	<1 %
96	Olmos Roa Cinthya Enetzy. "Control de acceso a red inalámbrica (WNAC) utilizando software libre y biometría", TESIUNAM, 2010 Publicación	<1 %
97	catalogo.ulacit.ac.cr Fuente de Internet	<1 %
98	de.slideshare.net Fuente de Internet	<1 %
99	doku.pub Fuente de Internet	<1 %
100	espanol.optimum.com Fuente de Internet	<1 %
101	repositorio.uncp.edu.pe Fuente de Internet	<1 %
102	repositorio.untels.edu.pe Fuente de Internet	<1 %
	worldwidescience.org	

103	Fuente de Internet	<1 %
104	www.osde.org.ar Fuente de Internet	<1 %
105	Alvaro Mena. "Framework to implement information security management systems: An asset to project management processes", 2018 37th International Conference of the Chilean Computer Science Society (SCCC), 2018 Publicación	<1 %
106	Baltazar Gálvez José Miguel,Campuzano Ramírez Juan Carlos. "Diseño e implementación de un esquema de seguridad perimetral para redes de datos. Caso práctico : Dirección General del Colegio de Ciencias y Humanidades", TESIUNAM, 2011 Publicación	<1 %
107	García Gachuz Daniel. "Análisis de riesgos en la gerencia de tecnologías de la información del Instituto Mexicano del Petróleo", TESIUNAM, 2007 Publicación	<1 %
108	aws.amazon.com Fuente de Internet	<1 %
109	doczz.com.br Fuente de Internet	<1 %

110	forum.huawei.com Fuente de Internet	<1 %
111	juandalmau.com Fuente de Internet	<1 %
112	portal.gasnatural.com Fuente de Internet	<1 %
113	profesores.elo.utfsm.cl Fuente de Internet	<1 %
114	repositorio.usil.edu.pe Fuente de Internet	<1 %
115	www.dspace.uce.edu.ec:8080 Fuente de Internet	<1 %
116	www.ecoportal.net Fuente de Internet	<1 %
117	www.opein.com Fuente de Internet	<1 %
118	www.otcolombia.com Fuente de Internet	<1 %
119	www.repositorio.upla.edu.pe Fuente de Internet	<1 %
120	www.researchgate.net Fuente de Internet	<1 %
121	Acosta Castillo Rubén,Pacheco Cámara Sergio Alfredo. "Seguridad informática en los sitios	<1 %

de café Internet en la Ciudad de México", TESIUNAM, 2009
Publicación

---

122 Barrera Saldaña Maria Elena. "Sistema de mensajeria, venta, envio y recepcion de paquetes a nivel nacional", TESIUNAM, 2001 <1 %
Publicación

---

123 González Castillo Ignacio David,Montes Medina Israel. "Manual de prácticas para la asignatura seguridad informática avanzada", TESIUNAM, 2014 <1 %
Publicación

---

124 Trejo Zamora Yenni. "Diseño e implementacion de la red inalambrica para el laboratorio de dispositivos logicos programables", TESIUNAM, 2005 <1 %
Publicación

---

125 Zendejas Gonzalez Luis Cesar. "Redes inalambricas wlan : aspectos basicos del IEEE 802.11b para la comunicacion de datos entre computadoras", TESIUNAM, 2005 <1 %
Publicación

---

126 docs.google.com <1 %
Fuente de Internet

---

127 issuu.com <1 %
Fuente de Internet

---

128 livrosdeamor.com.br

	Fuente de Internet	<1 %
129	moam.info Fuente de Internet	<1 %
130	patents.google.com Fuente de Internet	<1 %
131	proyectoa.com Fuente de Internet	<1 %
132	rd.udb.edu.sv:8080 Fuente de Internet	<1 %
133	renati.sunedu.gob.pe Fuente de Internet	<1 %
134	repositorio.uisrael.edu.ec Fuente de Internet	<1 %
135	repositorio.upsc.edu.pe Fuente de Internet	<1 %
136	repositorioinstitucional.buap.mx Fuente de Internet	<1 %
137	repository.ucc.edu.co Fuente de Internet	<1 %
138	tics-jimenez2.blogspot.com Fuente de Internet	<1 %
139	trafficamerican.com Fuente de Internet	<1 %

140	tuinformatika.wordpress.com Fuente de Internet	<1 %
141	upc.aws.openrepository.com Fuente de Internet	<1 %
142	virtual.urbe.edu Fuente de Internet	<1 %
143	www.clubensayos.com Fuente de Internet	<1 %
144	www.consecri.com.ar Fuente de Internet	<1 %
145	www.gub.uy Fuente de Internet	<1 %
146	www.linksys.com Fuente de Internet	<1 %
147	www.questionpro.com Fuente de Internet	<1 %
148	www.tdx.cat Fuente de Internet	<1 %
149	www.unipiloto.edu.co Fuente de Internet	<1 %
150	zombiecerebros.blogspot.com Fuente de Internet	<1 %
151	Aguilar Lara Héctor Leonardo,González Cruz Israel,Solís Santana David Octavio,Huizar	<1 %

Sánchez Xiuhnel,Arvizu Barbosa Leticia. "Sistema de seguridad en alta disponibilidad para una red corporativa de datos y servicios", TESIUNAM, 2004
Publicación

152	Campos Valdovinos Yesenia. "Administración de riesgos en las tecnologías de información", TESIUNAM, 2010 Publicación	<1 %
153	Submitted to Keiser University Trabajo del estudiante	<1 %
154	Marquez Orozco Carlos Alberto. "Monitoreo de los servicios de internet para el aseguramiento de la calidad", TESIUNAM, 2004 Publicación	<1 %
155	bibliotecadigital.udea.edu.co Fuente de Internet	<1 %
156	es.unionpedia.org Fuente de Internet	<1 %
157	idoc.pub Fuente de Internet	<1 %
158	yessiksit.blogspot.com Fuente de Internet	<1 %
159	Monroy Suárez Diego. "Praxis de la seguridad informática", TESIUNAM, 2011 Publicación	<1 %

Dedicatoria

Esta investigación está dedicada a todos y a cada uno de los profesionales que nos apoyaron en este largo camino recorrido. A nuestros maestros, amigos y colegas de estudios. A nuestras familias por ser el pilar fundamental en todo lo que somos, en toda nuestra educación, tanto académica como en nuestra vida cotidiana, por su apoyo absoluto a través del tiempo.

Agradecimientos

A Dios por bendecir cada instante de nuestras vidas y por permitirnos hacer realidad nuestros sueños.

A la UNIVERSIDAD CONTINENTAL por brindarnos la oportunidad de estudiar y prepararnos para ser profesionales. Al Ing. Giancarlo Condori Torres por su apoyo y dedicación, quien, con sus conocimientos y motivación, ayudó en la culminación del proyecto de tesis. Agradecemos a todos los docentes por sus aportes a lo largo de nuestra carrera profesional.

Finalmente, agradecemos a nuestras familias por ser el principal motor de nuestros sueños; gracias porque siempre confiaron y creyeron en nosotros.

Índice de Contenidos

Pág.

Índice de Tablas

Índice de Figuras

Resumen

Con el crecimiento tecnológico las entidades públicas y privadas de los diferentes rubros dependen mucho de cómo se encuentra implementada la infraestructura tecnológica, principalmente la informática, ya que dicha implementación es importante para tener un buen manejo y cuidado de la información relevante para la entidad; vale decir, para lograr la seguridad de la información de todas las áreas de la entidad.

Este proyecto lleva por título *Propuesta de implementación de políticas de seguridad basado en CISCO ISE (Identity Services Engine) en la red Lan de Caja Huancayo* y tiene como objetivo elaborar una propuesta de Implementación de CISCO ISE en la infraestructura tecnológica de la CMAC HUANCAYO S.A, con la finalidad de optimizar la seguridad por intermedio de políticas de seguridad aplicadas a la red interna de la Caja Huancayo.

La investigación es pre experimental, explicativa y cuantitativa. La población estuvo conformada por los 30 departamentos en que opera Caja Huancayo distribuidos a nivel nacional existentes al cierre del año 2021. La muestra fue seleccionada de forma no probabilística e intencionada, y estuvo conformada por los departamentos de Marketing e Infraestructura Tecnológica de la agencia principal de Caja Huancayo. Asimismo, la tecnología de seguridad a utilizar se decidirá mediante la encuesta a 10 expertos de seguridad informática que laboran en empresas establecidas en Lima. Como resultado se obtuvo que la tecnología de seguridad CISCO ISE consiguió la prioridad más alta en siete aspectos y prioridad media en dos aspectos. Debido a ello CISCO ISE debería utilizarse para la propuesta.

Teniendo en cuenta que inicialmente Caja Huancayo no cuenta con una correcta configuración de los *swiches* y con una plataforma centralizada, este problema se solucionó mediante las pruebas piloto en los departamentos de Marketing e Infraestructura Tecnológica de la agencia principal de Caja Huancayo. Se llegó a la conclusión que la tecnología Cisco ISE optimizaría la seguridad interna en la agencia principal de Caja Huancayo, de esta manera se logró elaborar la propuesta de Implementación de políticas de seguridad para la Red LAN de Caja Huancayo basado en Cisco ISE (Identity Services Engine).

Palabras clave: Cisco ISE, seguridad, implementación, informática, optimización, configuración, propuesta, pruebas.

Abstract

With the technological growth of public and private entities in different areas, it depends a lot on how the technological infrastructure is implemented, mainly information technology, since said implementation is important to have a good management and care of relevant information for the entity, that is, to achieve information security in all areas of the entity.

This project is entitled *Security policy implementation proposal based on CISCO ISE (Identity Services Engine) in the Caja Huancayo Lan Network* and its objective is to prepare a CISCO ISE Implementation proposal in the technological infrastructure of CMAC HUANCAYO S.A., with the purpose of optimizing security through security policies, applied in the internal network of Caja Huancayo.

The research is pre-experimental, explanatory and quantitative, the population was made up of the 30 departments distributed nationwide of Caja Huancayo, existing at the end of 2021, the sample was selected in a non-probabilistic and intentional way, which were the departments of Marketing and Technological Infrastructure of the main agency of Caja Huancayo, and the security technology to be used will be decided, through the survey of 10 information security experts who work in companies established in the city of Lima, which turned out that the security technology CISCO ISE, acquired the highest priority in 7 aspects and medium priority in 2 aspects, therefore CISCO ISE should be used for the proposal.

Taking into account that initially Caja Huancayo does not have a correct configuration of the switches and in addition to not having a centralized platform, this problem was solved through pilot tests in the Marketing and Technological Infrastructure departments of the Caja Huancayo main agency, through Cisco ISE technology, due to this, it was concluded that Cisco ISE technology will optimize internal security in the main agency of Caja Huancayo, in this way the proposal for the Implementation of security policies for the Network was elaborated Caja Huancayo LAN, based on Cisco ISE (Identity Services Engine).

Keywords: Cisco ISE, Security, implementation, computing, optimization, configuration, proposal, testing.

Introducción

En la actualidad, diferentes entidades financieras han sido atacadas por *hackers* informáticos o ataques cibernéticos, lo cual no será fácil evitarlo en el plazo más corto, sino que, por el contrario, muestra un serio problema que debe ser abordado; por tanto, las entidades financieras deben tomar medidas que eviten este tipo de ataques que afecta a la entidad bancaria. Se ha decidido, entonces, realizar un proyecto de implementación de políticas de Seguridad con Cisco ISE para la Caja Huancayo.

La presente investigación está dividida por los siguientes capítulos:

En el primer capítulo se describen los problemas que actualmente tiene la Caja Huancayo y por qué es necesario y conveniente la implementación de políticas de seguridad con Cisco ISE.

En el segundo capítulo se hace referencia a los antecedentes de algunos autores que describen implementaciones de seguridad en la red que realizaron para evitar ataques de *hackers* y ataques cibernéticos para proteger y mejorar la seguridad de las redes internas de las entidades.

En el tercer capítulo se elige la metodología que permitirá encontrar alternativas acerca de cómo se implementarán las políticas de seguridad con Cisco ISE.

Finalmente, en el cuarto capítulo se muestran los resultados obtenidos para fortalecer la seguridad de la red interna de Caja Huancayo para la solución de los problemas planteados y las acciones para la implementación de Cisco ISE.

Capítulo I: Planteamiento del estudio

1.1. Planteamiento y formulación del problema

1.1.1. Planteamiento del problema

Con el crecimiento tecnológico las entidades públicas y privadas de los diferentes rubros dependen mucho de cómo se encuentra implementada la infraestructura tecnológica, principalmente la informática, ya que dicha implementación es importante para tener un buen manejo y cuidado de información relevante para la entidad; vale decir, para lograr la seguridad de la información de todas las áreas de la entidad.

A nivel internacional, en Arizona, Trellix observó un aumento en las detecciones de correo electrónico malicioso que alcanzó su punto máximo alrededor de las elecciones primarias del 2 de agosto en el estado del Gran Cañón. Subieron un 78 %, de 617 en el primer trimestre de 2022 a 1101 en el segundo trimestre. Volvieron a subir un 104 % a 2246 en el tercer trimestre. (1) Solo en lo relativo al primer semestre del 2022, América Latina y el Caribe ha registrado cerca de 140 mil millones de intentos de ciberataques. Si ello se compara con el mismo periodo del 2021, se está ante un incremento del 50 %, tal y como precisa FortiGuard Labs de Fortinet (2).

Respecto al Perú, los intentos de ciberataque constituyen 5.2 mil millones, que corresponde a un 10 % más en relación al primer semestre del 2021. (2)

A través del avance tecnológico existen mayores probabilidades de ataques en la red LAN, siendo el rubro de BANCA y FINANZAS el más afectado, ya que dichas entidades brindan numerosos servicios y son utilizados por los clientes. Considerando este punto, toda institución financiera tiene el deber de proteger y salvaguardar la información de sus clientes. (3)

A nivel regional, Caja Huancayo posee las siguientes vulnerabilidades: a nivel de los equipos *swiches*, estos tienen habilitados protocolos inseguros y, asimismo, no se cuenta con una plataforma centralizada para la administración; por consiguiente, a nivel de WLC, este no cuenta con una plataforma para la administración. Finalmente, a nivel de la vulnerabilidad Man in The Middle no cuenta con una correcta configuración en los equipos *swiches*. A partir de lo mencionado, en el caso que dichas vulnerabilidades no sean resueltas se podrían generar ataques internos en la red LAN de la Caja Huancayo, lo cual generaría perdidas a la institución y provocaría los siguientes riesgos:

- Comprometer información confidencial de los usuarios y colaboradores.
- Indisponibilidad de la Red Campus, afectando las actividades diarias de las distintas Unidades Orgánicas.

- Indisponibilidad de la Red DataCenter, donde se alojan todos los servidores de la Caja Huancayo, lugar de operación de los servicios que brinda a sus clientes.
- Riesgo reputacional que puede causar la pérdida de confianza en la Caja Huancayo, generando pérdida de clientes.

Para mitigar estas vulnerabilidades o riesgos se debería realizar una correcta configuración en los *swiches* de acceso, y para control centralizado se deberían implementar políticas de seguridad, pero antes de ello se debe realizar pruebas piloto a nivel reducido (en el área de Marketing y en el dpto. de Infraestructura Tecnológica de la oficina principal de la Caja Huancayo) y así evitar posibles fallos a nivel general. Si las pruebas son exitosas, se propondría una propuesta de implementación de políticas de seguridad a Caja Huancayo mediante una documentación que valide los hechos y, de esta manera, desplegarlo en toda la Oficina Principal de la Caja Huancayo.

Actualmente, existen diferentes vendedores como CISCO, FORTINET, HUAWEI, ARUBA, entre otros. Sin embargo, implementar una solución distinta podría generar cierta incompatibilidad con la arquitectura actual, debido a que la arquitectura Campus y Data Center de la Caja Huancayo está basada en la tecnología de CISCO, por lo que fue conveniente mantener la marca para la ejecución de la propuesta de implementación con CISCO ISE. Así mismo, se debe indicar que la Caja Huancayo cuenta con un *memorándum* de estandarización de marca CISC para adquirir cualquier solución en beneficio de la institución (ver Anexo 10).

"Caja Huancayo actualmente es supervisada por la Superintendencia de Banca, Seguros y AFP, de acuerdo a la resolución establecida N.° 504-2021 en el Articulo 8, Responsabilidades de la Seguridad de la Información y Ciberseguridad" (4). Se tiene que crear un sistema que pueda autenticar todo el proceso y asegurar el control de los accesos a la información, los propios sistemas y los servicios que proporciona, en atención a dicha responsabilidad. La Caja Huancayo está obligada en implementar dichos procesos de autenticación, por lo que se planteó la *Propuesta de implementación de políticas de seguridad basado en CISCO ISE.* Esta propuesta de implementación para el despliegue de CISCO ISE únicamente será con los colaboradores de la Oficina Principal. Para estudiar el comportamiento y funcionamiento únicamente se empezará con el área de Marketing y el Dpto. de Infraestructura Tecnológica. Luego de obtener los resultados, se procederá con el despliegue general en toda la Oficina Principal. Con la propuesta de implementación estaríamos fortaleciendo aún más la seguridad en la Red LAN de la Caja Huancayo; sin embargo, los pantallazos son solo una muestra que valida el funcionamiento del CISCO ISE.

1.1.2. Formulación del problema

La implementación de Cisco ISE permite a las empresas "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 o VPN" (5). Ello proporcionó la oportunidad de investigar acerca de las bondades que tiene el controlador de políticas de seguridad de CISCO-Cisco ISE, para la propuesta de implementación de Políticas de Seguridad en la Red LAN de la agencia principal de Caja Huancayo. En ese sentido, el problema objeto de estudio se formuló en los términos que prosiguen, para ello se debe tener en cuenta que las pruebas piloto serán realizadas en los departamentos de Marketing e Infraestructura Tecnológica de la oficina principal de la Caja Huancayo, para lograr la validez de la implementación y así desplegarla en toda la oficina principal.

1.1.2.1. Problema general. ¿De qué manera, basándose en Cisco ISE (Identity Services Engine), se pueden implementar las pruebas de políticas de seguridad en los departamentos de Marketing e Infraestructura Tecnológica de la oficina principal de la Caja Huancayo, para lograr optimizar la seguridad de la Red LAN de Caja Huancayo?

1.1.2.2. Problemas específicos. ¿Cuáles son las políticas de seguridad informática actualmente operativas en la agencia principal de Caja Huancayo y qué vulnerabilidades poseen?

¿Qué políticas de seguridad para ataques internos (intencionados o inocentes), basado en Cisco ISE, se pueden implementar en la Red LAN para las pruebas en los departamentos de Marketing e Infraestructura Tecnológica de la oficina principal de Caja Huancayo?

1.2. Objetivos

1.2.1 Objetivo general

Elaborar una propuesta de implementación de políticas de seguridad para la Red LAN de Caja Huancayo, basado en la tecnología informática Cisco ISE (Identity Services Engine).

1.2.2. Objetivos específicos

Determinar las vulnerabilidades de las políticas de seguridad para mitigar ataques internos en la Red LAN en la agencia principal de Caja Huancayo.

Determinar las políticas de seguridad para ataques internos (intencionados o inocentes) basado en Cisco ISE que se pueden implementar en la Red LAN, para las pruebas en los departamentos de Marketing e Infraestructura tecnológica de la agencia principal de Caja Huancayo.

1.3. Justificación

La investigación se justifica metodológicamente porque acude al empleo de técnicas de investigación, como el cuestionario y su procesamiento para la validación y análisis de datos

concernientes a la seguridad de la Red LAN. Con ello se pretende conocer que la seguridad en la Red LAN, mediante el uso de tecnologías de seguridad, son más eficientes.

La investigación se justifica en la práctica porque, de acuerdo los objetivos, estos permiten encontrar soluciones a los problemas de seguridad en la Red LAN, mediante una correcta configuración de los componentes, previo a un análisis correspondiente.

La investigación se justifica teóricamente, ya que la aplicación de la teoría y los conocimientos sobre la tecnología de seguridad Cisco ISE (Identity Services Engine) ayudarán a corregir las vulnerabilidades internas en la Red LAN.

En cuanto a la justificación operativa, la propuesta de implementación de políticas de seguridad basado en la tecnología de seguridad Cisco ISE (Identity Services Engine) permitirá realizar sus procesos en la Red LAN de forma rápida y segura.

Esta investigación se justifica tecnológicamente porque la propuesta de implementación de políticas de seguridad basado en la tecnología de seguridad Cisco ISE (Identity Services Engine) permitirá contar con una sofisticada tecnología en la autentificación, gestión y administración, lo cual solucionará las vulnerabilidades internas en la Red LAN.

Finalmente, como justificación institucional, la propuesta de implementación de políticas de seguridad basado en la tecnología de seguridad Cisco ISE (Identity Services Engine) requiere ser ejecutada para mejorar la Red LAN mediante el uso de nuevas medidas de autentificación, gestión y administración centralizada.

1.4. Hipótesis y descripción de variables

1.4.1. Hipótesis general

Las pruebas de implementación de políticas de seguridad, basado en la tecnología informática Cisco ISE (Identity Services Engine), optimizarán la seguridad en la Red LAN en los departamentos de Marketing e Infraestructura tecnológica de la agencia principal de Caja Huancayo.

1.4.2. Hipótesis específicas

Se logrará determinar las vulnerabilidades existentes en la Red LAN en los departamentos de Marketing e Infraestructura tecnológica de la agencia principal de Caja Huancayo.

Se logrará determinar las políticas de seguridad a implementar en los departamentos de Marketing e Infraestructura tecnológica de la agencia principal de Caja Huancayo.

Mediante las pruebas de implementación de políticas de seguridad para ataques internos (Intencionados o Inocentes) basado en Cisco ISE, se logrará optimizar las vulnerabilidades internas en la Red LAN en los departamentos de Marketing e Infraestructura tecnológica de la agencia principal de Caja Huancayo.

1.4.3. Matriz operacional de variables

Tabla 1

Matriz operacional de variables

Variables	Dimensiones	Indicadores	Medición
Variable Independiente: Implementación de políticas de seguridad basado en Cisco ISE a través de sus vulnerabilidades en la Red LAN.	Vulnerabilidad de la política de seguridad para mitigar ataques internos.	15 equipos *switches* vulnerables en la agencia principal.	Ordinal
		Nivel de criticidad media en el equipo Wireless LAN Controller,	
		Ocho equipos *switches* vulnerables al ataque Man in The Middle en el servidor DHCP.	
		Siete equipos *switches* vulnerables en el control de acceso (PORT-SECURITY)	
Variable Dependiente: Optimizar la seguridad en la Red LAN mediante la tecnología de seguridad Cisco ISE.	Políticas de seguridad para ataques internos (intencionados o inocentes)	Nivel de protección alta para el control de acceso a la red a los distintos dispositivos finales.	
		Nivel de protección alta para gestión y administración centralizada a través de los protocolos (TACACS+ y RADIUS).	
		Nivel de protección alta para obtener visibilidad de los dispositivos que se conecten a la red interna de los diferentes sistemas operativos (Microsoft Windows, Mac OS, Linux).	
		Nivel de protección alta en el acceso del usuario, para la visibilidad del medio de conexión, tiempo y tipo de acceso que utilizan los dispositivos para conectarse a la red LAN (Cable, Wireless, VPN).	

Nota. Elaboración propia.

Capítulo II: Marco teórico

2.1. Antecedentes de investigación

2.1.1. Antecedentes internacionales

El Ministerio de Defensa de España (2021) presenta una Guía de Seguridad de las TIC en la cual establece un procedimiento de empleo seguro para Cisco ISE. Sostiene una instalación segura desde la obtención hasta la operación del producto, con el fin de evitar posibles problemas de seguridad derivados de la presencia de malware y/o técnicas de manipulación (*Tampering*). Debido a ello, se propuso como objetivo recoger el procedimiento de empleo seguro del software Cisco ISE 2.6. Para llevarlo a cabo, se realizó el análisis de los dispositivos (físicos o virtuales) donde se despliega el producto, para una instalación correcta según el hardware y distribución; por consiguiente, se realizó la instalación en tres partes fundamentales, las cuales fueron: fase de despliegue e instalación física (por el cual se verificó la manipulación del producto); fase de configuración (lugar donde se ajustó la seguridad del producto, tales como: protocolos de red y criptografía, auditoría, autentificación, bloqueos de usuarios y VPN); y fase de operación y mantenimiento (por el cual se verificó el entorno operacional y su mantenimiento respectivo para garantizar el rendimiento eficaz del producto). En conclusión, Cisco ISE recoge procedimientos seguros de instalación, configuración y operación y mantenimiento para control de acceso de red unificada, y así mitigar posibles problemas de seguridad derivados de la presencia de malware y/o técnicas de manipulación (Tampering). (6)

Aporte: A través del presente antecedente se pudo contar con previo conocimiento de la usabilidad y las funciones de la plataforma de CISCO ISE.

En una investigación en el Ecuador, a partir de la cual se aplicaron Políticas de Seguridad Informática con ISO/IEC 27002, Guerrero (2017) afirma que la seguridad informática no es incluida en el departamento de sistemas como parte de un programa de seguridad que permita establecer procedimientos y responsabilidades, sistemas de control, sistema de acceso, entre otros.

Por tanto, el autor se trazó el objetivo de implementar dicho sistema, a fin de alcanzar niveles apropiados de integridad, confidencialidad y disponibilidad de la información en el departamento de Sistemas. Para dicho objetivo se llevó a cabo un análisis que diagnostique la realidad del departamento de sistemas, a partir de encuestas y de la recopilación de información y estadísticas sobre los incidentes. Ello derivó en un análisis de los controles seleccionados teniendo en consideración la norma, además de la medición del riesgo a través de la metodología seleccionada. Como punto último se tuvo el diseño de la política.

Se concluyó con el análisis y la implementación de tal propuesta considerando la recomendación del ISO/IEC 27002:2013, además de difundir dichos conocimientos a los trabajadores de dicho departamento para que tomen conciencia y desarrollen una cultura de seguridad. Así, se expusieron los objetivos de la política y sus beneficios en pro de la realización de las actividades de forma segura. (7)

Aporte: A través del presente antecedente se obtuvo conocimiento del estándar ISO/IEC 27002, que establece buenas prácticas para la seguridad de la información.

También en el marco de la ciberseguridad en empresas de Ecuador, Zurita (2017) se propuso mejorar o proponer alternativas de solución de control de acceso, remediación, *profiling* y servicio AAA para la red de información del Ministerio de Finanzas de dicho país, ello en concordancia con lo dispuesto por el acuerdo No. 66 del Esquema de Gestión Gubernamental de la Información. Como dicho ministerio está a cargo de gestionar, controlar y asegurar la información y la red de datos de las finanzas públicas de Ecuador, debe mejorar su sistema de protección, para lo cual ha adquirió la red Cisco ISE; sin embargo, no han sabido aprovechar sus beneficios.

Para llevar a cabo el estudio, se tuvo como objetivo el fortalecimiento de la seguridad informática del Ministerio de Finanzas, mejorando la "Solución actual de Control de Acceso, Remediación, Profiling y Servicio AAA para la red de datos institucional", con el objetivo de aprovechar la tecnología para incrementar los niveles de seguridad. Para lograrlo, se reunió información acerca de lo que acontece en la red, así como información de los dispositivos que acceden y sus usuarios. Con ello, se pretende orientar a los responsables de la seguridad informática a decidir sobre la base de las políticas implementadas.

Se concluyó que, a través de la "Solución actual de Control de Acceso, Remediación, Profiling y Servicio AAA del Ministerio de Finanzas", se fortaleció la seguridad informática de dicho ministerio. Y, por último, se puede decir que ahora se ofrece un mejor servicio tecnológico-institucional, con altos niveles de seguridad y en estricto cumplimiento de dichas políticas. (8)

Aporte: A través del presente antecedente se pudo profundizar conocimientos acerca del control de acceso a la red, profiling y servicios AAA, y el soporte y garantía por parte del fabricante.

Bermúdez y Bailón (2015), en su tesis desarrollada en el contexto ecuatoriano, analizaron las potencialidades de la norma ISO/IEC 27001 en lo relativo a la seguridad informática y de la información. En dicha investigación se toma como punto de referencia a Credigestion, una empresa cuya gestión de crédito y cobranza de cartera se encentra en proceso crítico pese a que sostiene aún sus operaciones. Dicha empresa, de mediana escala en el rubro

financiero, se vio obligada a mejorar su sistema de seguridad de la información, a fin de evitar que esta sea manipulada.

Dicha realidad se agrava si se tiene en cuenta que la empresa no tiene un área especializada en seguridad informática, razón por la que dichos problemas no han sido abordados. Por ello, se decidió aplicar la norma ISO/IEC 27001 a partir de la cual se observarán los procesos críticos de la empresa en lo relativo a la gestión de seguridad que garantice la integridad, confidencialidad y seguridad correspondientes.

Para llevarse a cabo, la muestra asignada fue de 230 empleados del departamento de Credigestión, y, a partir de ello, se obtuvo una muestra de 23 funcionarios mediante muestreo intencional; por consiguiente, para la recolección de información se utilizaron los siguientes mecanismos: encuestas, entrevistas, consultas, reuniones, observación y revisión de documentación; y para el análisis o tratamiento se utilizó Microsoft Excel, el cual permite clasificar, verificar y contrastar las variables de investigación. Se concluye que, producto de la falta de un sistema de seguridad de la información, los activos de información las áreas en situación crítica y, en general, la seguridad de la empresa, proyectan índices de riesgo. Asimismo, existe un peligro real en cuanto a la manipulación, el daño o el robo de la información, y es potencialmente lesivo a los intereses de la empresa. (9)

Aporte: A través del presente antecedente se obtuvo información del estándar internacional ISO/IEC 27001, que establece el aseguramiento, la confidencialidad e integridad de los datos y la información.

Jiménez y Urban (2015), en su tesis desarrollada en el contexto mexicano, realizaron una *Migración de Servicios Cisco NAC a Cisco ISE* en la red de una dependencia de gobierno. La investigación nace a partir de la observación de una realidad atípica, eso es, que la dependencia del Gobierno tenía, en su red de invitados y en su red empresarial 3000 y 800 usuarios, respectivamente.

Para implementar la solución CISCO ISE, primero tuvieron que llevar a cabo la documentación e impulsar la migración de los servicios administrados en la red. Ello requirió que el fabricante cesé el soporte técnico de NAC y actualice sus servicios y equipos. Respecto a los servicios de internet, estos debían tener una mejor administración y control del ancho de banda.

Se concluye que dicha migración y todo lo que implicó tuvo un final exitoso, pues se estableció un control más granular de la infraestructura inalámbrica, con lo cual se vita que usuarios extraños puedan acceder a la red y asegura, al mismo tiempo, una mejor visibilidad de los usuarios y dispositivos que acceden. (10)

Aporte: A través del presente antecedente se obtuvo información acerca de la migración de servicio.

Ramírez (2016) realizó una tesis cuyo objeto de estudio tiene como eje central la plataforma de CISCO-CNAC, pues se propone una guía metodológica para llevar a cabo una serie de políticas orientadas al control de acceso. La tesis principal del autor es la fragilidad de las infraestructuras de red hoy en las empresas, con problemas como los robos de información, entre otros.

Las redes que se utilizan hoy en las organizaciones, afirma, deben asegurar la seguridad en la conexión inalámbrica y no inalámbrica a partir de software y hardware especializados, ello teniendo en cuenta criterios como el almacenamiento y la recuperación de la información. El estudio se llevó a cabo en la Universidad Autónoma de Bucaramanga.

Dicha implementación se realizó a la luz de etapas yuxtapuestas y sistemáticas: se ideó productos entregables que fueron el resultado de objetivos claros; los productos que resulten de la primera etapa, pasarán a la segunda y luego a la tercera. Se concluye que, con dicha implementación, las organizaciones pueden prevenirse de amenazas como virus, spyware y gusanos que quieran acceder a la red corporativa y a los dispositivos. (11)

Aporte: A través del presente antecedente se obtuvo información sobre una guía metodológica de implementación a través de la plataforma CISCO – CNAC para protegerse de las amenazas.

2.1.2. Antecedentes nacionales

Benites (2019) realizó un trabajo orientado a la implementación de un Sistema de Gestión de Seguridad de la Información-Norma ISO 27001 para la Fábrica Radiadores Fortaleza.

Hoy lo que amenaza a las organizaciones es, según Benites, la proliferación d malware producto de negligencias en el uso e implementación de software que se dediquen a eliminarlos.

Por tanto, la seguridad de la información es urgente en las organizaciones. A partir de esta realidad, el objetivo fue implementar un Sistema de Gestión de Seguridad de la información en la Oficina de Proyectos que se encuentra dentro de un área de la fábrica Radiadores Fortaleza.

Para llevar a cabo la investigación exitosamente, se recopiló información necesaria, así como datos estadísticos que permitan ver un panorama más amplio. Se concluye que dicha implementación precisa de gran dedicación y esfuerzo por parte de la Fábrica de Radiadores Fortaleza, desde los colaboradores hasta los puestos de jerarquía. (12)

Aporte: El siguiente antecedente aportó para tomar conocimiento del plan y gestión de la seguridad de la información de una empresa nacional.

En una investigación llevada a cabo con los trabajadores de la DIGERE del Ministerio de Educación del Perú (MINEDU), Calderón (2019) se propuso analizar la gestión de riesgos y la seguridad de la información. Dicha problemática también ataca a las empresas públicas,

razón por la cual han empezado a trabajar en sus sistemas de información y en la gestión de riesgos, incorporando medidas que velen por la información digital y física. El estudio lleva a cabo el análisis acerca de cómo impacta la seguridad de la información en la gestión. Se recopilaron datos y se utilizó el programa SPSS. Se concluye que la seguridad de la información y la gestión de riesgos tienen una relación directa. (13)

Aporte: El siguiente antecedente aportó información acerca de la seguridad de la información y gestión de riesgos en los trabajadores.

Para perfeccionar el proceso de acceso remoto en una empresa financiera, Romero (2018) propuso, mediante su investigación, un modelo de seguridad informática. Dicha entidad financiera presenta diferentes debilidades en cuanto a sus procesos de conexión de su red interna, todo lo cual redunda en una mayor inestabilidad de su seguridad informática. Los trabajadores, cuando trabajan remotamente, precisan del servicio de Virtual Private Network (VPN) para acceder a los servicios informáticos

Partiendo de esta realidad, lo que el autor plantea es una alternativa tecnológica orientada a la seguridad informática que mejore el acceso remoto de la empresa. Se emplearon encuestas con un enfoque cuantitativo y el programa de análisis de datos SPSS. Se concluyó que la propuesta mejora la seguridad informática y ello redunda en un fortalecimiento de la transmisión y autenticación de datos, reduciendo los niveles de riesgo de dicho proceso. (14)

Aporte: El siguiente antecedente brindó información sobre protocolos seguros para la autenticación.

A partir de un diseño utilizando el Identity Services Engine (ISE), López (2017) se propuso analizar cómo dicho servicio puede ayudar a eliminar accesos no autorizados a la red corporativa. Dicha investigación surge teniendo como panorama el rápido crecimiento de las organizaciones y sus amplias redes geográficas, cuyas oficinas y centros de trabajo necesitan de un control de sus redes internas. Por intermedio de un sistema de seguridad, el autor se propuso mitigar accesos no autorizados a la red cableada de la empresa objeto de estudio.

Para lograr el objetivo, se propuso una investigación cualitativa de tipo descriptiva. Se usó la metodología PPDIOO de Cisco, que consiste en preparar, planear, diseñar, implementar, operar y optimizar para su simulación respectiva, y de esta manera mostrar la causa, el problema y el efecto de un riesgo, y con base en ello implementar medidas, tales como: mitigar amenazas, proteger y asegurar los datos y la información. En conclusión, se podrá atenuar los riesgos de accesos extraños o no autorizados mediante una simulación con ISE, siempre y cuando se asegure el acceso solamente a recursos necesarios y se autentifiquen los equipos. (15)

Aporte: El siguiente antecedente sirvió de guía para la propuesta de implementación de CISCO ISE, brindando seguridad y protección.

2.2. Bases teóricas

2.2.1. Redes de Área Local (LAN)

Las redes de área local (*Local Area Network* – LAN por sus siglas en inglés) son un conjunto de dispositivos electrónicos conectados entre sí que están sujetos a control informático de los datos que se transmiten a través de la arquitectura electrónica conformada por la configuración de dichos dispositivos; y que comparten una línea de comunicación común o un enlace inalámbrico con un servidor u ordenador central encargado del procesamiento de la información. En una Red de Área Local - Red LAN convergen varias tecnologías, siendo las más preponderantes la electrónica, para el diseño de la parte física, y la informática, para la transmisión de datos. Como consecuencia de ello, se tiene que en situaciones que se requiera comunicación común entre dispositivos y un ordenador central o servidor, la implementación de una Red LAN se constituye en una de las mejores opciones a adoptar como solución.

Las Redes de Área Local – LAN constituyen las configuraciones de redes de mayor adaptabilidad a prestaciones a menor escala, en redes de área reducidas o no tan amplias. Así, las LAN:

> Son redes ubicadas en un área restringida, cuya propiedad es privada; pueden estar situadas en una oficina o en el edificio de la empresa. Las hogareñas también se consideran LAN siempre y cuando tengan, al menos, dos computadoras. Para que una PC pueda tener acceso a la red, debe poseer una tarjeta de red (NIC). Los componentes de una LAN pueden ser: computadoras, servidores e impresoras, entre otros. Los medios utilizados para conectarlas son los cables y/o el aire (el más común es el sistema WiFi, a través de un access point), y los dispositivos de enlace (networking): switch, router. […] La infraestructura varía según el tamaño del área por cubrir, la cantidad de usuarios que se pueden conectar, y el número y los tipos de servicios disponibles. (16 p.15).

Las Redes de Área Local – LAN presentan características propias que se deben tener en cuenta cuando se analizan las mismas, con el fin de abordar problemáticas referidas a cualquiera de los aspectos de dichas redes. En la Tabla 1 se detallan algunas de dichas características clave de las LAN:

Tabla 2

Características de LAN

PARÁMETRO CARACTERÍSTICO	DESCRIPCIÓN
Amplitud	Mejoran las comunicaciones internas al ser redes que, mediante tecnologías, logran compartir localmente archivos y hardware eficientemente.
Pertenencia de la Red	Redes que pertenecen a un hogar, una oficina o una empresa pequeña Son redes privadas.
Uso de la Red	Permite la conexión entre computadoras personales, lo cual facilita el intercambio de información y recursos.
Restricciones de la Red	El tamaño es una de las restricciones.
Uso de Tecnologías	Se elige Ethernet (broadcast) a partir de un UTP, un cable simple, con el que los equipos se conectan a un switch.

Nota. Adaptado de "BENCHIMOL", por Daniel, Redes Cisco, p.16.

Por otro lado, para efectos de cubrir las necesidades de los usuarios, es fundamental tener en cuenta que "hay que prestar atención a la convergencia de múltiples servicios, a la mayor movilidad de los usuarios, al aumento en las velocidades de conexión y a un mayor número de parámetros de seguridad ante nuevos peligros emergentes" (16 p.17). Complementando dicha información, en la Tabla 2 se detallan los requerimientos que tiene LAN, de acuerdo con la demanda y las necesidades cotidianas.

Tabla 3

Métodos de control de acceso basado en reglas.

MÉTODOS DE CONTROL	DESCRIPCIÓN
Escalabilidad	Debería absorber el crecimiento futuro de la red que se cree, una función que es importante, puesto que no en todos los casos una red se crea desde cero, sino que se realizan mejoras sobre las ya creadas.
Administración	La administración de las redes se debe realizar a través de aplicaciones o programas que identifiquen los problemas cotidianos, los analicen y brinden soluciones.
Costo-Beneficio	El costo beneficio debe ser una razón preponderante al momento de impulsar una red nueva realizar modificaciones.
Alta Disponibilidad	La operatividad debe ser una característica de la red, y para ello se debe contar con ambientes redundantes en las conexiones y en los equipos.
Servicios	El servicio de *Wireless* debe estar garantizado, al tiempo que soporta el movimiento de las distintas personas que acceden.

Nota. Adaptado de "BENCHIMOL", por Daniel. Redes Cisco, pp.16-17.

2.2.1.1. Diferencias entre LAN y otros tipos de redes. El concepto de LAN (*Local Area Network*) se inicia con el desarrollo del procesamiento distribuido, procesamiento que tiene que ver con la interconexión de dos o más computadoras idénticas punto a punto. Una vez que se reparó en los beneficios y ventajas que ofrecía el procesamiento distribuido, las redes de computadoras se desarrollaron rápidamente a tal punto que, principalmente, con el auge de las computadoras personales, surgió entre los usuarios de programas de aplicación la necesidad de compartir programas, compartir archivos (files), compartir periféricos (impresoras) y compartir memoria de masa o almacenadores (discos duros). (17 p.116)

Una Red de Área Local – LAN es un sistema de comunicación de datos que permite a un determinado número de dispositivos independientes comunicarse dentro de un área local, entendiéndose esta última como un espacio reducido capaz de circunscribirse a una casa, un departamento o un edificio. Las diferencias entre una red local y cualquier otro tipo de red son las siguientes: 1) las comunicaciones parten de una misma área geográfica que podría ser una universidad, un edificio o un almacén de trabajo; 2) tiene porcentajes de errores bajos, al tiempo que su velocidad es moderada y alta (1 a 100 Mbps); 3) la comunicación no requiere de ningún nodo de conmutación intermedio al emplear un medio físico común sobre enlace de punto a punto; 4) la opera una solo organización; 5) y hace posible la compatibilidad entre equipos de fabricantes distintos.

Dichas características son opuestas a las de las redes de área amplia (WAN), aquellas que posibilitan la interconexión de equipos de comunicación de diferentes empresas y de diferentes lugares, con lo que pueden ofrecer un servicio público. (17)

2.2.1.2. Aplicaciones de LAN. Las aplicaciones de las Redes de Área Local, o simplemente LAN por sus siglas en inglés, son múltiples, y es que tal como se señaló anteriormente, donde hay que interconectar dos o más computadoras para aprovechar las ventajas del procesamiento distribuido, las LAN encuentran su oportunidad. En ese respecto, las aplicaciones de las LAN responden a la necesidad de compartir programas, archivos, periféricos y memoria. En concordancia con lo expuesto, las aplicaciones de las LAN pueden aglutinarse en cuatro rubros funcionales.

Procesamiento de datos: Constituye el primer rubro funcional de las Redes de Área Local - LAN. En este rubro, LAN es utilizado en el procesamiento de transacciones, transferencia de archivos, etc. Básicamente, el procesamiento de datos tiene que ver con actividades relacionadas con el manejo de la información. La función realizada por las Redes de Área Local principalmente tiene que ver con:

- Trabajo en lotes, el cual considera un grupo de tareas enviadas a una instancia que permite su procesamiento automático. En dicha instancia, denominada *Application*

Object Server - AOS por sus siglas en inglés, los trabajos por lotes se ejecutan mediante las credenciales de seguridad del usuario que creó el trabajo.

- Entrada Remota de Trabajos, *Remote Job Entry – RJE* por sus siglas en inglés. RJE es el procedimiento para enviar solicitudes de tareas de procesamiento de datos no interactivas a un ordenador central (*mainframe computer*) desde estaciones de trabajo remotas; luego, si se remonta a cada una de las estaciones de trabajo, RJE también tiene que ver con el proceso de recibir la salida de dichos trabajos desde el ordenador central en cada una de las estaciones de trabajo remotas.

Automatización de oficinas: La automatización de oficinas constituye el segundo rubro funcional de las Redes de Área Local - LAN. En este rubro, LAN es utilizado para el procesamiento de palabras y documentos, es decir, para la distribución, recepción, organización y almacenamiento de documentos electrónicos; por ejemplo, recibir, enviar, almacenar y/o distribuir correos electrónicos, organizar documentos recibidos, enviados o rechazados.

Automatización de fábricas: La automatización de fábricas constituye el tercer rubro funcional de las Redes de Área Local - LAN. En este rubro, LAN suele ser utilizado en la monitorización de los equipos de planta, en el control de los procesos de Diseño Asistido por Computadora (*Computer Aided Design* - CAD por sus siglas en inglés) y en el control de los procesos de fabricación asistida por computadora (*Computer Aided Manufacturing* – CAM por sus siglas en inglés, CAM).

Administración de energía: Constituye el cuarto rubro funcional de las Redes de Área Local - LAN. En este rubro, LAN es utilizado en el control de los procesos de administración de la energía demandada por la entidad en la que está inmersa LAN; por ejemplo, control de la energía administrada tanto para el funcionamiento del aire acondicionado como para la regulación de los niveles de ventilación.

Por otro lado, se destaca que la topología puede entenderse como un plano de la red, o un mapa de todos los elementos implicados en la configuración de la misma; luego, en un contexto de aplicaciones de LAN referenciadas a los cuatro rubros funcionales descritos en los párrafos precedentes (procesamiento de datos, automatización de oficinas, automatización de fábricas y administración de energía). La presente investigación se desarrolló en el contexto del primer rubro funcional, vale decir, en el contexto de la aplicación de las LAN para el procesamiento de datos.

2.2.1.3. Topologías de LAN. Una topología de red se define como la serie de lazos o caminos de comunicación que utilizan los nodos o puntos de unión de lazos que conforman una determinada red, para comunicarse entre sí y con otras redes. Un ejemplo de topología puede comenzar con “la inserción del servicio de internet desde el proveedor, pasando por el

router, luego por un *switch* y esta deriva a otro *switch* u otro *router* o sencillamente a los *hosts* (estaciones de trabajo). El resultado de esto es una red con apariencia de árbol" (18 p.41).

En las Redes de Área Local – LAN, la topología se define como un mapa físico o lógico de la red que sirve para intercambiar datos circunscritos a un área físicamente pequeña; luego, las topologías de LAN constituyen las formas en las que dichas redes locales se encuentran diseñadas tanto en el plano físico como en el constructo lógico. Cuando las formas de diseños o arquitecturas antes señaladas se presentan independientemente de las funciones que estas cumplirán, se está frente a una topología. En este punto es menester recordar que: "La topología se ocupa de aquellas propiedades de las figuras que permanecen invariantes cuando dichas figuras son plegadas, dilatadas, contraídas o deformadas, de modo que no aparezcan nuevos puntos o se hagan coincidir puntos diferentes" (19 p.63).

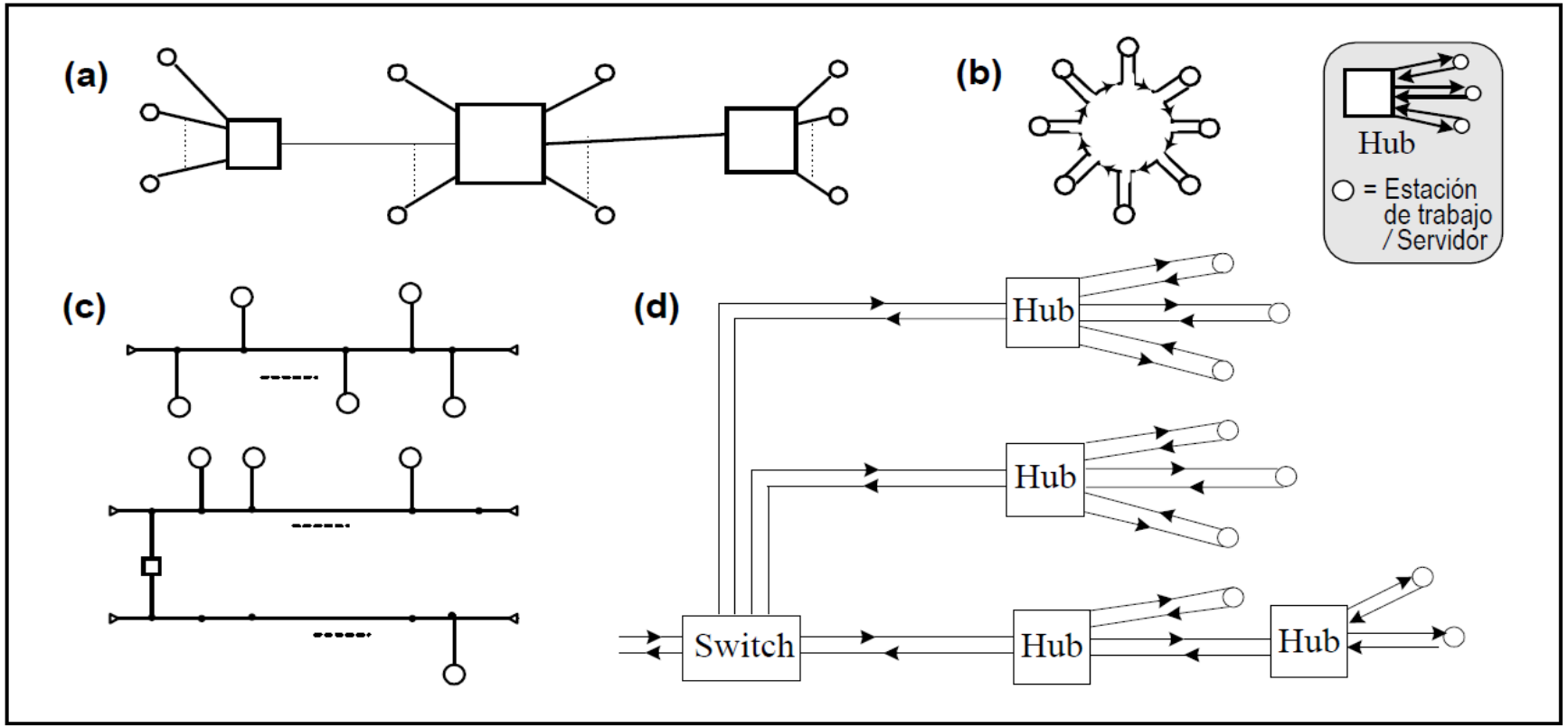
Ya sea en el plano físico o lógico, el concepto de red puede concebirse como un conjunto de nodos interconectados, y la topología de la misma como la distribución física de los elementos de dicha red, incluyendo la localización de cada elemento *hardware* y cómo está conectado con los demás. En ese sentido, y por su adaptación y funcionalidad en áreas pequeñas, las redes LAN suelen estructurarse siguiendo, principalmente, los siguientes tipos de topologías:

- Topología de Anillo: Topología de red en la que cada nodo se conecta exactamente a otros dos nodos, formando una única ruta continua.
- Topología de Árbol (Hub/Tree): Topología de red en la que los nodos están colocados en forma de árbol, es decir, distribuidas en ramas diversificadas.
- Topología de Bus: Topología que se caracteriza por tener un único bus de comunicaciones al cual se conectan los diferentes dispositivos.
- Topología de Estrella: Topología en la cual los dispositivos están conectados directamente a un punto central.

Teniendo en cuenta los cuatro tipos de topologías más usuales en la configuración de Redes de Área Local – LAN, en la Figura 1 se muestran gráficamente los medios físicos empleados por dichas redes LAN.

Figura 1

Topologías más usuales en la configuración de LAN



Nota. Adaptado de "Redes de computadoras", por Alcocer, A., p.118.

Notas. Topología tipo Estrella, Topología tipo Anillo, Topología tipo Bus, Topología tipo Hub/Tree.

2.2.2. Seguridad en redes informáticas

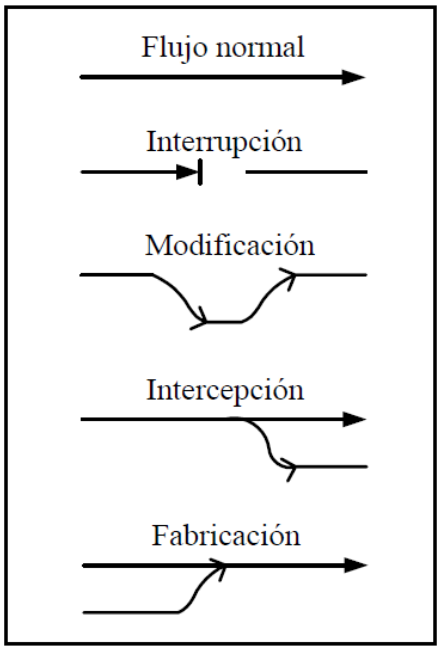
La seguridad en redes informáticas se refiere o tiene que ver tanto con la ausencia de riesgo en el plano físico de red, vale decir, en el conjunto de dispositivos que se encuentran conectados entre sí, con el objetivo de compartir recursos, servicios y/o información; así como con la confianza en el funcionamiento de los medios de transmisión por donde viaja la información digital que puede ser alámbrica o inalámbrica, vale decir, confianza en el buen funcionamiento del plano lógico de la red.

Dado que la seguridad de las redes de computadoras o redes informáticas se puede organizar teniendo en cuenta los tres aspectos señalados en el párrafo anterior, es pertinente señalar que, para efectos de la presente investigación, se tuvo en cuenta solamente el aspecto referido a los ataques a la seguridad.

En un contexto de tipos de ataques a las comunicaciones, lo cual conlleva una amenaza contra la seguridad del sistema informático, se tienen cuatro tipos de amenazas: interrupción, modificación, intercepción y fabricación. En la Figura 2 se presentan los esquemas de dichos tipos de amenazas que pueden deberse a ataques desde dentro de la Red (ataques internos) o desde fuera de la Red (ataques externos).

Figura 2

Amenazas contra la seguridad de sistemas informáticos



Nota. Adaptado de “Redes de computadoras”, por Alcocer, A., p.354.

La interrupción es una amenaza contra un recurso del sistema y afecta la disponibilidad del mismo. De lo mostrado en la Figura 2 se tiene que esta amenaza se produce cuando “se pierde una parte del sistema o no está disponible o no puede usarse. Por ejemplo: la destrucción

física de un equipo, el borrado de una aplicación o de un archivo de datos, una falla del sistema operativo, etc." (17 p.354)

Con respecto a la intercepción, se tiene que esta se produce cuando una entidad no autorizada consigue acceso a un recurso; luego, este es un ataque contra la confidencialidad. De lo mostrado en la Figura 2 se tiene que este tipo de ataque se produce cuando "alguien no autorizado logra acceder al sistema. Puede tratarse de una persona, un programa o sistema de computación. Ejemplo: reproducción ilícita de archivos, intercepción de cables para sacar los datos de una red. Como no se pierden datos, es difícil detectar este tipo de ataques" (17).

Por su parte, con respecto a la modificación, se tiene que este tipo de amenaza se refiere a la alteración, desinstalación o borrado por parte de personal no autorizado, de datos, software y archivos, respectivamente; es decir, constituye un ataque a la modificación desautorizada. De lo mostrado en la Figura 2 se tiene que este tipo de ataque se produce cuando "alguien no autorizado accede a la información del sistema y la modifica. Ejemplo: cambiar valores en una base de datos o alterar un programa para que realice operaciones adicionales" (17).

Asimismo, con respecto a la fabricación, se tiene que este tipo de amenaza se produce cuando una entidad no autorizada inserta objetos falsificados en el sistema; es decir, constituye un ataque contra la autenticidad. De lo mostrado en la Figura 2 se tiene que este tipo de ataque se produce cuando "alguien no autorizado crea y añade objetos a un sistema de cómputo. Por ejemplo: insertar registros a una base de datos existente o añadir transacciones a un sistema de comunicación de redes" (17).

Finalmente, en caso de encontrar elementos vulnerables a cualquiera de los tipos de amenazas antes descritos, en el sistema de seguridad informático, se procede al desarrollo de un sistema de seguridad informática o la dotación de elementos robustos que eliminen dichas vulnerabilidades. Dicho desarrollo estará sujeto a las políticas para un Sistema de Seguridad Informática.

2.2.3. Políticas de seguridad en redes informáticas

Las teorías referidas a la generación de políticas de seguridad basado en tecnologías informáticas, también llamadas políticas de seguridad en redes informáticas o simplemente Políticas de Seguridad Informática – PSI, constituyen las actividades realizadas para la protección de amenazas de los sistemas de información. En este punto, se trae a colación que la seguridad de las redes de computadoras se puede organizar en tres aspectos: servicios de seguridad, mecanismos de seguridad (encriptación) y ataques a la seguridad.

En un contexto de protección específica de una empresa, institución o entidad, las Políticas de Seguridad Informática – PSI "surgen como una herramienta organizacional para concientizar a cada uno de los miembros de una organización sobre la importancia y la

sensibilidad de la información y servicios críticos que favorecen el desarrollo de la organización y su buen funcionamiento" (20 p.11).

Complementando lo señalado en el párrafo precedente, y en un contexto reglamentario y normativo, se tiene que:

> Las políticas de seguridad informática consisten en una serie de normas y directrices que permiten garantizar la confidencialidad, integridad y disponibilidad de la información y minimizar los riesgos que le afectan. […] Una política de seguridad se define a alto nivel, esto es, qué se debe proteger y cómo, es decir, el conjunto de controles que se deben implementar. Esta se desarrolla en una serie de procedimientos e instrucciones técnicas que recogen las medidas técnicas y organizativas que se establecen para dar cumplimiento a dicha política. (21)

Restringiendo la definición de política de seguridad a un contexto organizacional, se tiene que esta "debe estar basada en una identificación y análisis previo de los riesgos a los que está expuesta la información y debe incluir todos los procesos, sistemas y personal de la organización. Además, tiene que haber sido aprobada por la dirección de la organización y comunicada a todo el personal" (21).

Por otro lado, las teorías referidas a la generación de políticas de seguridad informática basado en tecnologías informáticas señalan que estas deben establecerse, principalmente, en el contexto referenciado a los ataques a la Seguridad de las Redes de Computadoras; luego, dichas políticas deben estar orientadas al control de acceso a las mismas. En este punto es pertinente destacar que "la autorización concede derecho a un usuario para acceder a un recurso. El control de acceso es el medio de hacer cumplir esas autorizaciones. En general, se puede afirmar que el control de acceso es el método empleado para prevenir el uso no autorizado de los recursos" (17 p.362).

Para el control de accesos, existen dos métodos para prevenir los accesos no autorizados, que varían dependiendo de si el usuario o solicitante tiene autorización para el ingreso al sistema informático (usuario interno) o no lo tiene (usuario externo).

En caso que el solicitante es usuario interno, el procedimiento regular establecido para el control de accesos exige un filtro de la solicitud de acceso. Para tal efecto se realiza una verificación de los derechos de dicho usuario respecto a un recurso cuando el usuario intenta acceder a este. En este caso, se establece el denominado control de acceso basado en la identidad. En este tipo de solicitud de acceso cabe establecer diferencias entre los accesos individuales y los accesos grupales. En la Tabla 3 se presentan las diferencias en cuestión.

Tabla 4

Control de acceso basado en la identidad

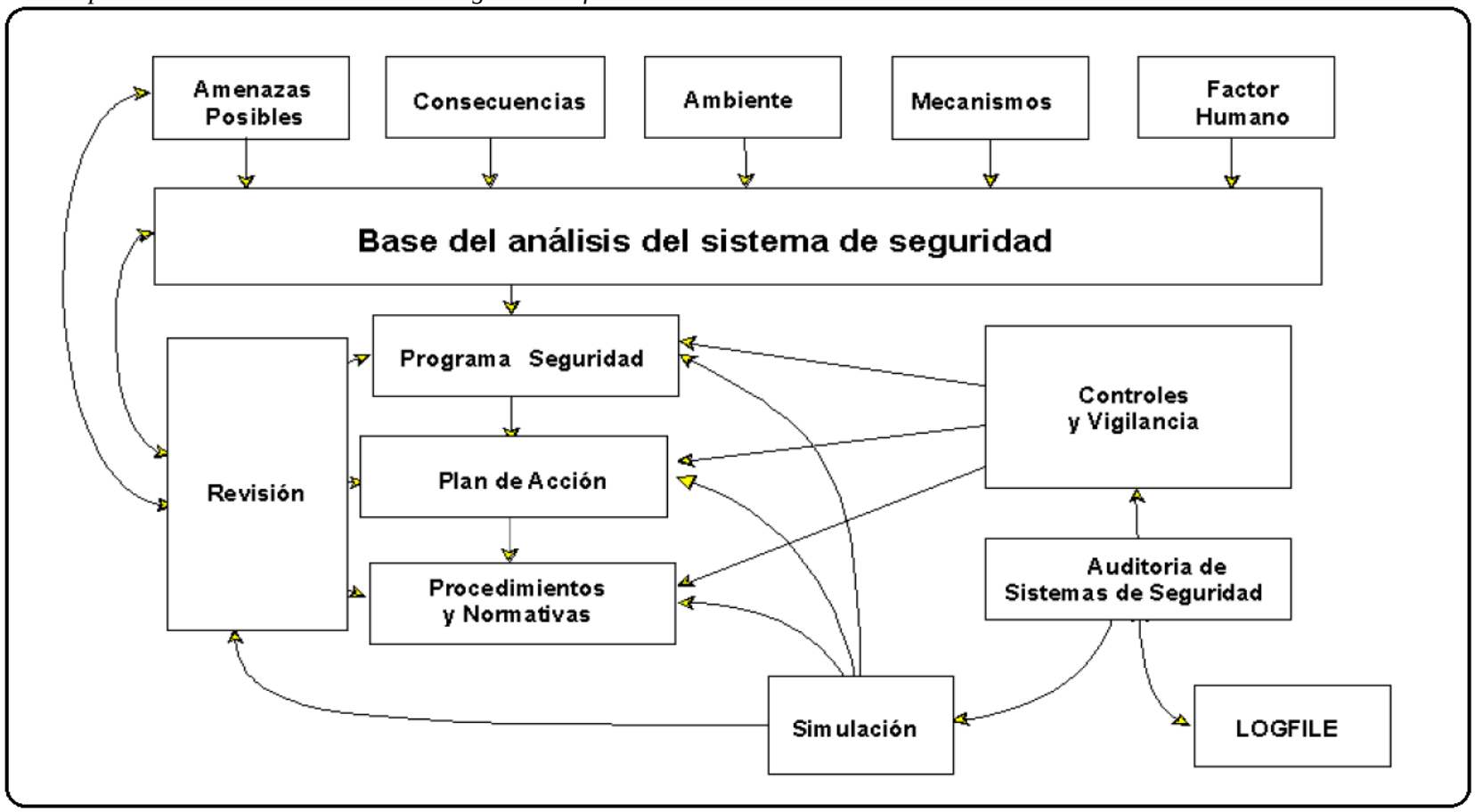
TIPO DE SOLICITUD DE ACCESO	DESCRIPCIÓN
Accesos individuales	Si los usuarios señalan los derechos que posee, podrán acceder a una serie de recursos enlistados. Determinado usuario podrá utilizar dos recursos (lectura y escritura), mientras que otro usuario tal vez solo pueda acceder a uno de ellos.
Accesos grupales	A partir de un nombre único que se les otorga a grupos de usuarios con iguales derechos, estos podrán acceder a los mismos recursos, con lo que se dinamiza las tareas de auditoría y administración.

Nota. Adaptado de "Redes de computadoras", por Alcocer, A., p.363.

Las teorías referidas a la generación de políticas de seguridad basadas en tecnologías informáticas establecen que las políticas en mención se sustentan en el precepto principal establecido para la seguridad en redes, el cual es: "mantener bajo protección los recursos y la información con que se cuenta en la red, a través de procedimientos basados en una política de seguridad que permita el control de lo actuado" (20 p.12). Además, en el desarrollo de Políticas de Seguridad Informática – PSI se sigue un esquema sustentado en el análisis de seguridad; en ese sentido, en la Figura 3 se presenta un modelo de desarrollo de PSI.

Figura 3

Modelo para el desarrollo de Políticas de Seguridad Informática - PSI



*Nota***.** ARCERT. Manual de Seguridad en Redes p.19.

En la ejecución o implementación de las Políticas de Seguridad Informática – PSI, previamente planeadas, se sigue un proceso que se configura en función a etapas y/o fases de implementación secuenciales. En la Tabla 4 se detallan las etapas del proceso de implementación de Políticas de Seguridad Informática– PSI.

Tabla 5

Proceso de implementación de una política de seguridad.

NOMBRE DE LA ETAPA DEL PROCESO	DESCRIPCIÓN
Definición de los alcances	Etapa en la cual se define el alcance de la política, incluyendo sistemas y personal sobre el cual se aplica.
Planteamiento de objetivos	Etapa en la cual se plantean los objetivos de la política y descripción clara de los elementos involucrados en su definición.
Responsabilidades de la organización	Etapa en la cual se establecen las responsabilidades de cada uno de los servicios, recursos y responsables en todos los niveles de la organización.
Responsabilidades de los usuarios	Etapa en la cual se establecen las responsabilidades de los usuarios con respecto a la información que generan y a la que tienen acceso.
Establecimiento de los requerimientos	Etapa en la cual se definen los requerimientos mínimos para la configuración de la seguridad de los sistemas al alcance de la política.
Definición de las reglas	Etapa en la cual se definen las reglas a seguirse. Dichas reglas tienen que ver con la definición de violaciones y las consecuencias del no cumplimiento de la política.
Establecimiento de penalidades	Se llevan a cabo sanciones ante determinados actos que contravienen los reglamentos. Estas sanciones se deberán imponer a partir de determinadas políticas. Pero, puesto que no es obligación de la ley, la exactitud con la que se llevará a cabo o el momento en que sucederá, no será especificado.
Transparencia de las políticas	Las decisiones que han sido tomadas deben ser explicadas, con precision y sin ambiguedades, para transparentar la información.
Actualización de políticas	Como parte de la actualización constante, aquí se mejoran las políticas, modificaciones mediadas por los cambios en la estructura interna de la organización.

*Nota***.** Adaptado de “Implementación de una Política de Seguridad”, por Borghello, C. (ed.), 2021.

En síntesis, las políticas de seguridad informática de una empresa u organismo deben adaptarse a todas sus necesidades y, en la medida de lo posible, ser atemporales; y es que a la hora de compartir información y recursos en una red, "se ponen en juego activos y valores muy importantes para su poseedor, ya sea que se trate de una persona o de una empresa. Por eso, la aplicación de mecanismos de protección para esos activos es una de las tareas más importantes a la hora de trabajar con redes" (16 p.5). Es por ello que "cada vez se hace más necesario el rol del experto en ciberseguridad dentro de las organizaciones, un perfil profesional especializado en ciberseguridad y que responde a las nuevas necesidades en materia seguridad en un contexto de digitalización de las organizaciones" (21).

2.2.4. Cisco Identity Services Engine (CISCO ISE)

Cisco Identity Services Engine - CISCO ISE se concibe como "una plataforma de control y administración de políticas de seguridad. Automatiza y simplifica el control de acceso y el cumplimiento de las normas de seguridad para redes cableadas, inalámbricas y conexiones mediante VPN" (22 p.2).

Cisco ISE se utiliza principalmente para proporcionar acceso seguro tanto a los usuarios de la plataforma como a los invitados. Con respecto a los primeros, la plataforma apoya las iniciativas BYOD, luego: "Ya sea porque deba implementar prácticas de trabajo en las que cada empleado trae su propio dispositivo (bring your own device, BYOD) u ofrecer un acceso más seguro a los recursos del Data Center, Cisco Identity Services Engine (ISE) es la solución ideal" (22 p.1).

High Tech Center – HTC (22) es una empresa boliviana que presta servicios en asesoramiento, consultoría, diseño, soporte e implementación en soluciones que integran transmisión de voz, datos y video integrados; destaca las siguientes ventajas de Cisco ISE:

- En el aspecto referido a la seguridad de redes, CISCO ISE permite mejorar la visibilidad y el control de todas las actividades y dispositivos en su red física e infraestructura virtual.
- En el aspecto referido al cumplimiento de los requerimientos específicos de seguridad, CISCO ISE permite establecer políticas uniformes en toda la infraestructura para mejorar el cumplimiento de las normas empresariales.
- En el aspecto referido a la eficiencia, CISCO ISE permite la automatización de las tareas intensivas y simplifica la prestación de servicios para aumentar la productividad del personal de TI.

Por otro lado, además de las ventajas antes señaladas, es pertinente destacar los beneficios que ofrece CISCO ISE. En ese sentido, en la Tabla 5 se destallan algunos beneficios de dicha plataforma.

Tabla 6

Beneficios de usar CISCO ISE

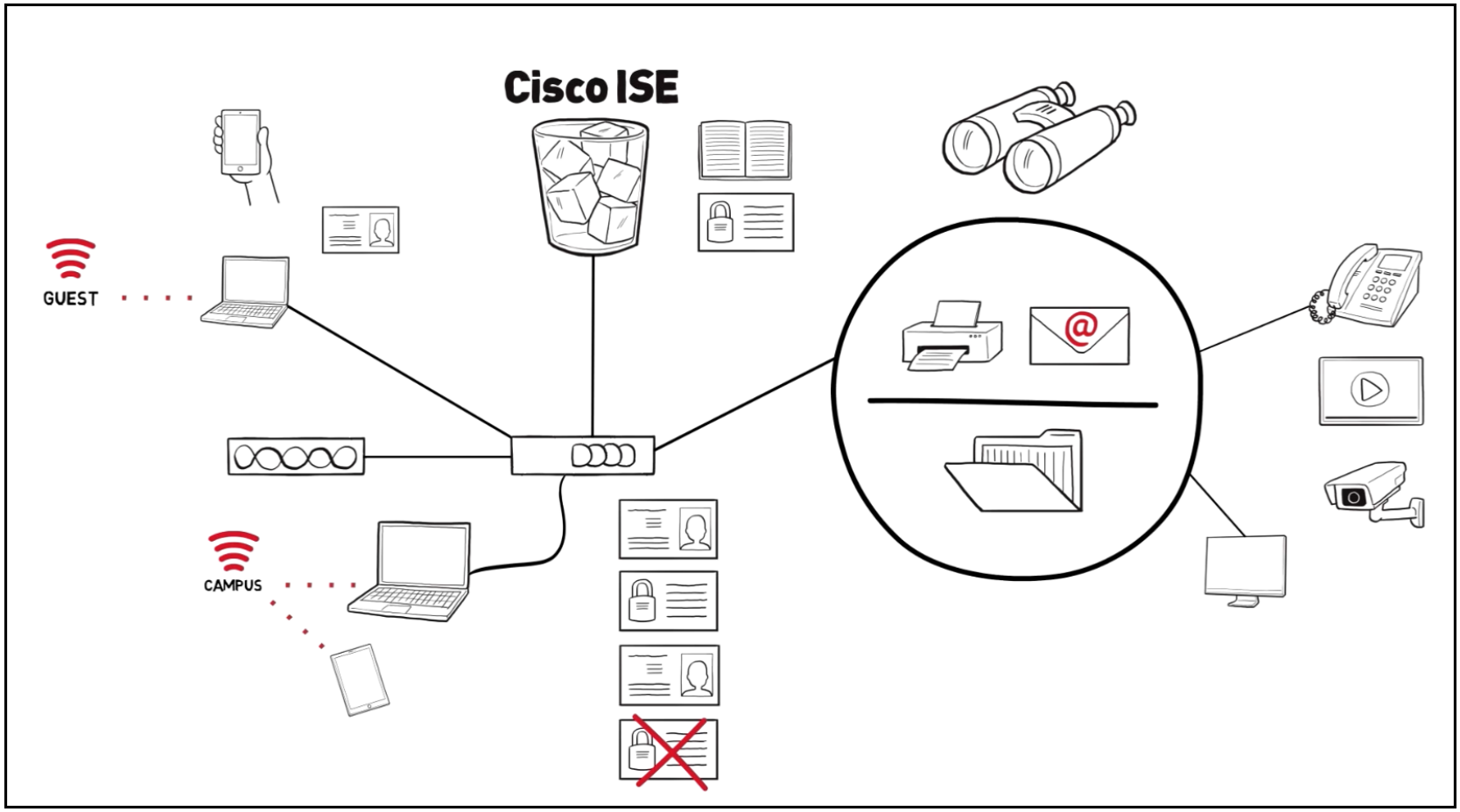
BENEFICIO	DESCRIPCIÓN
Beneficios en la verificación rigurosa y reconocimiento automático del perfil de dispositivo	Puede identificar todos los equipos de la red, en todo lo relativo a la ubicación, el tiempo, y otros atributos. Los dispositivos no podrán sortear su identificación o visibilidad, y, además, las características de los dispositivos también serán identificadas.
Beneficios en la aplicación y cumplimiento de políticas de seguridad	Facilita las auditorias y las regulaciones a partir de la visibilidad y creación de reportes para todas las redes, ello mediante la interfaz gráfica. Además, se cumple con la normativa 802.1x, norma del IEEE, identificando todos los equipos que estén conectados a un puerto LAN; si la autenticación tiene errores, se limita el acceso por tal puerto.
Beneficios en la integración automática de los dispositivos con acceso seguro y confiable desde cualquier lugar	De acuerdo a las políticas TI, los usuarios podrán registrarse y registrar sus dispositivos de manera automática mediante un portal de auto registro. Con ello, TI podrá acceder a la información y cumplir con sus objetivos de seguridad, al tiempo que libra a los usuarios de requerir apoyo de TI.
Beneficios en la eficiencia operativa	Dicha automatización mejorará la eficiencia, al tener al personal de TI más liberado respecto a los problemas con la red.

*Nota***.** High Tech Center. ISE Cisco Identity Services Engine – High Tech Center; p.3.

En síntesis, CISCO ISE es una plataforma de seguridad digital estructurada sobre la base de dos capas. La primera referida a la TRUSTSEC, que es un mecanismo que permite segmentar dinámicamente el tráfico de la red organizando los dispositivos terminales en diferentes grupos lógicos, solución de seguridad que se ha ido desarrollando e integrando en los diferentes dispositivos de infraestructura que ofrece Cisco Systems; y el acceso seguro basado en BYOD. En la Figura 4 se presenta el esquema funcional de la plataforma de seguridad informática CISCO ISE.

Figura 4

Esquema funcional de la plataforma CISCO ISE



*Nota***.** De “How IT Works Cisco Identity Services Engine”, por Coutinho, N. (Director).

Finalmente, es pertinente destacar que, en los últimos años, las redes corporativas han comenzado a migrar hacia una arquitectura de red definida por software (SDN). En ese escenario, CISCO ISE ha lanzado sus propuestas SD Access y SD WAN. La arquitectura SD Access permite dinamizar y automatizar la operación de la red para dar lugar a una red que responda rápida y flexiblemente a los objetivos institucionales de las organizaciones (integra TrustSec). La arquitectura SD WAN permite la comunicación a través de Internet mediante el cifrado entre las ubicaciones de una organización (integra BYOD).

2.2.4.1. Seguridad informática basada en CISCO ISE. Brindar seguridad informática, principalmente, busca una solución a los ataques; en efecto, para "el armado de una red es un trabajo que requiere contar con conocimientos teóricos y prácticos. Desde su diseño inicial, es importante tener en cuenta una serie de factores que harán que cumpla con su cometido sin sufrir caídas ni ataques que la hagan inaccesible a los usuarios o que generen pérdida de información o de dinero" (16 p.16). Para el logro del cometido referido a los ataques, se han desarrollado tecnologías orientadas a la ciberseguridad organizacional las cuales, como se señaló anteriormente, deben ser establecidas en función a las necesidades propias de cada organización, empresa o institución.

En el contexto descrito en el párrafo anterior, la tecnología CISCO *Identity Services Engine* (CISCO ISE) se constituye como una tecnología desarrollada en el campo de la seguridad de redes informáticas que permite gestionar las Políticas de Seguridad Informática - PSI, permitiendo o negando el acceso a una red corporativa a todo tipo de usuarios que quieren ingresar a la red con una gran variedad de dispositivos que van desde portátiles o equipos de escritorio hasta *ipads* y *smartphones*.

CISCO *Identity Services Engine* - CISCO ISE es una tecnología de seguridad de redes informáticas que integra funcionalmente diversos aspectos relevantes de la seguridad en un servidor de políticas que permite gestionar el acceso a una red corporativa. Los tipos de seguridad de red que ofrece CISCO ISE son variadas y consideran diferentes tipos de seguridad para la red física e inalámbrica.

CISCO ISE brinda soluciones específicas a las demandas relacionadas con la seguridad en la identificación de usuarios de una red informática; por ejemplo, una Red LAN. En efecto, la tecnología ISE de CISCO permite la autenticación de los usuarios, permitiendo el acceso a la red sólo a usuarios autorizados, aplicando políticas por perfiles de usuarios para autorizar o denegar el acceso. Luego, dado que hay una tendencia en las organizaciones hacia el uso de aplicaciones corporativas para dispositivos móviles, y que no todos los usuarios deben tener acceso a la red, entonces, la parte ISE de la tecnología CISCO se convierte en una tecnología adecuada para la seguridad en la autenticación de usuarios.

En la Tabla 7 se detallan los tipos de seguridad de red ofrecidos mediante la Tecnología CISCO tanto para la seguridad de la red como para la implementación de Políticas de Seguridad Informática– PSI.

Tabla 7

Tipos de seguridad en la identificación basado en la tecnología CISCO - ISE.

TIPO	DESCRIPCIÓN
Seguridad del correo electrónico (Email Security)	Con objeto de impedir que se pierdan datos importantes, se bloquen ataques que entran y se controlan los mensajes que salen.
Segmentación de la red (Network Segmentation)	Identidad lograda a partir de EndPoints y no únicamente en las direcciones IP. Se identifican equipos sospechosos y se asignan roles para que personas adecuadas puedan tener determinados accesos.
Control de acceso (Access Control)	El NAC (control de acceso a la red) permitirá bloquear equipos de EndPoint y asignarles accesos con límites.
Seguridad de las aplicaciones (Application Security)	*Hardware* y *software* son tenidos en cuenta dentro de la seguridad, además de todo aquel proceso que pretende identificar y fortalecer las vulnerabilidades.
Análisis del comportamiento (Behavior Analysis)	Identifican todo aquello que no se ajusta a la norma.
Seguridad de dispositivos móviles (Mobile Device Security)	Con objeto de mantener la seguridad de la red, puede permitir o rechazar el acceso de los dispositivos.
Administración de eventos e información de seguridad (Security Information and Event Management)	Para que el personal puede hacer frente a las amenazas, SIEM aporta información valiosa a este respecto. Se incluyen aquí los dispositivos tanto físicos como virtuales.
VPN - Red Privada Virtual (Virtual Private Network)	Una red privada virtual cifra la conexión desde un terminal a la red, generalmente por Internet. VPN de CISCO permite autenticar las comunicaciones entre los dispositivos y la red.
Seguridad inalámbrica (Wireless Security)	Existen servicios orientados particularmente a preservar la seguridad de la red inalámbrica.

*Nota***.** Adaptado de "¿Qué es la seguridad de red?", por CISCO

2.2.4.2. Políticas de seguridad informática basadas en CISCO ISE. Las políticas de seguridad se establecen teniendo en cuenta que la seguridad de la información debe ser vista como un proceso continuo, no estático. En ese sentido, CISCO:

> Permite definir políticas de acceso de una forma dinámica y sencilla que cumpla con los requisitos de cambio que requiera la empresa. Por ejemplo, los administradores de TI pueden definir de forma sencilla políticas en el ISE que permitan diferenciar equipos de usuarios invitados de los equipos de los usuarios corporativos. Los usuarios invitados reciben un acceso limitado dentro de la red, mientras que los usuarios corporativos tienen acceso de acuerdo a las políticas asignadas. (22 p.3)

Con respecto a las funcionalidades que ofrece la plataforma CISCO ISE para el cumplimiento de las políticas de seguridad, se tiene que esta permite hacer cumplir las políticas de uso conjuntamente con Cisco TRUSTSEC en los cuatro rubros que se detallan en forma esquemática en la Figura 5.

Figura 5

CISCO ISE: Seguridad de acceso para las redes cableadas, inalámbricas y por VPN

*Nota***.** High Tech Center. ISE Cisco Identity Services Engine – High Tech Center, p.2.

Por otro lado, el *software* de la plataforma CISCO ISE tiene una función específica para la administración de políticas de seguridad; por ejemplo: “Cisco ISE 2.6 es un producto para control de acceso de red unificado que implementa funcionalidades de autenticación, autorización y auditoría. Todas las funcionalidades son configurables mediante la definición de políticas a través de la interfaz web o a través de línea de comandos” (6 p.5).

En la Tabla 8 se muestran los dispositivos (físicos o virtuales) donde se despliega el producto CISCO – ISE 2.6, siendo estos dispositivos de *hardware* compatibles y necesarios como parte del entorno de instalación.

Tabla 8

Dispositivos Hardware Compatibles CISCO - ISE

Nombre de la distribución	Características *Hardware*
Cisco ISE Appliance 3515 (SNS-3515)	CPU: Intel Xeon E5-2620 v3 (Haswell)
	RAM: 16 GB
	HDD: 1x600 GB (RAID 0)
	I/O: 2xPCIE, 2xRJ45, 4xUSB 3.0, 1xETHERNET, 2xVGA
Cisco ISE Appliance 3595 (SNS-3595)	CPU: Intel Xeon E5- 2640 v3 (Haswell)
	RAM: 64 GB
	HDD: 4x600 GB (RAID 0+1)
	I/O: 2xPCIE, 2xRJ45, 4xUSB 3.0, 1xETHERNET, 2xVGA
Cisco ISE Appliance 3615 (SNS-3615)	CPU: Intel Xeon Silver 4110 (Skylake)
	RAM: 32 GB
	HDD: 1x600 GB
	I/O: 2xPCIE, 2xRJ45, 4xUSB 3.0, 1xETHERNET, 2xVGA
Cisco ISE Appliance 3655 (SNS-3655)	CPU: Intel Xeon Silver 4110 (Skylake)
	RAM: 96 GB
	HDD: 4x600 GB (RAID 1+0)
	I/O: 2xPCIE, 2xRJ45, 4xUSB 3.0, 1xETHERNET, 2xVGA
Cisco ISE Appliance 3695 (SNS-36955)	CPU: Intel Xeon Silver 4110 (Skylake)
	RAM: 256 GB
	HDD: 8x600 GB (RAID 1+0)
	I/O: 2xPCIE, 2xRJ45, 4xUSB 3.0, 1xETHERNET, 2xVGA
Cisco ISE Engine virtualizado (ISE-VM) **(Características asociadas recomendadas)**	CPU: Intel Xeon Silver 4110 (Skylake)
	RAM: 96 GB
	HDD: 4x600 GB (RAID 1+0)
	I/O: 2xPCIE, 2xRJ45, 4xUSB 3.0, 1xETHERNET, 2xVGA
	Hipervisor: ESXi 6.7

*Nota***.** De "Procedimiento de empleo seguro Cisco ISE 2.6", por Ministerio de Defensa de España, p.6.

Asimismo, las políticas de seguridad para ataques internos, ataques intencionados o ataques inocentes, principalmente, deben responder al modo de ataque que puede afectar al sistema de información. A decir de CISCO, dichos ataques pueden variar en función a diversos aspectos; no obstante, es posible situar cada uno de ellos en alguna de las siguientes categorías:

- Ataques por interceptación: dichos ataques pueden ser activos o pasivos, y tienen como objetivo ganar acceso a información para la cual el atacante no se encuentra autorizado. "En un entorno de red, la interceptación pasiva, por ejemplo, podría encontrarse relacionada con una persona que, de manera rutinaria, monitorea el tráfico de red. Por su parte, el hecho de situar un sistema de cómputo entre el emisor y el receptor de algún mensaje o información podría considerarse interceptación activa" (16 p.269).
- Ataques por modificación: dichos ataques tienen como objetivo realizar cambios en el entorno. "En un ataque de este tipo, un usuario malicioso obtiene acceso no autorizado a un sistema o recurso con el nivel de privilegios necesarios para alterar, de algún modo, los datos o información que en él se encuentran para su beneficio. Por ejemplo, la modificación del flujo de datos en una comunicación o la edición del contenido de un archivo en un servidor representan ejemplos claros de este tipo de ataques" (16).
- Ataques por interrupción: dichos ataques tienen como objetivo afectar, dañar o dejar sin funcionamiento un sistema completo o parte de él. "Un aspecto característico de los ataques de interrupción es que, a menudo, estos son fáciles de detectar, debido, principalmente, a que su existencia es rápidamente notada por los usuarios autorizados de la red. Los daños ocasionados por la eventual suspensión del servicio y el tiempo de recuperación relacionado con este tipo de ataques pueden llegar a ser muy importantes" (16 p.270).
- Ataques por falsificación: dichos ataques tienen como objetivo falsificar alguno de los componentes de un sistema, por ejemplo, un usuario que altera su identidad simulando ser un anfitrión o *host* determinado, con la finalidad de conseguir algún beneficio propio. "La falsificación puede aplicarse tanto a escenarios donde se hayan construido determinados paquetes de datos arbitrariamente, con el objeto de hacer creer a un sistema o dispositivo acerca de la veracidad de los mismos, a fin de que este ejecute alguna acción que pueda ser aprovechada por el atacante; como a aquellos en los que una persona participa de una conversación simulando ser otro interlocutor" (16 p.271).

En síntesis, las políticas de seguridad informática basadas en CISCO ISE, tema objeto de estudio de la presente investigación, tiene como marco de actuación a la arquitectura de red definida por software (SDN) en un contexto referenciado por las redes corporativas. Dichas políticas se desarrollan en dos entornos diferenciados: el entorno TRUSTSEC, orientado a la funcionalidad de la red de tal manera que esta responda rápida y flexiblemente a los objetivos

institucionales de las organizaciones (Arquitectura SD Access); y el entorno BYOD, orientado a la comunicación a través de internet mediante el cifrado entre las ubicaciones de la organización (Arquitectura SD WAN).

2.3. Definición de términos básicos

En el presente subcapítulo se presentan las definiciones de aquellos términos, principalmente dimensiones e indicadores de las variables, de uso frecuente en el desarrollo de la presente investigación.

Acces point: el Punto de Acceso o Acces Point es un dispositivo utilizado en redes inalámbricas de área local, WLAN - Wireless Local Area Network. Dicho dispositivo cumple la función de "una puerta de entrada a la red inalámbrica en un lugar específico y para una cobertura de radio determinada, para cualquier dispositivo que solicite acceder, siempre y cuando esté configurado y tenga los permisos necesarios" (23 p.11).

Ataques internos: los ataques internos, también llamados intencionados o inocentes, son aquellas amenazas voluntarias que se derivan de ataques deliberados por agentes internos de una organización. "Los agentes internos pueden ser, por ejemplo, empleados descontentos o ex empleados cuyas credenciales de acceso no han sido revocadas" (22 p.29).

LAN (Cable, Wireless, VPN): Una Local Area Network es una red informática corta amplitud territorial, y, por lo general, se circunscribe a oficinas, viviendas, etc. Además, propicia la conexión entre diferentes dispositivos, (computadoras, laptops, impresoras, etc.). Estas pueden ser, también, redes inalámbricas. Las cableadas tienen mayor velocidad, pero tiene la desventaja de no poder mover los dispositivos. Por otro lado, una Red Privada Virtual Interna (VPN over LAN) "es una variante del tipo 'acceso remoto', pero, en vez de utilizar Internet como medio de conexión, emplea la misma red de área local (LAN) de la empresa. Sirve para aislar zonas y servicios de la red interna. Esta capacidad lo hace muy conveniente para mejorar las prestaciones de seguridad de las redes inalámbricas (WiFi)" (25 p.38).

Man in The Middle: Man In The Middle – MITM es un tipo de ataque informático por suplantación que "se produce cuando un *hacker* interviene en la transmisión de datos entre dos partes que realizan una comunicación electrónica. El ciberdelincuente se hace pasar por cualquier de ellas o por las dos «secuestrando» los datos y haciendo creer a las partes que se están comunicando entre ellas, cuando en realidad no es así, y es el *hacker* quien actúa como intermediario de esa comunicación" (26).

NAC (Network Access Control): Network Access Control (NAC) es una tecnología que permite controlar qué dispositivos pueden acceder a la red. La tecnología NAC permite el establecimiento de políticas de gestión tanto de los dispositivos fijos como de los dispositivos móviles, en este último caso, integra y compagina dichas políticas con la concepción trae tu propio dispositivo, BYOD por sus siglas en inglés.

Port-Security: denominación que alude a la necesidad que se tiene de proteger o brindar seguridad a todos los puertos (interfaces) del *switch*. La seguridad de los puertos se logra mediante el procedimiento de Control de Acceso a Medios (Media Access Control – MAC), ya sea limitando la cantidad de direcciones MAC válidas permitidas en el puerto, y/o permitiendo solamente el acceso a las direcciones MAC de los dispositivos considerados como legítimos.

Radius: es un protocolo que garantiza el acceso restringido a las redes inalámbricas y se caracteriza explícitamente por la prestación de los siguientes servicios en términos de seguridad: autenticación, autorización y auditoria - AAA. El Servicio de Usuario de Acceso Telefónico de Autenticación Remota (RADIUS por siglas en inglés) "es un protocolo que funciona sobre un equipo que hace las veces de servidor de acceso a través de autorización, autenticación y auditoria. RADIUS está pensado para distribución de acceso remoto seguro a redes y servicios que no poseen control de acceso a los usuarios. Este protocolo funciona bajo UDP/IP y cuenta con un servidor y usuarios" (27 p.46).

Switch (Conmutador de paquetes): también llamado *switching* o simplemente *switch*, envía los paquetes a los puertos basados en la dirección del paquete. El *switch* es aquel dispositivo "capaz de enlazar físicamente varios ordenadores de forma activa, enviando los datos exclusivamente al ordenador al que van destinados" (23 p.11). Asimismo, con respecto a los *switches* y su importancia en la seguridad informática, se tiene que estos constituyen "los dispositivos de capa más implementados sobre las redes modernas. Además, funcionan como primera línea de defensa" (16 p.268).

TACACS+: es un protocolo de comunicación de redes AAA que "utiliza una administración de red simplificada incrementando su seguridad al permitir centralizar la gestión de los usuarios en la red a través de políticas de acceso de usuarios, grupos, comandos, ubicación, subred o tipo de dispositivo. Del mismo modo […], proporciona un registro completo de todos los usuarios que se registraron y los comandos que utilizaron, reflejando de forma clara que es un protocolo orientado a la administración donde se puede tener de forma detallada toda aquella información sobre los usuarios y dispositivos de red que interactuaron en determinado momento y, además, proporcionar un registro detallado de cada acción realizada" (27 p.23).

Vulnerabilidades: vulnerabilidad de seguridad, también llamado agujero de seguridad o brecha de seguridad, se define como "un fallo técnico o deficiencia de un sistema que puede afectar la disponibilidad, integridad o confidencialidad de la información, pudiendo llevar a cabo operaciones no permitidas de manera remota" (24 p.23).

Wireless LAN Controller - WLC: el Controlador de Red Inalámbrica, WLC por sus siglas en inglés, permite centralizar el control de los Access Point o Puntos de Acceso en lugar

de delegar el control a cada uno de ellos. Mediante WLC los Acces Point ya no trabajan de manera autónoma, sino se convierten en un Acces Point Ligero – LWAP, todo ello con la ayuda del protocolo de Control y Aprovisionamiento para Puntos de Acceso Inalámbricos - CAPWAP. El LWAP enviará los datos hacia el WLC. Con esta funcionalidad se logrará, por ejemplo, hacer itinerancia o *roaming* y definir redes inalámbricas (WLAN – SSID) y autenticación. Además de ello, con un diseño de WLC y LWAP combinados se puede crear una única gran red WLAN, en lugar de crear varias redes separadas.

Capítulo III: Metodología

3.1. Métodos y alcance de la investigación

Puesto que lo que se procuró fue poner a prueba las hipótesis planteadas a partir de la recolección y el análisis de datos, se optó por el método cuantitativo. (28)

La investigación empezó como descriptiva, pero dado que se propone la implementación de políticas de seguridad haciendo uso de la tecnología CISCO ISE, esta tiene un alcance explicativo.

3.2. Diseño de la investigación

El diseño de la investigación es PRE experimental, ya que se mantiene en observación por un grupo de expertos, lo cual se presenta un escenario posible y sustentado en la propuesta de implementación de políticas de seguridad para la Red LAN de la agencia principal de Caja Huancayo.

3.3. Población y Muestra

3.3.1. Población

La población estuvo conformada por los 30 departamentos en que opera Caja Huancayo distribuidos a nivel nacional, existentes al cierre del año 2021.

3.3.2. Muestra

La muestra fue seleccionada de forma no probabilística e intencionada. Está conformada por los departamentos de Marketing e Infraestructura Tecnológica de agencia principal de Caja Huancayo, ubicada en la Calle Real N.° 341-343, Huancayo, Junín.

3.4. Técnicas e Instrumentos de Recolección de Datos

3.4.1. Técnicas

Observación: con esta técnica se pretende recoger información del *hardware* utilizado para la seguridad operativa en la agencia principal de la Caja Huancayo, documento hallado en el Anexo 4.

Entrevista: con esta técnica se pretende entrevistar al jefe de área de Infraestructura Tecnológica de la agencia de principal de la Caja Huancayo, con el objetivo de recolectar información relacionada con el *software* y con el sistema de protección implementado para la seguridad en las redes y comunicaciones, documento hallado en el Anexo 5.

Este documento se obtuvo mediante la entrevista sostenida con la Jefatura del dpto. de Infraestructura tecnológica. Además, se indicó que anualmente la Caja Huancayo pasa por un análisis interno que consiste en poder identificar ciertas vulnerabilidades; dicha identificación es realizado por una empresa terciaria. Luego que la empresa culmine de identificar todas las

vulnerabilidades, emite un informe con todas las vulnerabilidades encontradas con sus respectivos CVE (vulnerabilidades y exposiciones comunes). Este informe es emitido únicamente a la Jefatura del dpto. de Infraestructura Tecnológica, área encargada de derivar a cada unidad orgánica, con la finalidad que estas vulnerabilidades sean subsanadas bajo un *memorándum*. Dicho informe es altamente confidencial y por seguridad no se podría bridar mayor información, y en el caso que haya algún incumpliendo, este podría generar el despido del colaborador a cargo.

Encuesta: con esta técnica se pretende recolectar información valiosa sobre la propuesta de implementación por parte de 10 expertos de seguridad informática que laboran en empresas establecidas en la ciudad de Lima, documentos hallados en el Anexo 6.

3.4.2. Instrumentos

Cuestionario: este instrumento permitió la recopilación de información necesaria sobre los nueve aspectos de propuestas de implementación por parte de los 10 expertos en la implementación de tecnologías de seguridad informática que laboran en empresas establecidas en la ciudad de Lima, documentos hallados en el Anexo 6.

3.5. Validez y confiabilidad del instrumento

Validez del instrumento: con la finalidad de garantizar la eficacia del instrumento, se desarrolló una ficha de validez que fue desarrollada por tres ingenieros de Sistemas, de los cuales se obtuvo resultados aprobatorios. De esta manera se procede a utilizar el instrumento para la recolección de datos, documentos hallados en el Anexo 8.

Confiabilidad del instrumento: para garantizar la eficacia de los datos del instrumento, se utilizó el Alfa de Cronbach:

$$\alpha = \frac{k}{k-1}\left[1 - \frac{\sum V_i}{V_t}\right]$$

Donde: **α**: Alfa de Cronbach; **k**: Número de ítems; $\mathbf{V_i}$: Varianza de cada ítem; y $\mathbf{V_t}$: Varianza total.

Para ello se debe tomar en cuenta que la confiabilidad **α:**

- De 0 a 0.2: confiabilidad muy baja.
- De 0.2 a 0.4: confiabilidad baja.
- De 0.4 a 0.6: confiabilidad moderada.
- De 0.6 a 0.8: confiabilidad buena.
- De 0.8 a 1.0: confiabilidad alta.

De los resultados obtenidos en el Anexo 9, el Alfa de Cronbach resultó 0.89, por lo que se puede garantizar la validez de los resultados del instrumento con confiabilidad alta.

3.6. Procesamiento de la información

Para ello se realizó el cuestionario a 10 expertos de seguridad informática que laboran en empresas establecidas en la ciudad de Lima (siendo especialistas en implementaciones en soluciones de seguridad en la marca CISCO) sobre los nueve aspectos de propuestas de implementación. Para ello se contactó a cada uno de ellos para su participación en el cuestionario. Regresaron el cuestionario resuelto con su nombre, grado y firma digital en formato pdf. A partir de ello se procesará la información mediante el *software* Microsoft Excel 2021, se tabularán los resultados para cada aspecto y el análisis correspondiente para la tecnología de seguridad a utilizar.

Capítulo IV: Resultados y Discusión

4.1. Resultados

La etapa de ejecución de la investigación se caracteriza por estar conformada por tres fases secuenciales: el procesamiento de la información recolectada, el análisis de datos de la información previamente procesada y la interpretación de los resultados del análisis de datos.

En el presente subcapítulo se muestran los resultados del procesamiento de la información recolectada. En términos del cumplimiento de los objetivos de investigación, en el presente subcapítulo se da cuenta del logro del siguiente objetivo específico: identificar la política de seguridad informática actualmente operativa en la agencia principal de Caja Huancayo.

Como marco referencial o contexto de la investigación es pertinente destacar que la entidad financiera Caja Huancayo "tiene como cliente objetivo la pequeña y la micro empresa, principalmente en los sectores económicos C y D, a través de servicios crediticios para obtener capital de trabajo y para adquisición de activos fijos, complementado con créditos de consumo y con créditos hipotecarios para empleados y para empresarios vinculados a estos sectores" (29 p.5).

En cuanto a presencia institucional dentro de su rubro, se tiene que al cierre del año 2021 Caja Huancayo contaba con 183 oficinas distribuidas en todo el territorio nacional; además, "Caja Huancayo, con sus 33 años de vida institucional, continúa creciendo de manera sostenible, posicionándose como una empresa sólida y con una fuerte presencia de marca a nivel del sistema microfinanciero" (30). Lo que se ha señalado se verifica con lo expuesto por la Clasificadora de Riesgo Class & Asociados S.A., quienes al respecto destacan que: "Caja Huancayo es la tercera Caja Municipal con mayor número de agencias en todo el Perú, contando a junio del 2021 con 175 oficinas distribuidas a nivel nacional (55 en Lima y Callao y 120 en las demás regiones del país)" (29 p.5). Estas 175 oficinas, en términos de regiones del Perú, se encontraban distribuidas tal como se detalla en la tabla que prosigue:

Tabla 9

Estructura de negocios por Región de Caja Huancayo a junio de 2021

REGIÓN	N° AGENCIAS	COLOCACIONES		DEPÓSITOS	
		Miles S/	%	Miles S/	%
Junín	35	1,533,997	29.43%	1,647,863	39.09%
Lima	53	1,386,487	26.60%	1,714,954	40.68%
Ayacucho	6	275,213	5.28%	140,842	3.34%
Cusco	9	271,564	5.21%	69,832	1.66%
Pasco	7	224,131	4.30%	124,836	2.96%
Huánuco	8	197,548	3.79%	89,730	2.13%
Huancavelica	6	185,560	3.56%	104,038	2.47%
Ica	5	155,850	2.99%	76,641	1.82%
Puno	5	111,544	2.14%	7,920	0.19%
Piura	6	109,460	2.10%	28,039	0.67%
Ucayali	3	101,641	1.95%	32,039	0.76%
Arequipa	4	86,004	1.65%	23,487	0.56%
La Libertad	4	82,355	1.58%	20,195	0.48%
Tacna	3	65,676	1.26%	20,018	0.47%
Cajamarca	3	54,209	1.04%	8,700	0.21%
San Martín	2	48,475	0.93%	24,812	0.59%
Ancash	2	47,432	0.91%	18,435	0.44%
Moquegua	2	45,869	0.88%	6,388	0.15%
Lambayeque	2	42,220	0.81%	12,278	0.29%
Callao	2	39,093	0.75%	16,159	0.38%
Loreto	2	38,571	0.74%	8,527	0.20%
Apurímac	2	34,923	0.67%	8,426	0.20%
Tumbes	2	30,753	0.59%	4,402	0.10%
Amazonas	1	22,413	0.43%	3,346	0.08%
Madre de Dios	1	21,371	0.41%	3,437	0.08%
Total	**175**	**5,212,358**	**100%**	**4,215,345**	**100%**

*Nota***.** Adaptado de CLASS & ASOCIADOS S.A. Fundamentos de Clasificación de Riesgo: Caja Municipal de Ahorro y Crédito de Huancayo S.A., p.5.

Finalmente, se puede verificar por comparación entre los datos al finalizar el año 2021 y los datos presentados en la Tabla 8, correspondientes al segundo semestre del año 2021, que tan solo en dicho semestre la Caja Huancayo pasó de tener 175 a 183 agencias a nivel nacional. Dicho incremento representa un crecimiento del 4.57 % en el número de agencias en tan solo un semestre.

4.1.1. Proceso de propuesta de implementación de políticas de seguridad, basados en la tecnología Cisco ISE

Según la Tabla 4 que incluye las etapas de implementación, se realizaron de la manera siguiente:

- **Definición de los Alcances**: la propuesta de implementación fue aplicada a los departamentos de Infraestructura Tecnológica y Marketing, por lo que fue necesario identificar usuarios y equipos, y sobre la base de esta información se realizó la configuración de las políticas de seguridad basadas en Cisco ISE.
- **Planteamiento de Objetivos**: con la información recolectada del instrumento, se sostuvo que la tecnología Cisco ISE debería implementarse para mitigar las vulnerabilidades con base en políticas de seguridad, obteniendo la visibilidad de los distintos equipos y usuarios que se conectan a la Red LAN de Caja Huancayo.
- **Responsabilidades de la Organización**: se crea perfiles de administradores de red, operadores y monitoreo a fin de manejar niveles de seguridad por cargos “Analista y auxiliares del área de Redes y Comunicaciones”.
- **Responsabilidades de los Usuarios**: se definen ciertas políticas de seguridad con base en la unidad orgánica, permitiendo ciertas reglas de control de acceso.
- **Establecimiento de los Requerimientos**: identificar el área o unidad orgánica para las pruebas respectivas (departamentos de Infraestructura Tecnológica y Marketing), identificando los *swiches* y PCs, constatando que cada equipo de cómputo cuente con antivirus y la versión más reciente de Windows 10.
- **Definición de las reglas**: se crean perfiles de administradores y solo lectura, con la finalidad de garantizar el acceso controlado.
- **Establecimiento de Penalidades**: de darse esta situación, este deberá ser notificado al jefe del departamento de Infraestructura tecnológica, en donde él tomará las decisiones correspondientes, generando las sanciones de acuerdo a la magnitud.
- **Transparencia de las Políticas**: para este caso las políticas fueron creadas previo un análisis interno que consiste en identificar ciertas vulnerabilidades. Dicha identificación es realizada por una empresa terciaria; luego que la empresa culmine de identificar todas las vulnerabilidades, emitirá un informe con todas las vulnerabilidades

encontradas con sus respectivos CVE (vulnerabilidades y exposiciones comunes). Este informe es emitido únicamente a la Jefatura del dpto. de Infraestructura Tecnológica, área encargada de derivar a cada unidad orgánica con la finalidad que estas vulnerabilidades sean subsanadas bajo un *memorándum*, el cual se ajusta a las necesidades de la Caja Huancayo. Dicho informe es altamente confidencial y por seguridad no se podrá brindar mayor información sobre ello.

- **Actualización de Políticas**: la tecnología Cisco ISE está diseñada para lograr un despliegue a nivel institucional, sin embargo, para ello es necesario adquirir licencias adicionales.

4.1.2. Política de seguridad informática operativa en la agencia principal de Caja Huancayo

Para efectos de conocer la política de seguridad informática establecida para contrarrestar tanto ataques internos como externos a la Red LAN de la agencia principal de Caja Huancayo, se tuvo en consideración dos aspectos esenciales: la infraestructura informática de la Red LAN en la agencia principal de Caja Huancayo y la seguridad informática operativa en la agencia principal de Caja Huancayo.

4.1.2.1. Red LAN en la agencia principal de la Caja Huancayo. Para conocer la infraestructura informática de la Red LAN de la agencia principal de Caja Huancayo, se tuvo en consideración la técnica de la observación *in situ*, para tal efecto se utilizó un instrumento concordante con dicha técnica cuyo modelo es presentado en anexos (Anexo 1, Instrumentos de Recolección de Datos - Variable Independiente, ver A: Guía de observación *in situ*).

De la observación *in situ* de los aspectos relacionados con la seguridad informática que a finales del año 2021 se encontraban operativos en la Oficina Principal de Caja Huancayo, se obtuvo los siguientes resultados:

En la actualidad, la entidad financiera Caja Huancayo cuenta con los equipos de seguridad internos y externos que prosiguen:

- Firewall Palo Alto PA5060.
- Antivirus McAffe instalado en los equipos de cómputo.
- Equipos SWITCH de la Marca Cisco de los modelos 2960X y 9300L.
- Equipos SWITCH CORE CAMPUS de la marca Cisco Catalyst C9500-48.
- Directorio Activo en Microsoft Windows Server.

La oficina principal de Caja Huancayo cuenta con 500 PC de escritorio de la marca Lenovo, con 30 teléfonos IP’s de la marca Cisco asignado a cada oficina.

Las unidades operativas de la oficina principal de Caja Huancayo se encuentran enlazadas interna y externamente a través de los siguientes tipos de enlaces:

- Enlaces denominadas Cabecera Principal, para la interconexión con agencias de la Caja Huancayo.
- Enlaces por fibra óptica con el Shitch Core Campus y switches de acceso para la conectividad de los usuarios.
- Enlaces inalámbricos para la conexión con teléfonos IP's (Anexos) ubicados en la oficina principal.

A nivel de la arquitectura WAN, los servicios se encuentran configurados con el protocolo HSRP, a fin de contar con una alta disponibilidad de los enlaces WAN para garantizar la operatividad de las agencias a nivel nacional.

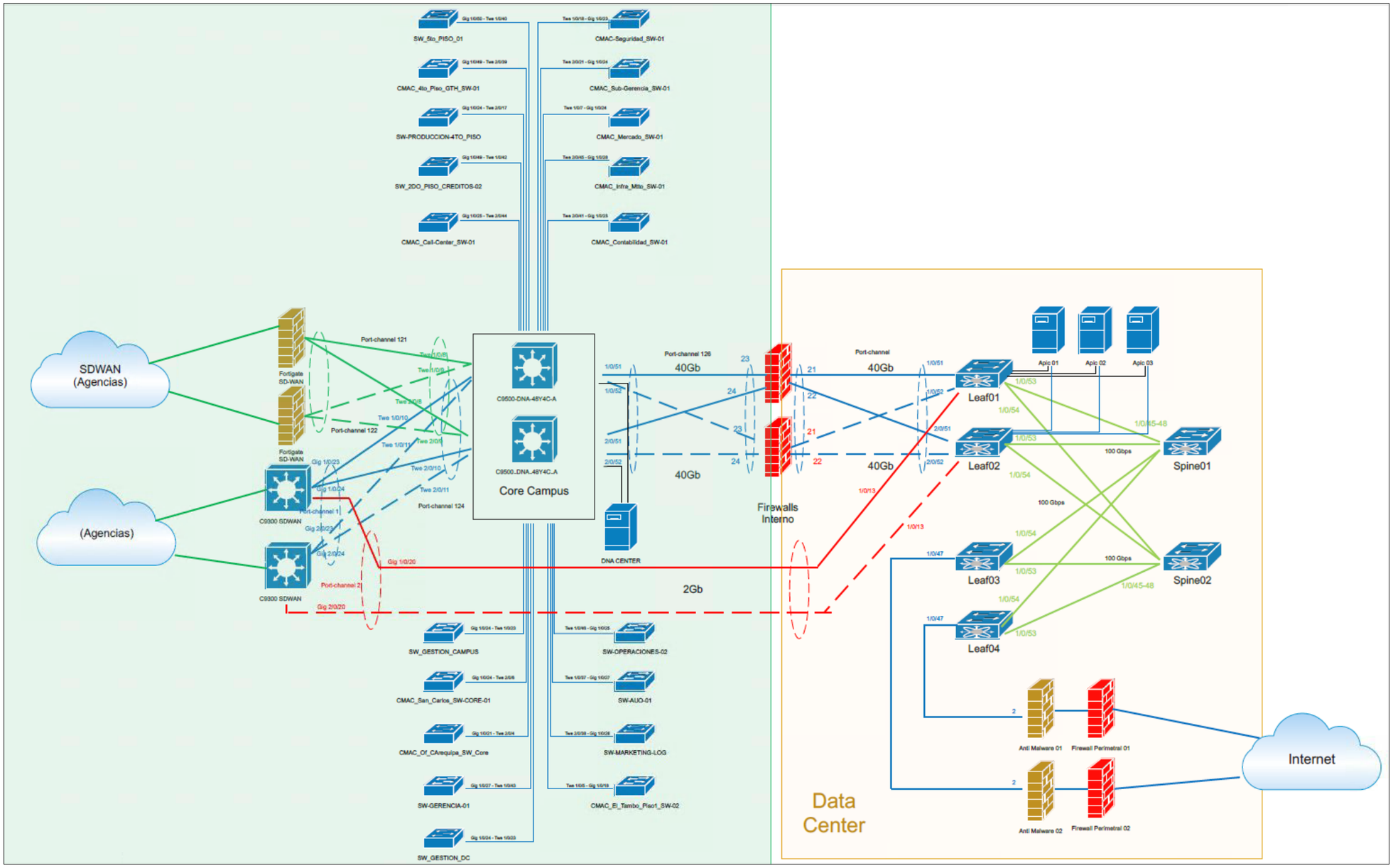
Por otro lado, la arquitectura Core Campus está compuesta por dos equipos Cisco Catalyst 9500, los mismo están configurados con la tecnología Virtual Stack, que ofrece mejoras en el diseño de las redes, alta disponibilidad, escalabilidad, gestión y mantenimiento.

Para la interconexión de los mundos de Campus y DataCenter se utiliza el protocolo de enrutamiento OSPF (Open Shortest Path First), con la finalidad de enrutar el tráfico entre áreas.

En concordancia con lo señalado en el párrafo anterior, en la Figura 6 se detalla esquemáticamente mediante un diagrama que a finales del año 2021 (noviembre y diciembre, meses de observación *in situ*) se encontraban instaladas en la oficina principal de Caja Huancayo.

Figura 6

Plano de distribución de las líneas informáticas conectadas a los principales equipos de seguridad instalados en la oficina principal de Caja Huancayo



Nota. Elaboración propia.

4.1.2.2. Vulnerabilidad de la seguridad informática en la agencia principal de Caja Huancayo.

Para efectos de conocer la vulnerabilidad de la seguridad informática de la Red LAN en la oficina principal de Caja Huancayo, implementada para contrarrestar tanto ataques internos como externos a la Red LAN de la agencia establecida en la Calle Real de la ciudad de Huancayo, se tuvo en consideración la información recolectada a través de la entrevista realizada al jefe encargado del área de Informática de dicha oficina principal.

La entrevista se realizó el primer día del mes de agosto del año 2021. Para tal efecto se utilizó un instrumento concordante con dicha técnica cuyo modelo es presentado en anexos (en Anexo 1, Instrumentos de Recolección de Datos - Variable Independiente; ver B: Guía de entrevista). De la consulta realizada al jefe del área de informática de la oficina principal de Caja Huancayo, se obtuvo las siguientes respuestas:

- La oficina principal está interconectada mediante la tecnología de conmutación de etiquetas multiprotocolo (Multiprotocol Label Switching - MPLS por sus siglas en inglés). Dicha interconexión se realiza mediante una Red Privada Virtual, suministrado por los proveedores de servicios Bitel, Telefónica del Perú, Optical Network y Global Fiber, suministrando cada uno de dichos proveedores una velocidad de 750 Mb, 1.5 Gb, 400 Mb y 200 Mb, respectivamente.

Por otro lado, con respecto a la seguridad interna, el jefe del área de informática de la oficina principal de Caja Huancayo destacó que, en el periodo enero-julio del año 2021, no se presentaron fallas relacionadas con el Core Campus, el Conmutador de paquetes (*Switch*), el enrutador (*Router*) y el punto de acceso a la Red LAN (*Access Point*).

Asimismo, con respecto a la seguridad externa, el jefe del área de informática de la oficina principal de Caja Huancayo destacó que tampoco se presentaron fallas debido a *software* malintencionado, reconocimiento de usuarios, denegación de servicio a usuarios no deseados o acceso remoto a la red de la agencia principal de Caja Huancayo. Además, añadió que el tipo de protección utilizado para evitar ataques externos es el Antivirus McAfee, el cual se encontraba instalado en cada uno de los equipos de cómputo.

4.1.3. Políticas de seguridad para ataques internos basada en CISCO ISE

La seguridad informática en un contexto de la tecnología CISCO ISE considera dos tipos de ataques: el ataque desde el interior de la entidad que se correspondería con la seguridad informática para ataques internos; y el ataque desde el exterior de la entidad, que se correspondería con la seguridad informática para ataques externos.

La seguridad informática basada en CISCO ISE, para el caso de las Pequeñas y Medianas Empresas – PYMES, grupo empresarial a la cual se ajusta en forma independiente la Caja Huancayo, en un contexto de ataques internos, se corresponde con la noción que tiene CISCO para la seguridad de las denominadas “Redes para una Empresa” o SMB (Small &

Medium Business). Estará compuesta por los siguientes dispositivos o, al menos, por una combinación de ellos: firewall inside, firewall outside, routers de servicios integrados (ISR), switches y familia de productos Wireless.

En la concepción de seguridad informática de CISCO, los dispositivos de capa 2 son aquellos que ofrecen variados servicios; por ejemplo, sobre la LAN cumplirán la función de establecer conexión entre diferentes equipos de la red, así como la capa de distribución. En ese marco de actuación de los dispositivos para la seguridad de las SMB (Small & Medium Business), presentados en el párrafo precedente, el *switch* es el dispositivo indispensable para contrarrestar ataques internos, siendo este el dispositivo de capa 2 más implementado en las redes modernas y que funciona como primera línea de defensa.

Como se mencionó anteriormente, el ataque desde dentro de la entidad se corresponde con la seguridad informática interna; luego, cada uno de los dispositivos que se han citado serán imprescindibles para mejorar los niveles de seguridad de la red. Según los roles que cumplan y las necesidades de cada empresa, algunos dispositivos tendrán un mayor protagonismo.

De lo señalado tanto para la "vulnerabilidad de la política de seguridad para mitigar ataques internos" (cuatro aspectos), como para las "políticas de seguridad para ataques internos (intencionados o inocentes)" (cinco aspectos), se obtuvo un total de nueve aspectos de la seguridad informática que se sometieron a juicio de expertos, utilizando el instrumento concordante con dicha técnica (en Anexo 2, Instrumentos de Recolección de Datos - Variable Dependiente; ver A: Guía Para el análisis mediante juicio de expertos).

Alternativa 1 (A1): la seguridad informática basada en tecnología CISCO ISE.

Alternativa 2 (A2): la seguridad informática actualmente operativa en la agencia principal de Caja Huancayo.

Alternativa 3 (A3): la seguridad informática basada en otra tecnología.

Combinando los nueve aspectos consultados con las tres alternativas se obtuvo 27 propuestas (P) que fueron calificadas por los jueces expertos (10 ingenieros).

Tabla 10

Diseño factorial para las propuestas analizadas mediante juicio de expertos

Categoría: Aspectos de seguridad informática		**Categoría:** Alternativas		
		Alternativa 1	**Alternativa 2**	**Alternativa 3**
Vulnerabilidad de la política de seguridad para mitigar ataques internos	Vulnerabilidad en la protección del conmutador de paquetes (*Switch*).	P1	P2	P3
	Vulnerabilidad en la protección del punto de acceso (Access Point y WLC – Wireless Lan Controller).	P4	P5	P6
	Vulnerabilidades en la protección de Man in The Middle.	P7	P8	P9
	Vulnerabilidades en mitigar la cantidad de dispositivos conectados en los equipos *switch* de acceso (Port-Security).	P10	P11	P12
Políticas de seguridad para ataques internos (intencionados o inocentes)	Políticas de seguridad NAC (Network Access Control).	P13	P14	P15
	Política de seguridad centralizada (Tacacs+ y Radius).	P16	P17	P18
	Política de seguridad de gestión y administración de dispositivos finales.	P19	P20	P21
	Política de Seguridad para visibilidad de la red (visibilidad de los dispositivos usando Microsoft Windows, Mac OS, Linux)	P22	P23	P24
	Política de seguridad basada en el acceso (Cable, Wireless, VPN).	P25	P26	P27

*Nota***.** Elaboración propia.

Para fines de tratamiento de los resultados de la consulta realizada a los expertos (10 ingenieros que participaron en la implementación de CISCO ISE en diversas empresas de Lima), acerca de su apreciación comparativa entre las propuestas. Dichos jueces, basados en su

experiencia en la materia y las tareas que realizan como parte de su práctica profesional, resultaron siendo los más indicados para valorar las propuestas que fueron formuladas. Luego, teniendo en cuenta ello, se pudo establecer la plantilla de preguntas de la encuesta de escala Likert de cinco niveles. En dicha plantilla los jueces dieron su opinión calificando las consultas según el siguiente esquema de calificación:

A: Si se considera la propuesta como «Excelente» (5 puntos en la ponderación).

B: Si se considera la propuesta como «Bueno» (4 puntos en la ponderación).

C: Si se considera la propuesta como «Regular» (3 puntos en la ponderación).

D: Si se considera la propuesta como «Malo» (2 puntos en la ponderación).

E: Si se considera la propuesta como «Pésimo» (1 punto en la ponderación).

De acuerdo a lo señalado, las respuestas de los jueces expertos a la consulta realizada sobre las 27 propuestas (3 alternativas x 9 aspectos de la seguridad informática) fueron las siguientes:

- Excelente, si en la plantilla el juez experto calificó con la letra “A”. Dicha respuesta en la ponderación vale 5 puntos.
- Bueno, si en la plantilla el juez experto calificó con la letra “B”. Dicha respuesta en la ponderación vale 4 puntos.
- Regular, si en la plantilla el juez experto calificó con la letra “C”. Dicha respuesta en la ponderación vale 3 puntos.
- Malo, si en la plantilla el juez experto calificó con la letra “D”. Dicha respuesta en la ponderación vale 2 puntos.
- Pésimo, si en la plantilla el juez experto calificó con la letra “E”. Dicha respuesta en la ponderación vale 1 punto.

En la Tabla 11 se presenta la calificación que hicieron los jueces expertos de cada una de las 27 propuestas (tres alternativas para cada uno de los aspectos de seguridad informática sometidos a consulta).

Tabla 11

Respuesta a las propuestas por parte de los jueces expertos

Jueces Expertos	**Calificación de las Propuestas**																										
	P1	**P2**	**P3**	**P4**	**P5**	**P6**	**P7**	**P8**	**P9**	**P10**	**P11**	**P12**	**P13**	**P14**	**P15**	**P16**	**P17**	**P18**	**P19**	**P20**	**P21**	**P22**	**P23**	**P24**	**P25**	**P26**	**P27**
Juez 1	A	B	E	B	B	B	B	B	C	A	B	C	A	B	B	B	C	C	A	B	A	B	C	B	A	D	C
Juez 2	B	C	C	B	D	D	A	D	C	B	C	E	B	B	D	B	C	D	B	E	A	C	D	C	A	B	C
Juez 3	B	B	E	B	C	B	C	B	D	B	E	E	B	A	D	C	B	C	B	C	A	B	D	C	A	C	E
Juez 4	A	C	D	B	B	B	B	D	C	A	E	D	A	A	B	A	D	C	B	E	A	B	C	D	A	B	D
Juez 5	A	C	C	A	C	B	B	C	C	A	C	B	A	A	B	A	C	B	C	B	A	B	B	C	A	C	B
Juez 6	C	D	C	C	C	D	B	B	B	B	C	C	C	C	D	B	D	D	C	E	B	C	D	C	C	D	D
Juez 7	B	C	C	C	C	C	B	B	D	B	D	C	C	D	C	B	D	D	C	E	B	C	D	E	B	D	B
Juez 8	A	B	B	A	B	C	B	B	B	A	D	C	A	A	B	B	C	C	C	D	A	B	C	C	A	B	B
Juez 9	A	B	C	A	C	B	A	C	C	A	D	B	A	A	D	A	C	C	B	B	A	B	B	C	A	C	B
Juez 10	B	B	C	B	C	E	B	E	C	B	C	C	C	B	E	C	C	D	C	D	B	C	D	C	A	C	B

*Nota***.** Elaboración propia.

En la Tabla 12 se presenta cómo evaluaron los jueces según la escala elegida en la presente investigación.

Tabla 12

Conteo general de las calificaciones de los jueces expertos a las propuestas formuladas

Propuesta	Respuesta de los Jueces Expertos					TOTAL
	Excelente	Bueno	Regular	Malo	Pésimo	
P1	5	4	1	0	0	**10**
P2	0	5	4	1	0	**10**
P3	0	1	6	1	2	**10**
P4	3	5	2	0	0	**10**
P5	0	3	6	1	0	**10**
P6	0	5	2	2	1	**10**
P7	2	7	1	0	0	**10**
P8	0	5	2	2	1	**10**
P9	0	2	6	2	0	**10**
P10	5	5	0	0	0	**10**
P11	0	1	4	3	2	**10**
P12	0	2	5	1	2	**10**
P13	5	2	3	0	0	**10**
P14	5	3	1	1	0	**10**
P15	0	4	1	4	1	**10**
P16	3	5	2	0	0	**10**
P17	0	1	6	3	0	**10**
P18	0	1	5	4	0	**10**
P19	1	4	5	0	0	**10**
P20	0	3	1	2	4	**10**
P21	7	3	0	0	0	**10**
P22	0	6	4	0	0	**10**
P23	0	2	3	5	0	**10**
P24	0	1	7	1	1	**10**
P25	8	1	1	0	0	**10**
P26	0	3	4	3	0	**10**
P27	0	5	2	2	1	**10**

*Nota***.** Elaboración propia.

Por su parte, en la Tabla 13 se presenta la ponderación de las respuestas de los expertos según la escala que se eligió para evaluar.

Tabla 13

Ponderación del conteo general de las calificaciones de los jueces expertos a las propuestas.

Propuesta	**Respuesta de los Jueces Expertos**					**TOTAL**
	Excelente	**Bueno**	**Regular**	**Malo**	**Pésimo**	
P1	25	16	3	0	0	**44**
P2	0	20	12	2	0	**34**
P3	0	4	18	2	2	**26**
P4	15	20	6	0	0	**41**
P5	0	12	18	2	0	**32**
P6	0	20	6	4	1	**31**
P7	10	28	3	0	0	**41**
P8	0	20	6	4	1	**31**
P9	0	8	18	4	0	**30**
P10	25	20	0	0	0	**45**
P11	0	4	12	6	2	**24**
P12	0	8	15	2	2	**27**
P13	25	8	9	0	0	**42**
P14	25	12	3	2	0	**42**
P15	0	16	3	8	1	**28**
P16	15	20	6	0	0	**41**
P17	0	4	18	6	0	**28**
P18	0	4	15	8	0	**27**
P19	5	16	15	0	0	**36**
P20	0	12	3	4	4	**23**
P21	35	12	0	0	0	**47**
P22	0	24	12	0	0	**36**
P23	0	8	9	10	0	**27**
P24	0	4	21	2	1	**28**
P25	40	4	3	0	0	**47**
P26	0	12	12	6	0	**30**
P27	0	20	6	4	1	**31**

*Nota***.** Elaboración propia.

Teniendo en cuenta la ponderación asignada, el rango de variación de las respuestas de los panelistas tuvo los siguientes límites de variación:

- Límite inferior: 10 puntos para el peor de los casos.
- Límite superior: 50 puntos para el mejor de los casos.

Basado la ponderación asumida, se tiene existe una variación de entre 10 y 50 en los puntajes obtenidos; además, se asignó el siguiente criterio de priorización de las propuestas según puntaje:

- Prioridad Alta: Si el puntaje varía entre 37 y 50.
- Prioridad Media: Si el puntaje varía entre 24 y 37.
- Prioridad Baja: Si el puntaje varía entre 10 y 24.

Tomando en cuenta los considerandos señalados en los párrafos anteriores, la evaluación de la ponderación de las respuestas brindada por los jueces expertos a cada una de las propuestas consultadas, permitió establecer el cuadro de calificación e identificación de las prioridades para la implementación de las propuestas.

Tabla 14

Cuadro para la evaluación e identificación de las propuestas formuladas

Prioridad de la propuesta	Rango de pertenencia	Color de identificación
Alta	$38 \leq \text{Valor} \leq 50$	
Media	$25 \leq \text{Valor} \leq 37$	
Baja	$10 \leq \text{Valor} \leq 24$	

*Nota***.** Elaboración propia.

Finalmente, las 27 propuestas (tres alternativas x nueve aspectos de la seguridad informática) fueron evaluadas por procedimientos aritméticos en términos de la ponderación obtenida (ver Tabla 12) y el rango al que se ajusta dicha ponderación (ver Tabla 14).

4.1.3.1. Seguridad informática contra ataques internos basados en CISCO ISE.

De la evaluación del conteo general de las calificaciones de los jueces expertos en función a los rangos establecidos para los puntajes obtenidos para cada una de las formulaciones, se puede advertir que la seguridad interna basada en Cisco ISE obtuvo prioridad alta, en comparación con las otras dos propuestas para la seguridad frente a ataques internos en la oficina principal de Caja Huancayo, en los cinco aspectos consultados.

En la Tabla 15 se presenta la calificación final de cada una de las propuestas para mejorar la seguridad interna en la oficina principal de Caja Huancayo.

Tabla 15

Prioridad en la atención de la seguridad informática frente a ataques internos

Aspecto consultado	Propuesta		Prioridad
Vulnerabilidad en la protección del conmutador de paquetes (*Switch*).	**P1**	Cambiar la Seguridad Informática Interna por otra basada en tecnología CISCO ISE.	**Alta**
	P2	Mantener la Seguridad Informática Interna actualmente operativa en la agencia principal de Caja Huancayo.	**Media**
	P3	Cambiar la Seguridad Informática Interna por otra basada en una tecnología distinta a las anteriores.	**Media**
Vulnerabilidad en la protección del punto de acceso (Access Point y WLC – Wireless Lan Controller).	**P4**	Cambiar la Seguridad Informática Interna por otra basada en tecnología CISCO ISE.	**Alta**
	P5	Mantener la Seguridad Informática Interna actualmente operativa en la agencia principal de Caja Huancayo.	**Media**
	P6	Cambiar la Seguridad Informática Interna por otra basada en una tecnología distinta a las anteriores.	**Media**
Vulnerabilidades en la protección de Man in The Middle.	**P7**	Cambiar la Seguridad Informática Interna por otra basada en tecnología CISCO ISE.	**Alta**
	P8	Mantener la Seguridad Informática Interna actualmente operativa en la agencia principal de Caja Huancayo.	**Media**
	P9	Cambiar la Seguridad Informática Interna por otra basada en una tecnología distinta a las anteriores.	**Media**
Vulnerabilidades en mitigar la cantidad de dispositivos conectados en los equipos *switch* de acceso (Port-Security).	**P10**	Cambiar la Seguridad Informática Interna por otra basada en tecnología CISCO ISE.	**Alta**
	P11	Mantener la Seguridad Informática Interna actualmente operativa en la agencia principal de Caja Huancayo.	**Baja**
	P12	Cambiar la Seguridad Informática Interna por otra basada en una tecnología distinta a las anteriores.	**Media**

*Nota***.** Elaboración propia.

4.1.3.2. Políticas de seguridad para ataques internos (intencionados o inocentes) basados en CISCO ISE. De la evaluación del conteo general de las calificaciones de los jueces expertos en función a los rangos establecidos para los puntajes obtenidos para cada una de las formulaciones, se puede advertir que la seguridad para ataques internos intencionados o inocentes basados en Cisco ISE obtuvo prioridad alta, en comparación con las otras dos propuestas para la seguridad frente a ataques internos en la oficina principal

de Caja Huancayo, solamente en uno de los aspectos consultados, el referido a los ataques de fuga de información.

En la Tabla 16 se presenta la calificación final de cada una de las propuestas para mejorar la seguridad externa en la oficina principal de Caja Huancayo.

Tabla 16

Prioridad en la atención de la seguridad informática frente a ataques internos intencionados o inocentes

Aspecto consultado	Propuesta		Prioridad
Políticas de seguridad NAC (Network Access Control).	**P13**	Cambiar la Seguridad Informática Interna por otra basada en tecnología CISCO ISE.	**Alta**
	P14	Mantener la Seguridad Informática Interna actualmente operativa en la agencia principal de Caja Huancayo.	**Alta**
	P15	Cambiar la Seguridad Informática Interna por otra basada en una tecnología distinta a las anteriores.	**Media**
Política de seguridad centralizada (TACACS+ y RADIUS).	**P16**	Cambiar la Seguridad Informática Interna por otra basada en tecnología CISCO ISE.	**Alta**
	P17	Mantener la Seguridad Informática Interna actualmente operativa en la agencia principal de Caja Huancayo.	**Media**
	P18	Cambiar la Seguridad Informática Interna por otra basada en una tecnología distinta a las anteriores.	**Media**
Política de seguridad de gestión y administración de dispositivos finales.	**P19**	Cambiar la Seguridad Informática Interna por otra basada en tecnología CISCO ISE.	**Media**
	P20	Mantener la Seguridad Informática Interna actualmente operativa en la agencia principal de Caja Huancayo.	**Baja**
	P21	Cambiar la Seguridad Informática Interna por otra basada en una tecnología distinta a las anteriores.	**Alta**
Política de Seguridad para visibilidad de la red (visibilidad de los dispositivos usando Microsoft Windows, Mac OS, Linux)	**P22**	Cambiar la Seguridad Informática Interna por otra basada en tecnología CISCO ISE.	**Media**
	P23	Mantener la Seguridad Informática Interna actualmente operativa en la agencia principal de Caja Huancayo.	**Media**
	P24	Cambiar la Seguridad Informática Interna por otra basada en una tecnología distinta a las anteriores.	**Media**
Política de seguridad basada en el acceso (CABLE, WIRELESS, VPN).	**P25**	Cambiar la Seguridad Informática Interna por otra basada en tecnología CISCO ISE.	**Alta**
	P26	Mantener la Seguridad Informática Interna actualmente operativa en la agencia principal de Caja Huancayo.	**Media**
	P27	Cambiar la Seguridad Informática Interna por otra basada en una tecnología distinta a las anteriores.	**Media**

*Nota***.** Elaboración propia.

4.1.4. Pruebas para la implementación de políticas de seguridad en la infraestructura de la Caja Huancayo en la plataforma de CISCO ISE – Agencia Principal

A fin de poder realizar las pruebas para la implementación de CISCO ISE en la arquitectura actual de Caja Huancayo, fue necesario conocer ciertos protocolos que serán necesarios para poder concluir con la implementación, entre los estándares utilizados se eligió al IEEE 802, el mismo realizó la estandarización del protocolo 802.1x con la finalidad de contar con una solución de control y acceso a la red tomando en consideración que ningún dispositivo malicioso se podría conectar, siendo necesario la previa identificación de los usuarios que quieran conectarse a la red interna.

Para equipos con soporte 802.1x, a través de CISCO ISE existen tres componentes utilizados para la autenticación, los cuales se detallan a continuación:

a. **Suplicante:** se utiliza un suplicante 802.x para la autenticación, autorización y auditoria (AAA), para el caso de Caja Huancayo se utilizó el producto propio de CISCO denominado AnyConnect. Los módulos a utilizar son los siguientes:
    - NAM (Network Access Manager): Control de acceso a la RED.
    - ISE POSTURE: Verifica y evalúa el estado del EndPoint.
b. **Autenticador:** Es el equipo *switch* que recibe la solicitud del suplicante y reenvía una solitud (protocolo de autenticación ampliable) EAP-Request/Identity.
c. **Servidor de autenticación:** CISCO ISE – Servidor Radius.

Para la autenticación se utilizó los protocolos seguros EAP-FAST y EAP-TLS**,** para la implementación de CISCO ISE en la agencia principal de Caja Huancayo.

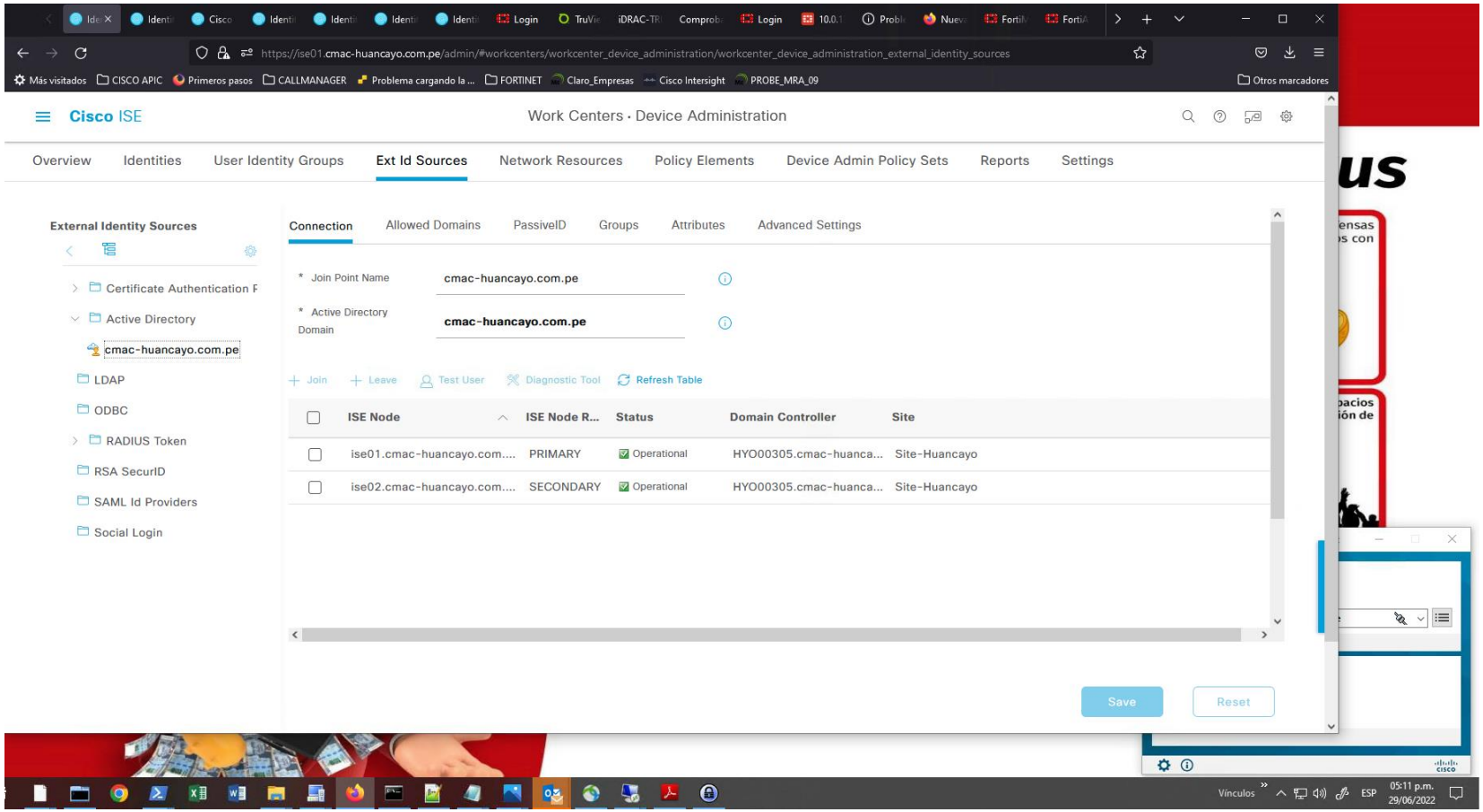
a. EAP- FAST: es la autenticación conformada a través de túneles seguros.
b. EAP-TLS: la autenticación se realiza a través de un certificado SSL, el cual fue firmado por el servidor de la Caja Huancayo.

A través del servidor ISE se habilitó la autenticación por Radius a fin de que pueda recibir las solicitudes de conexión de los distintos usuarios de Caja Huancayo y poder ser visualizados en el entorno web de CISCO ISE.

Previo a ello, fue necesario realizar el registro de los dispositivos de Red y realizar las configuraciones de autenticación, autorización y auditoria (AAA), tal como se puede mostrar en la plataforma CISCO ISE instalada en la oficina principal de Caja Huancayo.

Figura 7

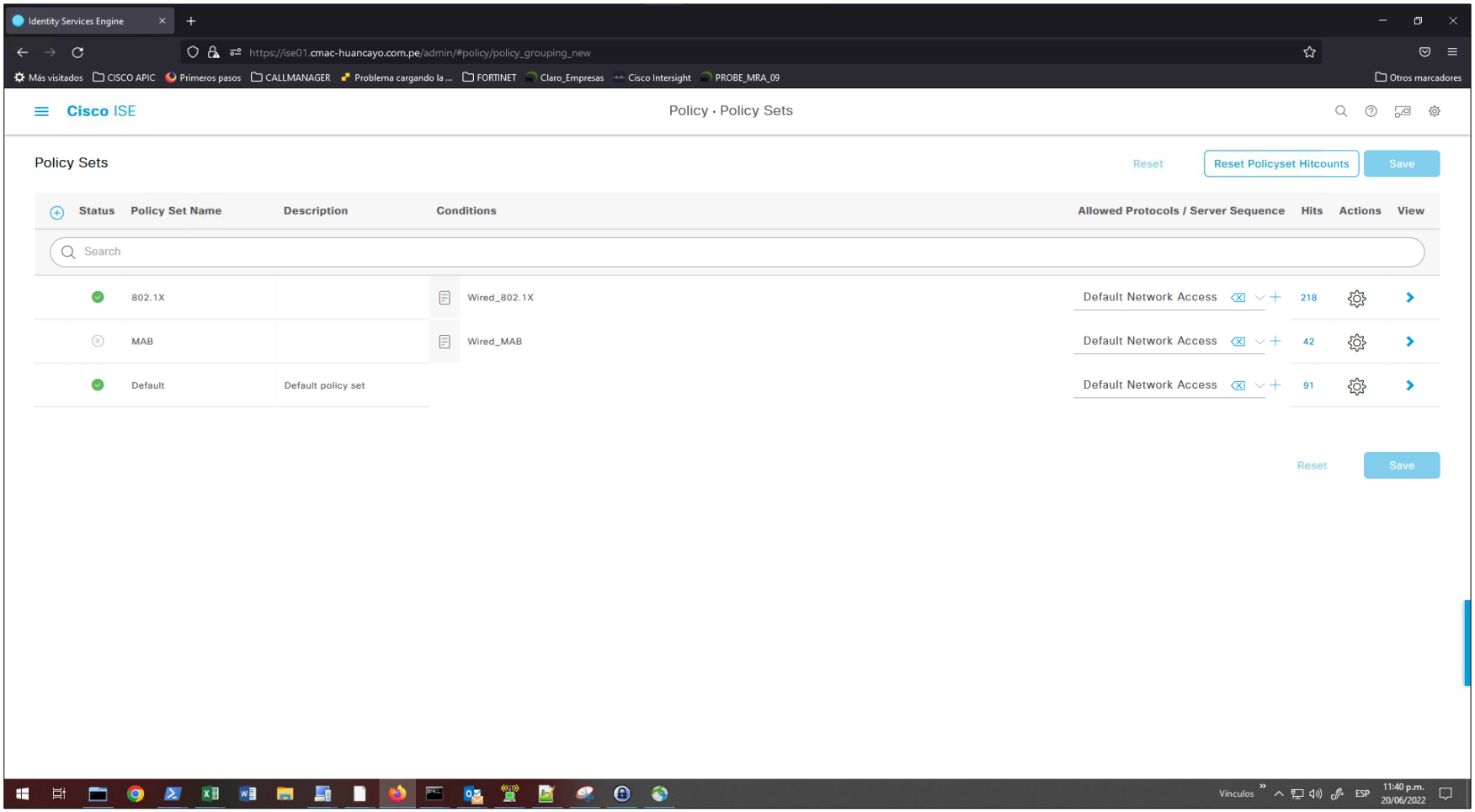
Las Políticas de Seguridad en Cisco ISE versión 3.1. (Conexión con el Directorio Activo)



*Nota***.** Elaboración propia.

Figura 8

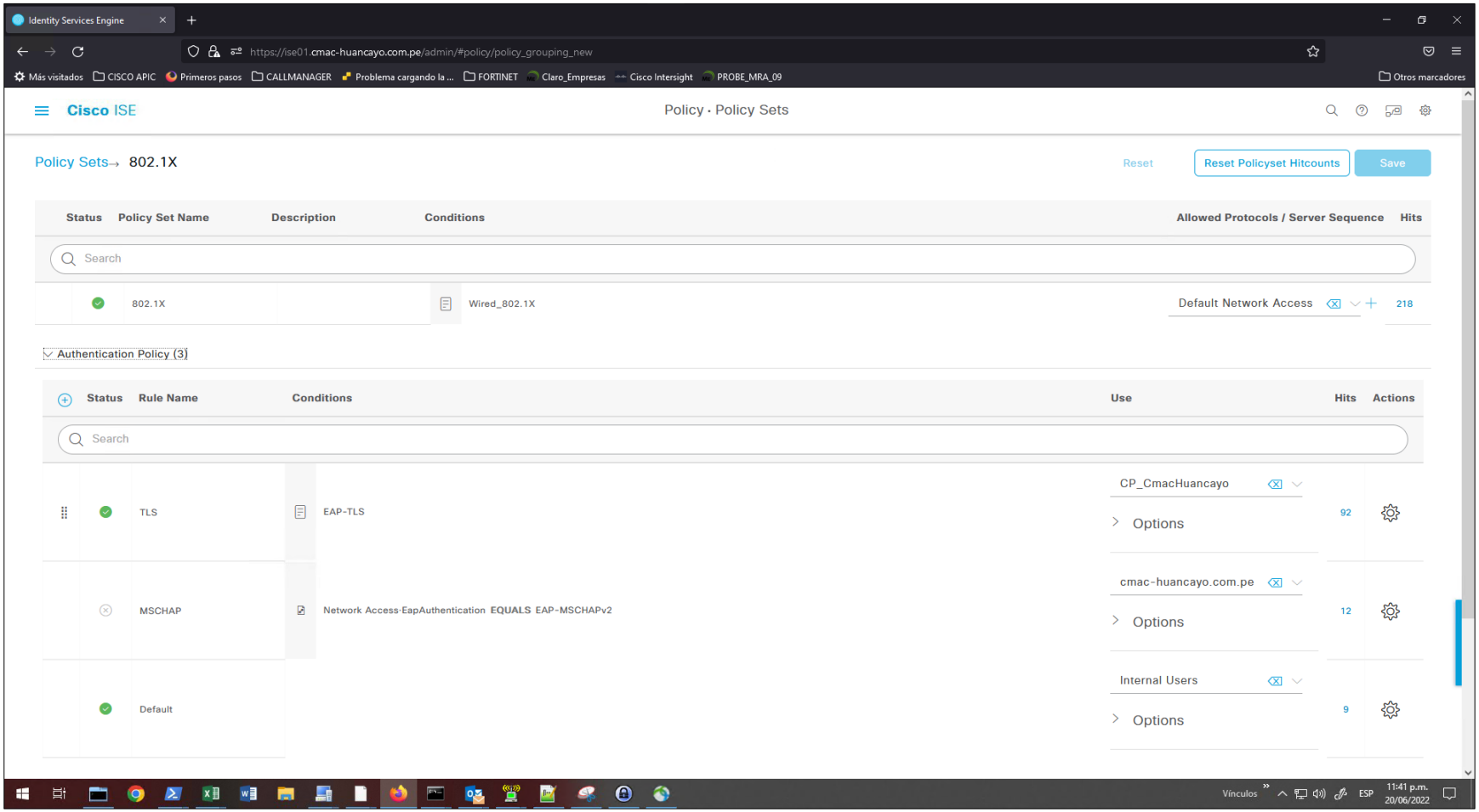
Las Políticas de Seguridad Informática en Cisco ISE versión 3.1. (Protocolo 802.1x Wired)



*Nota***.** Elaboración propia.

Figura 9

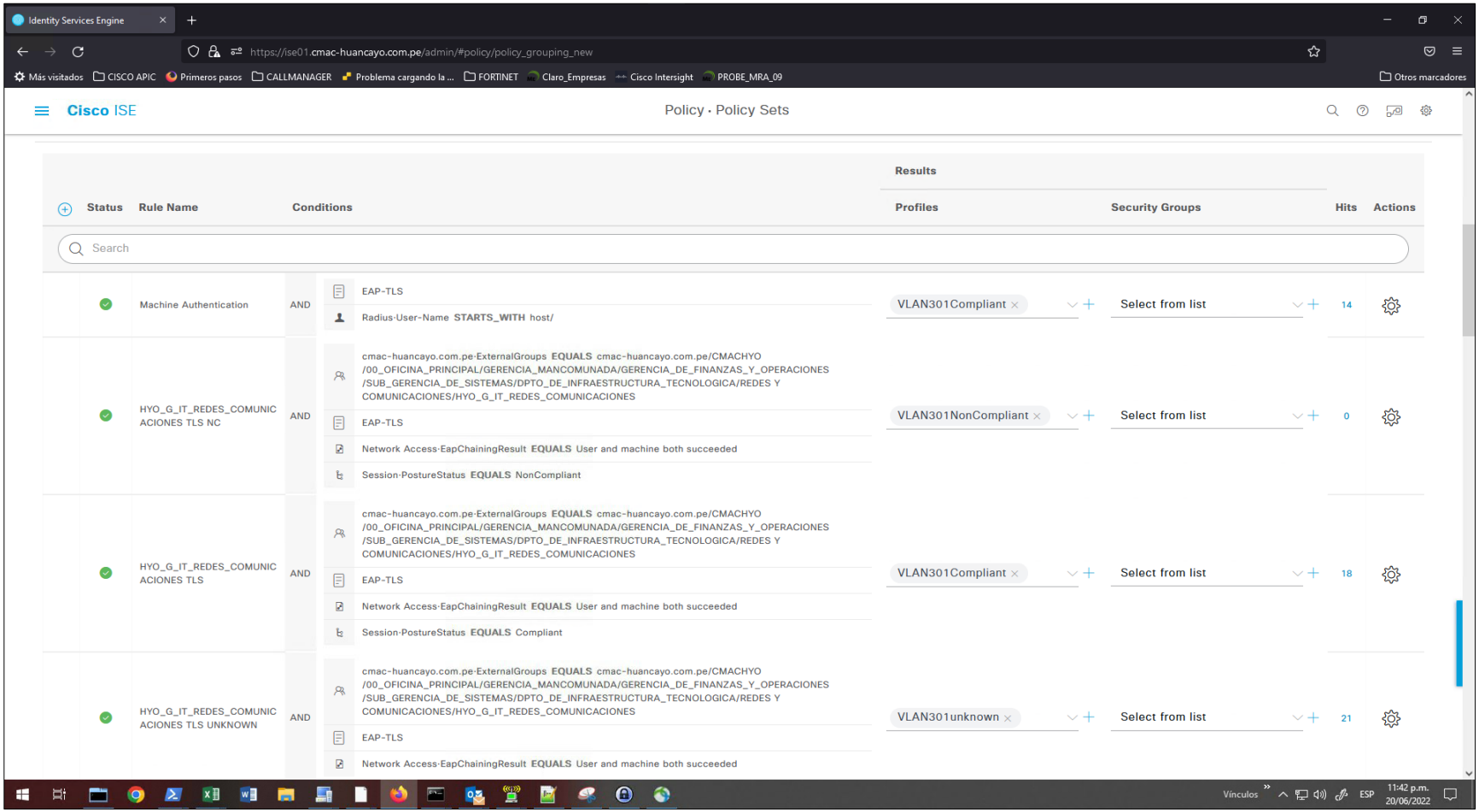
Las Políticas de Seguridad en Cisco ISE versión 3.1. EAP-TLS (Protocolo de Autenticación Ampliable-Transport Layer Security) // Autenticación



*Nota***.** Elaboración propia.

Figura 10

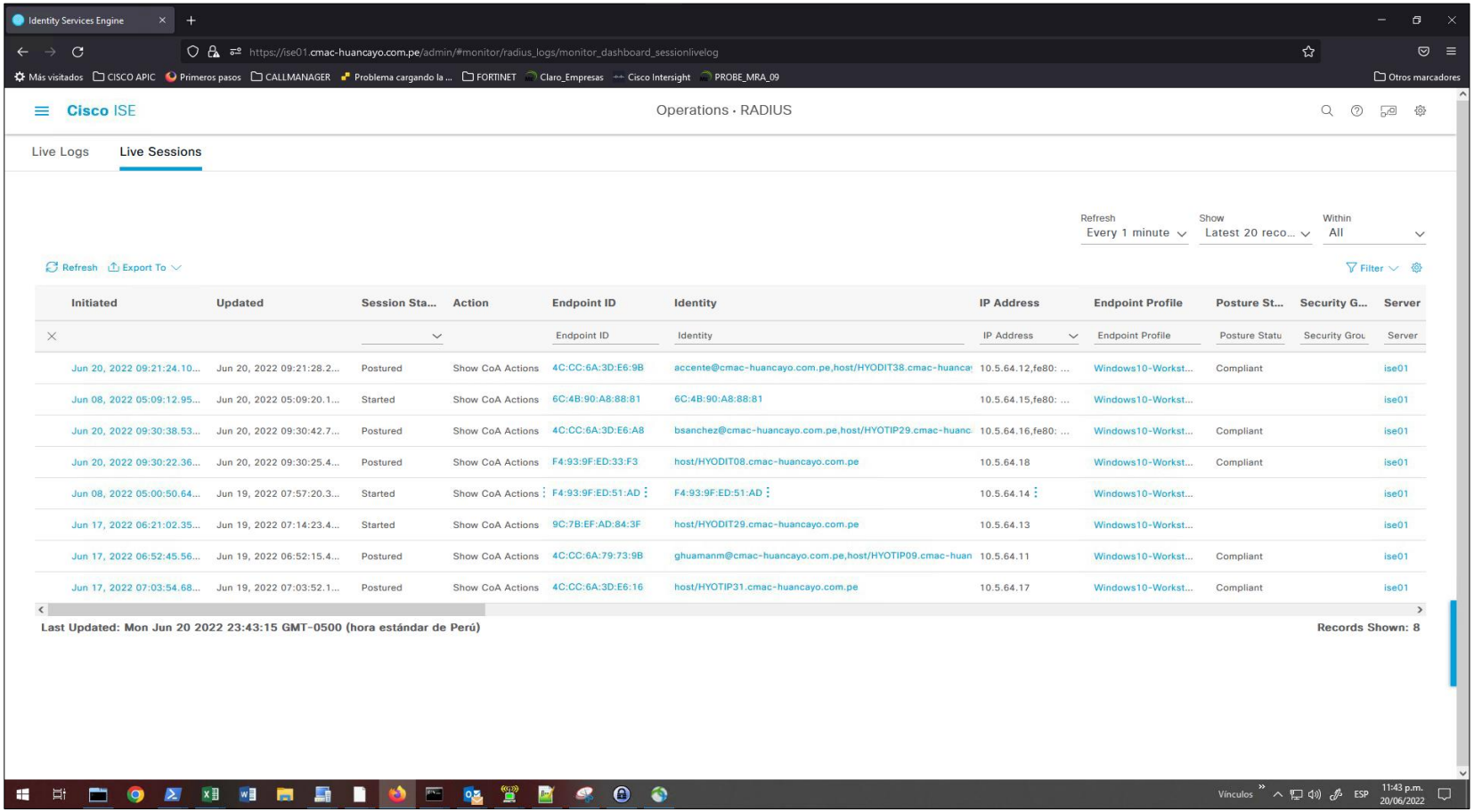
Las Políticas de Seguridad en Cisco ISE versión 3.1. (Unidad Organica / Usuarios de Dominio, EAP-TLS, Postura) // Autorización



*Nota***.** Elaboración propia.

Figura 11

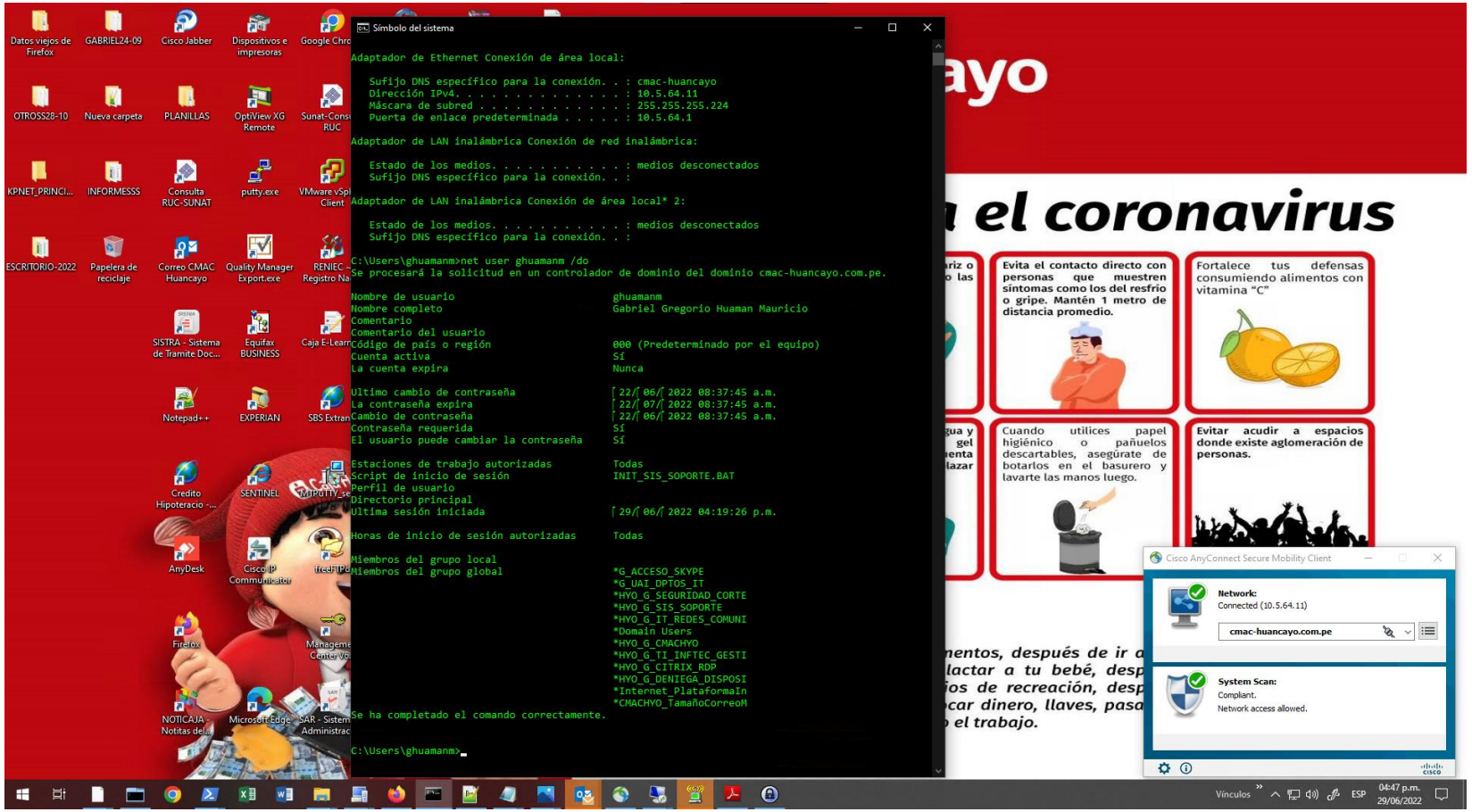
Las Políticas de Seguridad en Cisco ISE versión 3.1. (User Domain: ghuamanm@cmac-huancayo.com.pe/HYOTIP09. Posture: Compliant)



*Nota***.** Elaboración propia.

Figura 12

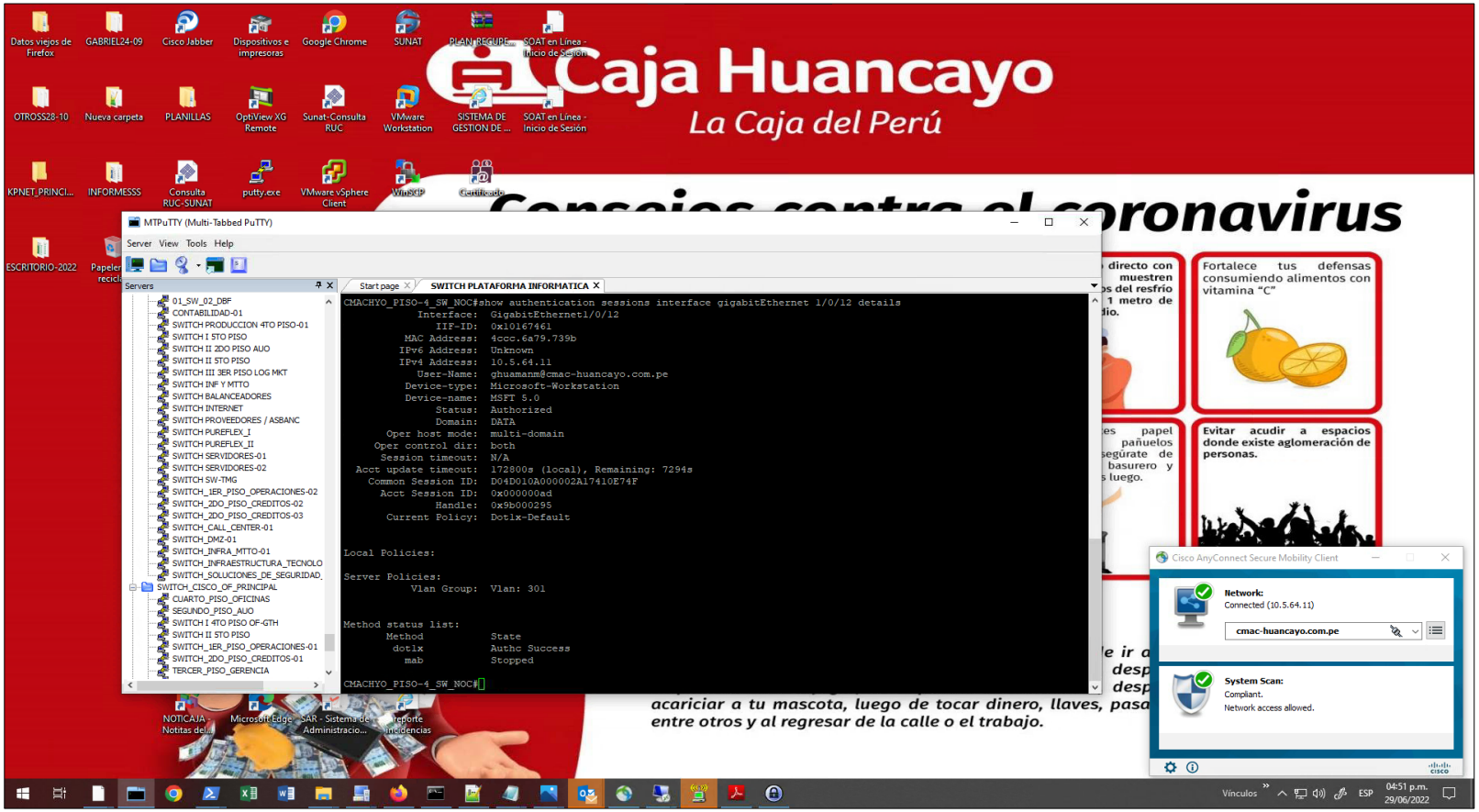
Las Políticas de Seguridad en Cisco ISE versión 3.1. (User Domain: ghuamanm / Permit Access – Host: HYODIT02 IP:10.5.64.11 / Compliant)



*Nota***.** Elaboración propia.

Figura 13

Las Políticas de Seguridad en Cisco ISE versión 3.1. (User Domain: ghuamanm / Method: dot1X Status: Auth / Switch Plataforma Informatica / Port: Gi1/0/12)



*Nota***.** Elaboración propia.

El motor de servicios de identidad de Cisco ISE se integra con fuentes de identidad externas para validar las credenciales en las funciones de autenticación de usuarios y para recuperar información de grupos y otros atributos que están asociados con el usuario para su uso en políticas de autorización. Para tal cometido, se debe configurar la fuente de identidad externa que contiene su información de usuario en Cisco ISE. Se debe recalcar que las fuentes de identidad externas también incluyen información de certificados para el servidor Cisco ISE y los perfiles de autenticación de certificados. Tanto las fuentes de identidad internas como las externas se pueden utilizar como fuente de autenticación para la autenticación del patrocinador y también para la autenticación de usuarios invitados remotos o grupos de usuarios a quienes se les permite el acceso.

En la Figura 13 se muestran las Políticas de Seguridad en Cisco ISE versión 3.1. (Usuarios de Dominio, EAP-TLS, Postura) // Autorización en la plataforma CISCO ISE de la oficina principal de Caja Huancayo.

Luego de las configuraciones realizadas se tomó un área DEMO a fin poder verificar el comportamiento de esta nueva solución, para lo cual se realizaron dichas pruebas con el área de Redes y Comunicaciones, en donde se observa que las pruebas realizadas fueron exitosas. Cabe precisar que luego de las pruebas realizadas se procederá con el despliegue de la autenticación por medio del protocolo 802.1x a las demás oficinas de la agencia principal de Caja Huancayo.

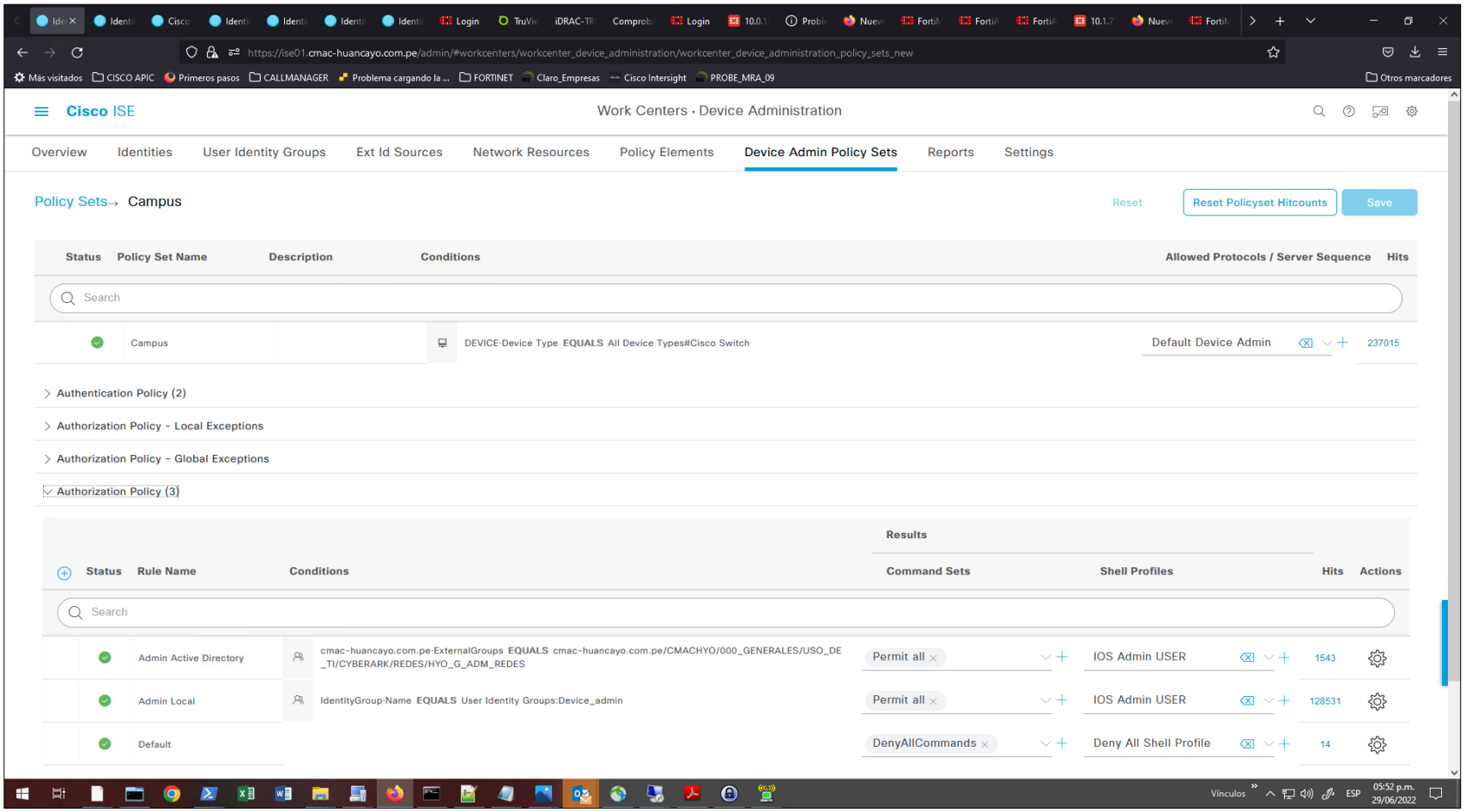
En la Figura 13 se muestra el acceso permitido al usuario en la plataforma Cisco ISE versión 3.1. de la oficina principal de Caja Huancayo.

4.1.5. Pruebas para la implementación de políticas de seguridad de gestión y administración AAA (autenticación, autorización y auditoria) – Servidor TACACS con CISCO ISE

A fin de poder habilitar la característica Device Admin “TACACS” de CISCO ISE a través de las políticas de gestión y administración sobre la base de roles por usuarios, para lo cual fue necesario identificar los usuarios que administran los distintos dispositivos de red, de acuerdo a la identificación se procede a habilitar los privilegios de solo Lectura / Lectura y Escritura, a través del Directorio Activo se invoca al grupo HYO_G_ADM_REDES.

Figura 14

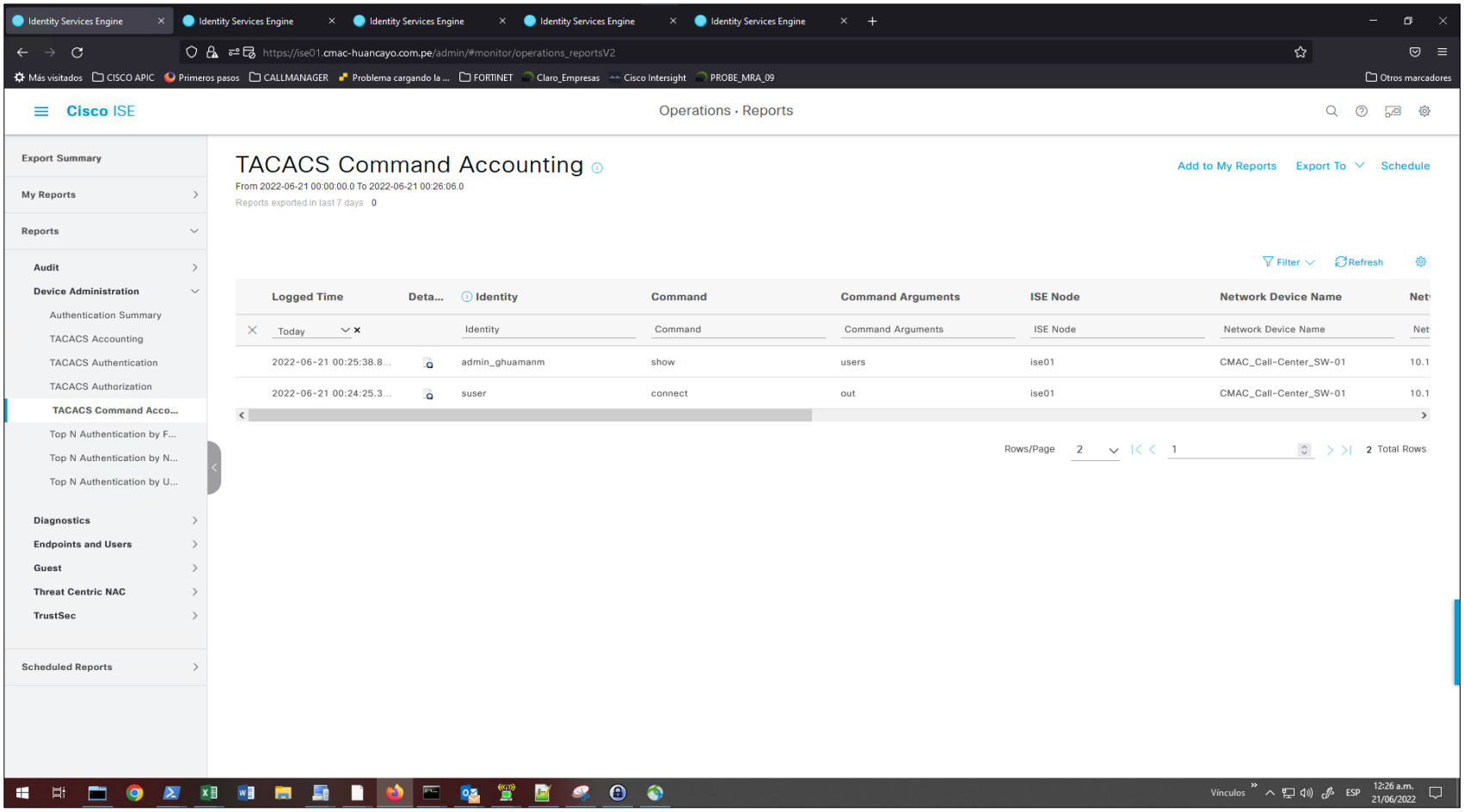
Las Políticas de Seguridad en Cisco ISE versión 3.1. (TACACS / Se procede a asociar al grupo con privilegios de administración a la plataforma CISCO ISE)



*Nota***.** Elaboración propia.

Figura 15

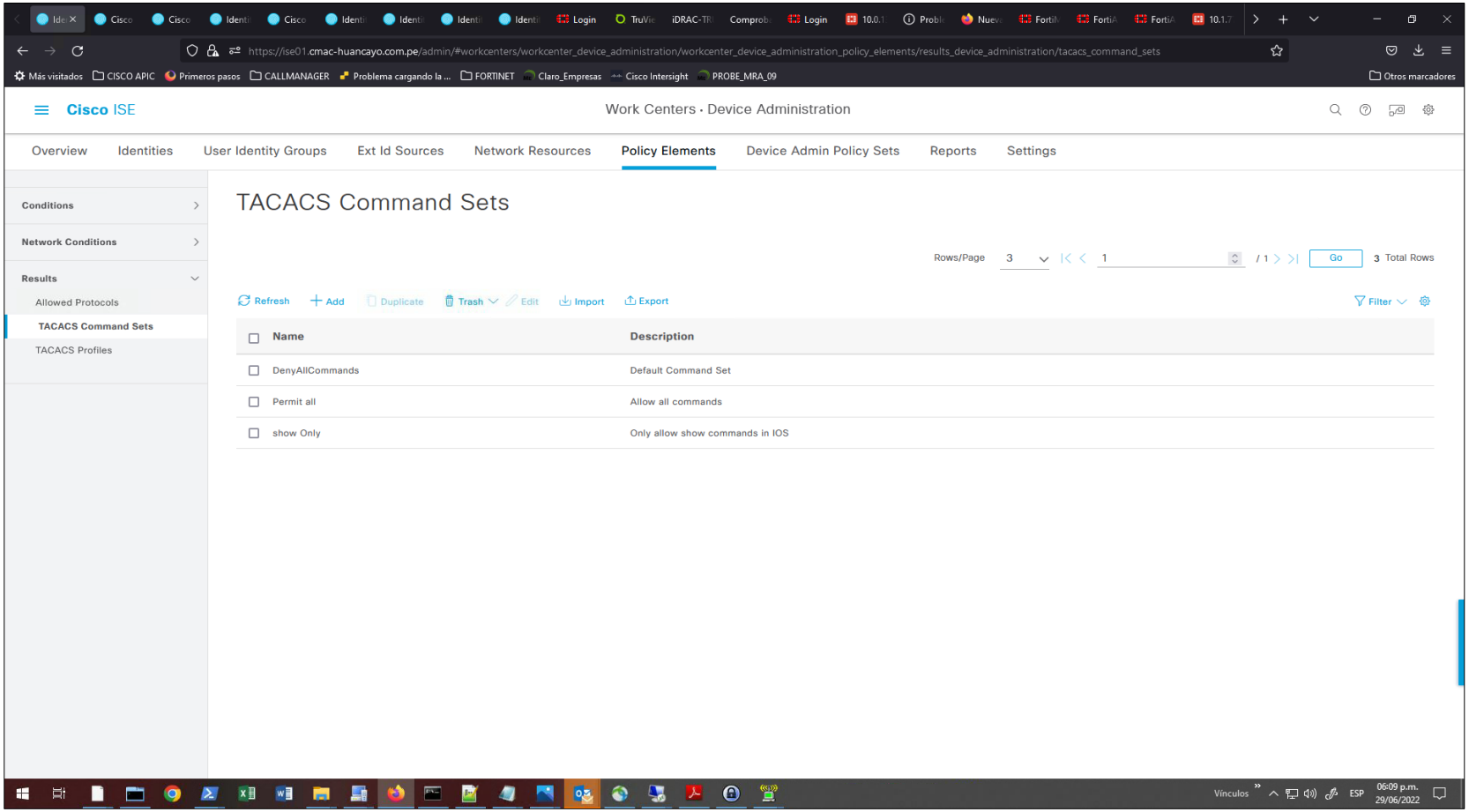
Las Políticas de Seguridad Informática – PSI en Cisco ISE versión 3.1. (User Domain: admin_ghuamanm / Permit Access Device Admin)



*Nota***.** Elaboración propia.

Figura 16

Las Políticas de Seguridad Informática – PSI en Cisco ISE versión 3.1.(DEVICE ADMIN TACACS – AAA / Command Set)



*Nota***.** Elaboración propia.

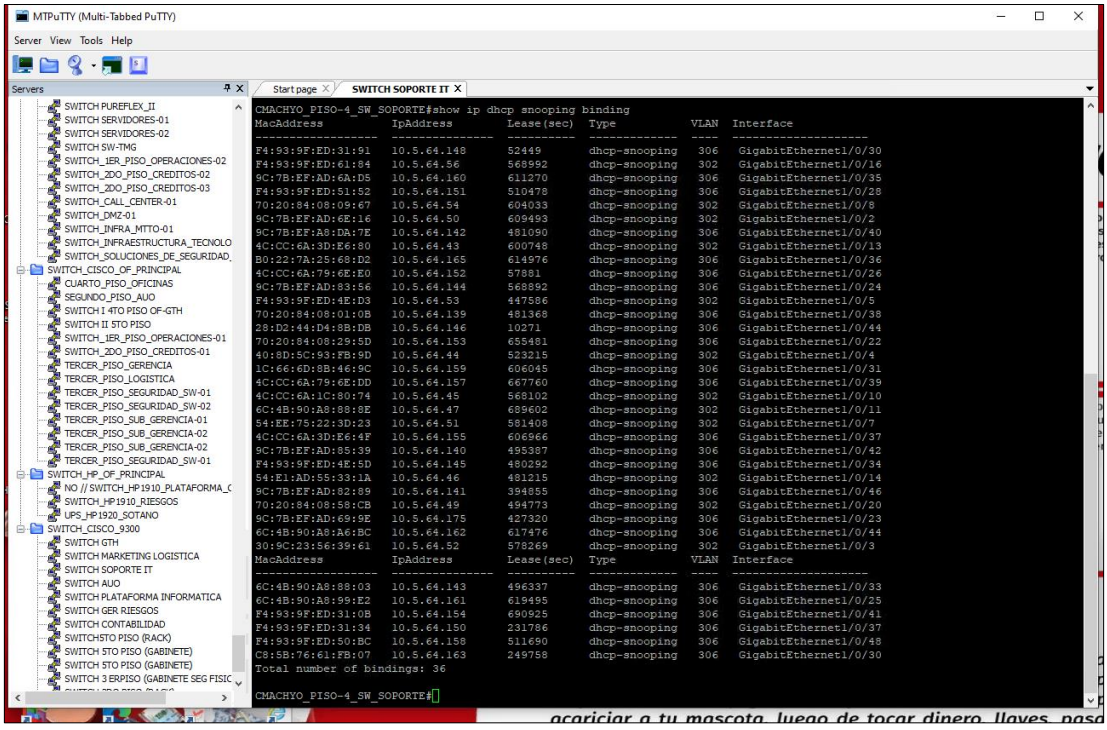
4.1.6. Pruebas para la implementación de seguridad para protección Man in The Middle en los equipos Swich'es de acceso

La vulnerabilidad conocida como Man in The Middle a nivel de los equipos *switch* tiene la principal característica de suplantar el servidor DHCP y el atacante pueda tomar control de los equipos que se interconectan a la Red interna. Este tipo de ataque opera en la capa 2 del modelo OSI (Enlace de Datos). Con la finalidad de prevenir dicha vulnerabilidad se procede a realizar las configuraciones necesarias en los equipos *switches* de acceso, lo cual se procede a habilitar las siguientes características de seguridad.

a. DAI (Dinamic ARP Inspection): esta característica previene la suplantación de direcciones IP's en la capa 2 del modelo OSI.
b. DHCP Snooping: esta característica permite que un *switch* pueda inspeccionar el tráfico DHCP.

Figura 17

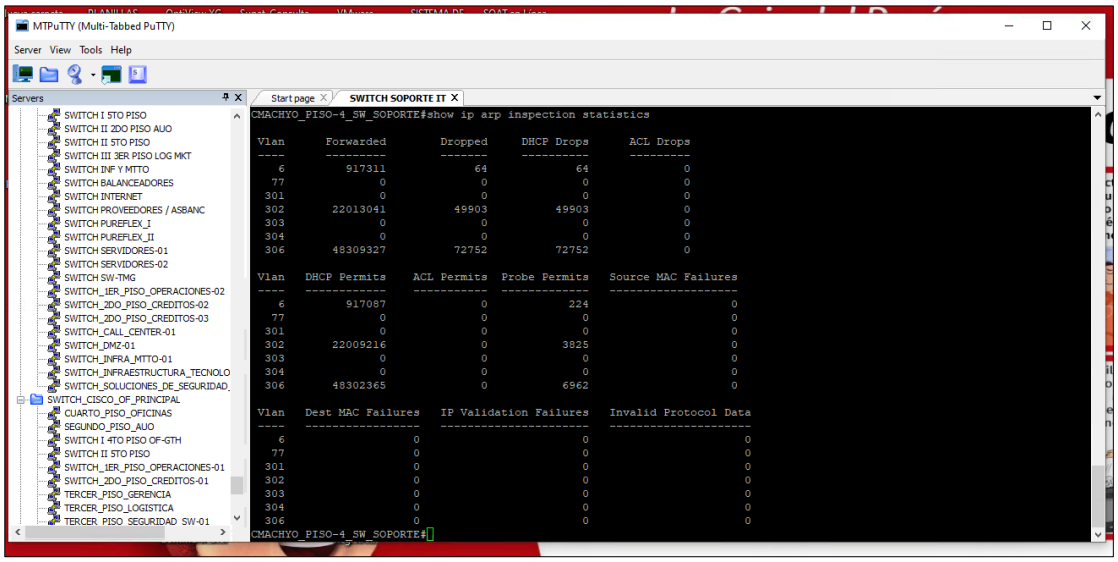
Las evidencias de configuración de la característica de seguridad ARP-INSPECTION



Nota. Elaboración propia**.**

Figura 18

Evidencias de configuración de la característica de seguridad DHCP SNOOPING

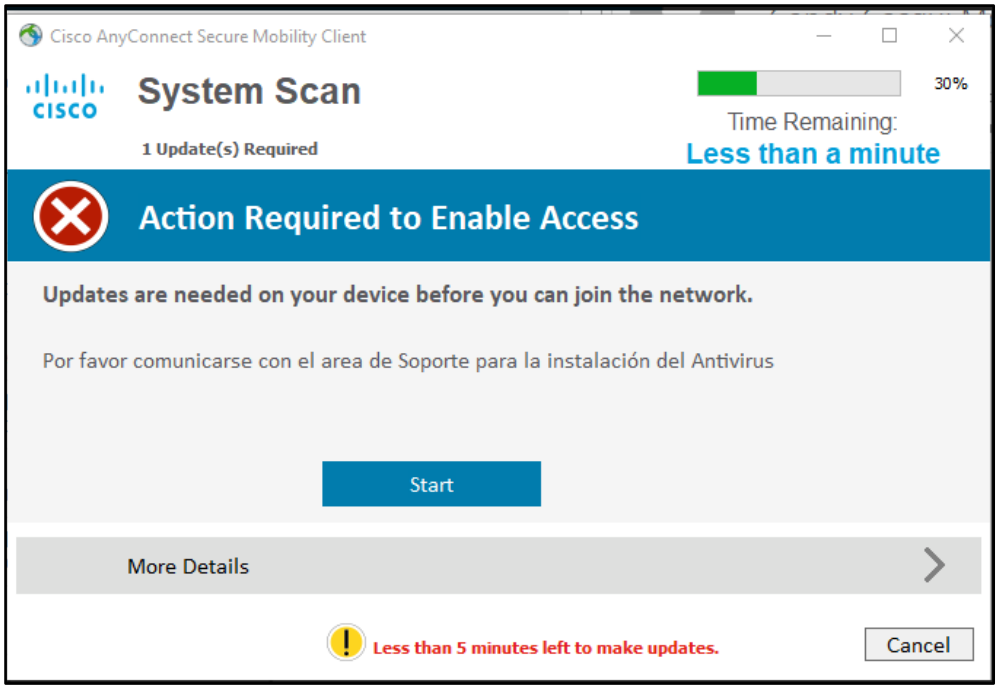


Nota. Elaboración propia**.**

En resumen, la Caja Huancayo actualmente cuenta con servidor de Directorio Activo, el mismo brinda el acceso a la red a los usuarios de acuerdo a cada unidad organizativa, en donde cada usuario que se autentica a la Red LAN sin ninguna validez de seguridad, lo cual es un riesgo que pueda filtrase algún virus interno y pueda afectar la Red LAN. Es por esta razón que se planteó la propuesta de implementación de CISCO ISE con la finalidad que dicha solución pueda brindar una autenticación de manera segura rigiendo que cualquier equipo de cómputo que quiera conectarse a la RED deberá cumplir con ciertos perfiles de seguridad para que este pueda tener el acceso a la red, tal como se muestra a continuación:

Figura 19

Políticas de seguridad cuando un equipo no cumple los perfiles de seguridad

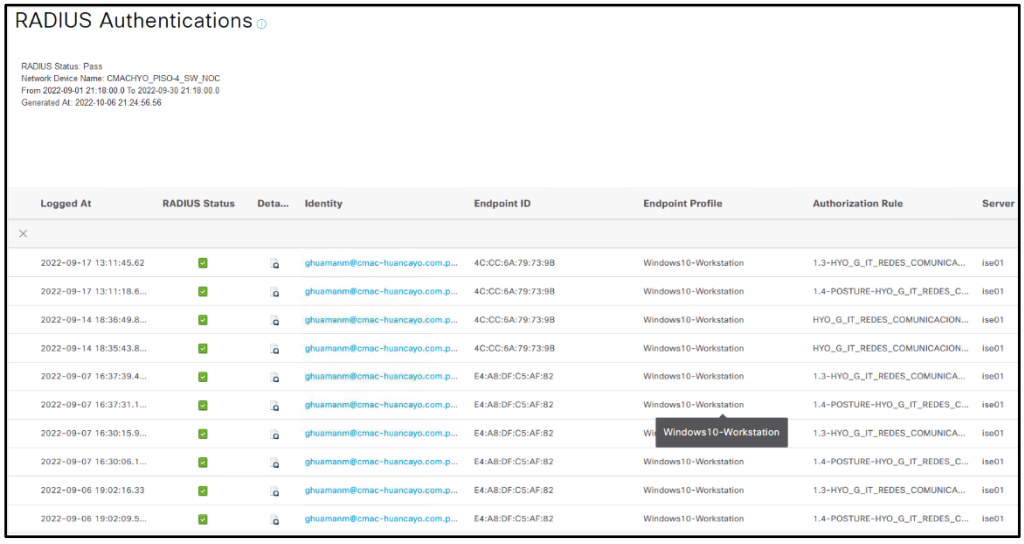


Nota. Elaboración propia**.**

Con la propuesta de implementación también se cuenta con reportes de autenticación de los usuarios que son necesarios ante cualquier auditoría interna o externa. De acuerdo a lo indicado se puede verificar que ha mejorado en el aspecto de autenticación de los usuarios de la Caja Huancayo.

Figura 20

Evidencias de configuración de la característica de seguridad DHCP Snooping



Nota. Elaboración propia

4.1.7. Antes y después de las pruebas de políticas de seguridad mediante Cisco ISE

En el siguiente cuadro se hallan las vulnerabilidades corregidas mediante la tecnología de seguridad Cisco ISE.

Tabla 17

Antes y después de las pruebas de políticas de seguridad mediante Cisco ISE

Pruebas de políticas de seguridad en los departamentos de Marketing y Infraestructura Tecnológica de la oficina principal de la Caja Huancayo	
Vulnerabilidades encontradas (antes)	**Vulnerabilidades corregidas (después)**
Vulnerabilidad en la protección del conmutador de paquetes (*switch*).	Políticas de seguridad para permitir la habilitación de protocolos seguros.
Vulnerabilidad en la protección del punto de acceso (Access Point y WLC – Wireless Lan Controller).	Políticas de seguridad para permitir la habilitación de protocolos seguros.
Vulnerabilidades en la protección de Man in The Middle.	Se realizó la reconfiguración de los equipos *swiches* a fin de mitigar ataques.
Vulnerabilidades en mitigar la cantidad de dispositivos (PORT-Security).	Políticas de seguridad para poder tener una visibilidad de los equipos de cómputo y usuarios que se autentican a la red LAN.

*Nota***.** Elaboración propia.

4.2. Discusión de resultados

De la evaluación del conteo general de las calificaciones de los jueces expertos en función a los rangos establecidos para los puntajes obtenidos para cada una de las formulaciones, se puede advertir que la seguridad interna basada en Cisco ISE obtuvo prioridad alta en siete aspectos consultados. Dichos resultados, en comparación con las otras dos propuestas para la seguridad frente a ataques internos en la oficina principal de Caja Huancayo, permitió establecer una propuesta de políticas de seguridad basado en CISCO ISE para ataques internos.

Luego de haber realizado las pruebas de implementación de políticas de seguridad en la Red LAN de los departamentos de Marketing e Infraestructura Tecnológica, se logró optimizar la seguridad interna, permitiendo contar con una visibilidad de los usuario y equipos que se conectan a la Red LAN, a través de los protocolos 802.1X, AAA (Authentication, Authorization, Accounting) y Radius. Para ello será necesaria la instalación de un agente en cada PC, denominado Cisco Anyconnect para los módulos de NAM (Network Access Manager) e ISE POSTURE. Así mismo, al nivel de los equipos *switches* de acceso se logró habilitar ciertas características de seguridad a fin de mejorar la seguridad de estos equipos.

La propuesta de políticas de seguridad se sustenta en las bondades y ventajas comparativas ofrecidas por la tecnología CISCO ISE, tanto para mitigar ataques internos como para ataques internos (intencionados o inocentes). Dichas bondades y ventajas se obtuvieron mediante la técnica del análisis documentario, cuyo instrumento se presenta en anexos (en Anexo 2, Instrumentos de Recolección de Datos - Variable Dependiente; ver B: Guía para el análisis documentario).

Las pruebas de implementación de políticas de seguridad consisten en establecer lineamientos a seguirse. Además, esta constituye un proceso técnico-administrativo que “debe abarcar toda la organización, sin exclusión alguna; ha de estar fuertemente apoyado por el sector gerencial, ya que, sin ese apoyo, las medidas que se tomen no tendrán la fuerza necesaria” (30). Por otro lado, se deberá tener en cuenta que este “trae aparejados varios tipos de problemas que afectan el funcionamiento de la organización. La implementación de un sistema de seguridad conlleva a incrementar la complejidad en la operatoria de la organización, técnica y administrativamente” (30).

Los hallazgos permiten concluir que la implementación de políticas de seguridad para la Red LAN de Caja Huancayo basado en la tecnología informática Cisco ISE (Identity Services Engine), será un acierto. Este resultado concuerda con lo indicado en la hipótesis de investigación: “Las pruebas de implementación de políticas de seguridad basado en la tecnología informática Cisco ISE (Identity Services Engine) optimiza la seguridad en la Red

LAN en los departamentos de Marketing e Infraestructura tecnológica de la agencia principal de Caja Huancayo". Por tanto, la hipótesis de investigación es aceptada.

Bermúdez y Bailón (2015), en su tesis desarrollada en el contexto ecuatoriano, realizaron un análisis de seguridad informática y seguridad de la información basado en la norma ISO/IEC 27001. Como sostienen los autores, Credigestión ha mostrado cómo los activos de información de todas aquellas áreas críticas, y, en general, la seguridad de la red, están en una situación de riesgo potencial, lo que puede devenir en robos de información y daños a la red, y posteriormente ello puede redundar en la organización. Dicho lo cual, ello se debe, en parte, a la falta de aplicación de la ISO/IEC 27001. Con respecto al presente trabajo de tesis, Cisco ISE cumple con la norma indicada al establecer parámetros de seguridad como asegurar la confidencialidad e integridad de la información de los colaboradores de Caja Huancayo.

Del antecedente de Jiménez y Urban (2015), autores cuyo objeto de estudio fue llevar a cabo una migración de servicios, ello permitió que se observara, con mayor especificación, a aquellos dispositivos y usuarios que quieren hacer uso de este recurso en las instalaciones, asegurando que todo aquel que no pertenece a la dependencia no pueda ingresar.

Dichos resultados se relacionan con el presente proyecto de tesis, pues se sostiene que Cisco ISE brinda el acceso seguro y controlado para contar con una visibilidad de usuarios y equipos que se conectan a la Red LAN.

Conclusiones

De la encuesta a los 10 expertos de seguridad informática que laboran en empresas establecidas en la ciudad de Lima, resultó que la tecnología de seguridad CISCO ISE debería ser utilizada; para ello se realizó un análisis de los datos por prioridades alta, media y baja, con ayuda del *software* Microsoft Excel. A partir del análisis se obtuvo que la propuesta de implementación debería realizarse con la tecnología de seguridad CISCO ISE, debido a que consiguió la prioridad más alta en siete aspectos y prioridad media en dos aspectos de la encuesta realizada.

Se determinó las vulnerabilidades de las políticas de seguridad para mitigar ataques internos en la Red LAN de la agencia principal de Caja Huancayo, las cuales se detallan a continuación:

- La protección del conmutador de paquetes (*switch*) no cuenta con un control de los puertos y protocolos.
- La protección del punto de acceso (Access Point y WLC – Wireless LAN Controller) no cuenta con un control centralizado para la gestión y administración.
- Se identificó que los *Ssitches* se encontraron inmersos ante un ataque Man in The Middle, el cual genera ataques al servidor DHCP.
- Se identificó que los puertos de los *switches* no cuentan con un límite de direcciones MAC address registrados.

Se determinaron las políticas de seguridad para ataques internos (intencionados o inocentes) basado en Cisco ISE, las cuales se pueden implementar en la Red LAN, en las pruebas en los departamentos de Marketing e Infraestructura Tecnológica en la agencia principal de Caja Huancayo. Dicha información se detalla a continuación:

- Se logró implementar políticas de seguridad NAC (Network Access Control) en las pruebas, lo que autenticará a los equipos y usuarios mediante las características de postura y remediación. Su objetivo es verificar si la PC cumple con el perfil para el acceso a la red, tomando como condición la actualización de la firma del antivirus McAfee.
- Se logró implementar políticas de seguridad centralizada (TACACS+ y RADIUS) en las pruebas, con lo cual se tendrá el control de las PCs y terminales como *switches*.
- Se logró implementar políticas de seguridad para la gestión y administración de dispositivos a través del protocolo TACACS (sistema de control de acceso del controlador de acceso a terminales) en las pruebas, tales como *switches* de acceso, Core Campos, Core Datacenter, WLC (Wireless Lan Controller) que actualmente Caja Huancayo posee.

- Se logró implementar políticas de seguridad basadas en los distintos sistemas operativos que existen en la actualidad en las pruebas. En el caso de Caja Huancayo, se permitirá que únicamente las PCs con sistemas operativos Windows 10 puedan autentificarse.
- Se logró implementar políticas de seguridad basadas en el acceso (Cable, Wireless, VPN) en las pruebas. En el caso de Caja Huancayo, se habilitará la visibilidad de los equipos y usuarios que se autentican a través de la red cableada (quién, cómo, qué y dónde se conectó).

Se elaboró la propuesta de implementación de políticas de seguridad para la Red LAN de Caja Huancayo, basada en la tecnología informática Cisco ISE (Identity Services Engine), lo que permitirá optimizar la seguridad interna en la agencia principal de Caja Huancayo.

Recomendaciones

Se recomienda realizar el despliegue de las políticas de seguridad en todas las oficinas administrativas de la agencia principal de Caja Huancayo.

Se recomienda implementar políticas de seguridad basadas en equipos inalámbricos para fortalecer el acceso no autorizado a la red de Caja Huancayo.

Se recomienda documentar toda la fase de la propuesta de implementación de la herramienta de seguridad CISCO ISE. Esto ayudaría a disminuir el margen de error y evitar contratiempos para el despliegue de nuevas políticas de seguridad.

Se recomienda actualizar las políticas de seguridad basado en la tecnología CISCO ISE, debido a que cumple con la norma ISO 27001, el cual proporciona un marco de seguridad más óptimo para el aseguramiento, confidencialidad e integridad de la información y, a su vez, es adaptable a cualquier tipo de organización. (31)

Referencias bibliográficas

Agencia de Gobierno Electrónico y Sociedad de la Información y del Conocimiento. (2021). Glosario de términos de ciberseguridad. Disponible en: https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/book/6034/download

Alcócer, A. (2000). *Redes de computadoras (2da Edición).* Lima : Editorial Infolink.

Alonso, I. (2013). *Análisis comparativo de dos protocolos para control de acceso y administración de equipos de telecomunicaciones* (Tesis de Grado, Universidad Católica de Colombia). https://repository.ucatolica.edu.co/bitstream/10983/812/2/ANALISIS%20COMPARATIVO%20DE%20DOS%20PROTOCOLOS%20PARA%20CONTROL%20DE%20ACCESO%20Y%20ADMINISTRACION%20DE%20EQUIPOS%20DE%20TELECOMUNICACIONES%20Final.pdf

Ayudaley**.** (2021). Ataque Man in the middle: Características, tipos y ejemplos. Disponible en: https://ayudaleyprotecciondatos.es/2021/07/15/ataque-man-in-the-middle/

Barboza, A., Medina, A., & Nip, I. (2007). *Enlace VPN para transporte de voz y datos. Caso: Master Equip C.A.* (Tesis de Grado, Universidad Dr. Rafael Belloso Chacín). Disponible en: https://virtual.urbe.edu/tesispub/0080297/

Benchimol, D. (2010). *Redes Cisco: Instalación y administración de hardware y software.* Banfield – Argentina : Editorial GRADI.

Benites, C**.** (2019). *Implementación de un Sistema de Gestión de Seguridad de la Información -Norma ISO 27001 para la Fábrica Radiadores Fortaleza*. (Tesis de grado, Universidad Tecnológica del Perú). Disponible en: https://repositorio.utp.edu.pe/bitstream/handle/20.500.12867/1933/Cesar%20Benites_Tesis_Titulo%20Profesional_2019.pdf?sequence=1&isAllowed=y

Bermúdez, K., & Bailón, E. (2015). *Análisis en Seguridad Informática y Seguridad de la Información basado en la Norma ISO/IEC 27001- Sistemas de Gestión de Seguridad de la información dirigido a una Empresa de servicios Financieros*. (Tesis de grado, Universidad Politécnica Salesiana). Disponible en: https://dspace.ups.edu.ec/handle/123456789/10372

Borghello, C. (2021). Implementación de una Política de Seguridad. Disponible en: https://www.segu-info.com.ar/politicas/implementacion

Caja Huancayo. (2020). Memoria Anual. Disponible en: https://www.smv.gob.pe/ConsultasP8/temp/Memoria%202019%20-%201.pdf

Caja Huancayo. (2021). Nuestra Historia. Disponible en: https://www.cajahuancayo.com.pe/PCM_NuesCaja/PCM_frmHistoria.aspx

Calderón, J. (2019). *Seguridad de la Información y la Gestión de Riesgos en los trabajadores de la DIGERE del Ministerio de Educación, 2018*. (Tesis de grado, Universidad César Vallejo). Disponible en: https://repositorio.ucv.edu.pe/bitstream/handle/20.500.12692/30014/Calder%c3%b3n_SJA.pdf?sequence=1&isAllowed=y

CISCO. (2021). ¿Qué es la seguridad de red? Disponible en: https://www.cisco.com/c/es_mx/products/security/what-is-network-security.html

CLASS & Asociados S.A. (2021). Fundamentos de Clasificación de Riesgo: Caja Municipal de Ahorro y Crédito de Huancayo S.A. Disponible en: https://www.smv.gob.pe/ConsultasP8/temp/CLASS%20Fund.pdf

Coutinho, N. (2017). How IT Works Cisco Identity Services Engine. *En: Canal de Youtube CDW People Who Get IT*. Disponible en: https://www.youtube.com/watch?v=cXde4AAnO7o

DataCom Global. (2016). Cisco ISE: Una nueva manera de proteger y administrar los cambios en su Red. *En: Datacom.Global.* Disponible en: https://datacom.global/cisco-ise-proteger-y-administrar-cambios-en-su-red/

EL Comercio. (2022). Perú recibió 5,2 mil millones de intentos de ciberataques en la primera mitad de 2022. *En: Actualidad/Noticias.* [Citado el: 22 de Octubre de 2022.] Disponible en: https://elcomercio.pe/tecnologia/actualidad/ciberseguridad-peru-recibio-52-mil-millones-de-intentos-de-ciberataques-en-la-primera-mitad-de-2022-cibercriminales-espana-mexico-colombia-argentina-noticia/?ref=ecr

Fireeye**.** (2022). Ataques en tiempo real. *En: fireeye.* [En línea] 2022. Disponible en: https://www.fireeye.com/cyber-map/threat-map.html

Flynn, P., House, F., & Shah, R. (2022). Election Phishing Attacks Target Election Workers. *En: News & Stories: Keeping you informed.* [Citado el: 20 de Octubre de 2022.] Disponible en: https://www.trellix.com/en-us/about/newsroom/stories/research/2022-election-phishing-attacks-target-election-workers.html

Garzón, H., & Bernal, H. (2021). *Implementación y migración de redes corporativas con CISCO DNA Center*. (Tesis de Grado, Universidad Santo Tomas). Disponible en: https://repository.usta.edu.co/handle/11634/33368

Guerrero, J. (2017). *Desarrollo e Implementación de Políticas de Seguridad Informática aplicando el estándar ISO/IEC 27002 para el Departamento de Sistemas de una Empresa del Sector Farmacéutico de Ecuador*. *En: Repositorio dspace.* (Tesis de grado, Escuela Superior Politécnica del Litoral. Guayaquil Ecuador). Disponible en http://www.dspace.espol.edu.ec/xmlui/handle/123456789/41521

Hernández, R., Fernández, C., & Baptista, P. (2017). *Metodología de la Investigación* (6ta edición). México : Mc Graw Hill Interamericana.

High Tech Center. (2021). ISE Cisco Identity Services Engine – High Tech Center. Disponible en: http://www.htc-bol.com/documents/ise-byod.pdf

IST la recoleta. (2021)**.** Curso de Redes. *En: Redes Universidad América Latina.* Disponible en: http://ual.dyndns.org/biblioteca/redes/Docs/Inicio.html

Jaén, J. (2016). *Diseño e implementación del control de acceso a la Red CISCO Identify Services Engine (ISE)*. (Tesis de Maestría, Escuela Superior Politécnica del Litoral). Disponible en: http://www.dspace.espol.edu.ec/xmlui/handle/123456789/34981.

Jara, E., Rodríguez, C., & Medina, W**.** (2015). *Implementación de SS7 en una Red CISCO interconectada a una PSTN*. (Tesis de Grado, Escuela Superior Politécnica del Litoral). Disponible en: http://www.dspace.espol.edu.ec/handle/123456789/25471

Jimenez, L., & Urban, G. (2015). Migración de Sevicios Cisco® NAC a Cisco® ISE. En: Repositorio Dspace. Disponible en: https://www.google.com/url?sa=t&source=web&rct=j&url=https://tesis.ipn.mx/jspui/bitstream/123456789/21035/1/TESIS%2520CISCO%2520NAC%2520A%2520CISCO%2520ISE.pdf&ved=2ahUKEwj9rYT_4ej6AhViH7kGHYhyCi0QFnoECAwQAQ&usg=AOvVaw1eQ79nBnxje9hGbMXLIrW7

López, C. (2018). *Diseño y simulación con ISE (Identity Services Engine) para mitigar accesos no autorizados a una red corporativa*. (Tesis de grado, Universidad Tecnológica del Perú). Disponible en: https://repositorio.utp.edu.pe/bitstream/handle/20.500.12867/935/Carlos%20Lopez_Tesis_Titulo%20Profesional_2017.pdf?sequence=1&isAllowed=y

Macho, M. (2002). ¿Qué es la Topología? En: Universidad del País Vasco. Disponible en: http://www.ehu.eus/~mtwmastm/sigma20.pdf

Ministerio de Defensa de España. (2021). Procedimiento de empleo seguro Cisco ISE 2.6. *En: Ministerio de la Presidencia, Relaciones con las Cortes y Memoria Democrática.* [En línea] Centro Criptológico Nacional. Disponible en: https://cpage.mpr.gob.es/producto/procedimiento-de-empleo-seguro-cisco-ise-2-6/

NQA. ISO 27001. (2019). Guia de implantacion. Disponible en: https://www.nqa.com/medialibraries/NQA/NQA-Media-Library/PDFs/Spanish%20QRFs%20and%20PDFs/NQA-ISO-27001-Guia-de-implantacion.pdf

Pinilla, D. (2013). *Diseño y propuesta de implementación de cableado estructurado para DIESELECTROS LTDA*. (Tesis de Grado, Universidad Libre. Bogotá, Colombia). Disponible en: https://repository.unilibre.edu.co/handle/10901/8878

Ramírez, A. (2016). *Propuesta de una guía metedológica para la implementación de Políticas de control de acceso utilizando la plataforma de Cisco – CNAC (Cisco Network Admission Control) en la Universidad Autónoma de Bucaramanga (Colombia).* (Tesis de grado, Universidad Autónoma de Bucaramanga). Disponible en: https://repository.unab.edu.co/bitstream/handle/20.500.12749/3544/2016_Tesis_Ramirez_Ardila_Alexa_Mar%C3%ADa.pdf?sequence=1&isAllowed=y

Romero, K. (2018). *Propuesta de seguridad informática para mejorar el proceso de acceso remoto en una entidad financiera.* (Tesis de grado, Universidad San Ignacio de Loyola). Disponible en: https://repositorio.usil.edu.pe/server/api/core/bitstreams/c10453a7-ef96-490a-b0f4-a6f27efac39e/content

Romero, M. (2018). *Introducción a la seguridad informática y el análisis de vulnerabilidades.* Alicante : Editorial Área de Innovación y Desarrollo.

S.B.S. Nº 504-2021**.** Función de Seguridad de Información y Ciberseguridad. [En línea] Superintendencia de Banca y Seguros. [Citado el: 2 de Enero de 2022.] https://intranet2.sbs.gob.pe/dv_int_cn/2046/v2.0/Adjuntos/504-2021.R.pdf.

Universidad Internacional de la Rioja. (2020). Claves de las políticas de seguridad informática. Disponible en: https://www.unir.net/ingenieria/revista/politicas-seguridad-informatica/

Zurita, W. (2017). *Mejoramiento de una solución de control de acceso, remediación, PROFILING y servicios AAA para la red de datos del Ministerio de Finanzas, orientadas al cumplimiento del acuerdo No. 166 del Esquema de Gestión Gubernamental de la Información*. (Tesis de grado, Universidad de las Fuerzas Armadas ESPE). Disponible en: http://repositorio.espe.edu.ec/bitstream/21000/13662/1/T-ESPE-053915.pdf

ANEXOS

Anexo 1. Instrumentos de Recolección de Datos

A) GUÍA DE OBSERVACIÓN IN SITU

I. Objetivo.

Recoger información in situ, en el mismo lugar, relacionada con el hardware utilizado para la seguridad operativa en la agencia principal de la Caja Huancayo.

II. Indicaciones.

- Apersonarse a la agencia principal de la Caja Huancayo.
- Solicitar el permiso para observar las instalaciones del centro de cómputo.
- Observar el hardware de seguridad instalado en la agencia principal y tomar evidencia de los mismos.

III. Ítems a ser cotejados.

Los ítems a ser cotejados, es decir, las categorías de las cuales se recogerá la información, serán los siguientes:

- Equipos de seguridad interno y externo.
- Disposición de los dispositivos de red que interconectan a las distintas oficinas administrativas de la agencia Principal de Caja Huancayo.

IV. Modelo de Ficha.

AMBIENTE	ELEMENTOS DE SEGURIDAD INFORMÁTICA	
	Elementos de la Red	Equipos Informáticos
Departamento de Marketing		
Departamento de Infraestructura tecnológica		

B) GUÍA DE ENTREVISTA

I. Objetivo.

Recolectar información relacionada tanto con el software como el sistema de protección implementado para la seguridad en las redes y comunicaciones de la Oficina Principal de Caja Huancayo.

II. Indicaciones.

- Solicitar entrevista con el jefe o encargado del área de Infraestructura Tecnológica de la agencia de principal de la Caja Huancayo.
- Realizar las preguntas y anotar las respuestas.

III. Preguntas para el Entrevistado.

3.1. Preguntas referidas al sistema actual, Red LAN, implementado.

a. ¿Cuál es la velocidad para los enlaces para las agencias de Caja Huancayo?

b. ¿Qué características de seguridad en la RED LAN se encuentra implementado actualmente?

3.2. Preguntas referidas a seguridad interna.

a. En lo que va del presente año 2021 ¿Hubo fallas en los Switch Campus o de Acceso?

b. En lo que va del presente año 2021 ¿Hubo ataques en el equipo Wireless Lan Controller y Access Point?

c. En lo que va del presente año 2021 ¿Hubo ataques al servidor DHCP de tipo MAN IN THE MIDDLE?

d. En lo que va del presente año 2021 ¿Hubo problemas con respecto a la configuración PORT-SECURITY?

3.3. Preguntas referidas a seguridad interna (Intencionados o Inocentes).

a. ¿Qué tipo de protección se utiliza para evitar el acceso no autorizado de algún dispositivo u usuario a red interna de la CAJA HUANCAYO?

b. ¿Cuentan con alguna plataforma centralizada para la autenticación seguro a través de los protocolos TACACS+ y RADIUS?

c. En lo que va del presente año 2021 ¿Hubo ataques en la gestión y administración de dispositivos finales por usuarios desconocidos?

d. En lo que va del presente año 2021 ¿Hubo ataques por algún tipo de virus de un dispositivo final y que labores hicieron a fin de no comprometer a los demás dispositivos finales?

e. ¿Cuentan con alguna plataforma de verificación para poder visualizar (que, como, donde y cuando se conecta un dispositivo final a la RED interna de la CAJA HUANCAYO)?

C) GUÍA PARA EL ANALÍSIS MEDIANTE JUICIO DE EXPERTOS

I. Presentación.

¡Buen Día!

En la actualidad vengo ejecutando una investigación que tiene como objetivo: "Implementar políticas de seguridad para la Red LAN de Caja Huancayo, basadas en la tecnología informática Cisco ISE (Identity Services Engine)". En ese sentido, como parte de proponer una mejora en la seguridad informática de la agencia principal de Caja Huancayo, es que recurro a usted que cuenta con experiencia en la implementación de las tecnologías CISCO, para que nos brinde su parecer, basado en su juicio como profesional, con respecto a las preguntas que aparecen más abajo.

II. Indicaciones.

Marcar con una equis (X), la calificación que asignaría a cada uno de los ítems del cuestionario, marcando:

A: Excelente.
B: Bueno.
C: Regular.
D: Malo.
E: Pésimo.

III. Cuestionario.

3.1. Aspectos consultados a 10 expertos en la implementación de tecnologías de seguridad informática que laboran en empresas establecidas en la ciudad de Lima:

Aspecto Consultado	Propuesta		Calificación				
			A	B	C	D	E
Vulnerabilidad en la protección del conmutador de paquetes (Switch)	**1**	Cambiar la Seguridad Informática Interna por otra basada en tecnología CISCO ISE.					
	2	Mantener la Seguridad Informática Interna actualmente operativa en la agencia principal de Caja Huancayo.					
	3	Cambiar la Seguridad Informática Interna por otra basada en otra tecnología distinta a las anteriores.					

Vulnerabilidad en la protección del punto de acceso (Access Point y WLC – Wireless Lan Controller)	**1**	Cambiar la Seguridad Informática Interna por otra basada en tecnología CISCO ISE.					
	2	Mantener la Seguridad Informática Interna actualmente operativa en la agencia principal de Caja Huancayo.					
	3	Cambiar la Seguridad Informática Interna por otra basada en otra tecnología distinta a las anteriores.					
Vulnerabilidades en la protección de MAN IN THE MIDDLE	**1**	Cambiar la Seguridad Informática Interna por otra basada en tecnología CISCO ISE.					
	2	Mantener la Seguridad Informática Interna actualmente operativa en la agencia principal de Caja Huancayo.					
	3	Cambiar la Seguridad Informática Interna por otra basada en otra tecnología distinta a las anteriores.					
Vulnerabilidades en mitigar la cantidad de dispositivos (PORT-SECURITY)	**1**	Cambiar la Seguridad Informática Interna por otra basada en tecnología CISCO ISE.					
	2	Mantener la Seguridad Informática Interna actualmente operativa en la agencia principal de Caja Huancayo.					
	3	Cambiar la Seguridad Informática Interna por otra basada en otra tecnología distinta a las anteriores.					
Políticas de seguridad NAC (Network Access Control)	**1**	Cambiar la Seguridad Informática Interna por otra basada en tecnología CISCO ISE.					
	2	Mantener la Seguridad Informática Interna actualmente operativa en la agencia principal de Caja Huancayo.					
	3	Cambiar la Seguridad Informática Interna por otra basada en otra tecnología distinta a las anteriores.					
Política de seguridad centralizada (TACACS+ y RADIUS)	**1**	Cambiar la Seguridad Informática Interna por otra basada en tecnología CISCO ISE.					
	2	Mantener la Seguridad Informática Interna actualmente operativa en la agencia principal de Caja Huancayo.					
	3	Cambiar la Seguridad Informática Interna por otra basada en otra tecnología distinta a las anteriores.					
Política de seguridad de gestión y administración de dispositivos finales	**1**	Cambiar la Seguridad Informática Interna por otra basada en tecnología CISCO ISE.					
	2	Mantener la Seguridad Informática Interna actualmente operativa en la agencia principal de Caja Huancayo.					
	3	Cambiar la Seguridad Informática Interna por otra basada en otra tecnología distinta a las anteriores.					
Política de Seguridad para	**1**	Cambiar la Seguridad Informática Interna por otra basada en tecnología CISCO ISE.					

visibilidad de la red (Usuarios Microsoft Windows, MAC OS, Linux)	**2**	Mantener la Seguridad Informática Interna actualmente operativa en la agencia principal de Caja Huancayo.					
	3	Cambiar la Seguridad Informática Interna por otra basada en otra tecnología distinta a las anteriores.					
Política de seguridad basado en el acceso (CABLE, WIRELESS, VPN)	**1**	Cambiar la Seguridad Informática Interna por otra basada en tecnología CISCO ISE.					
	2	Mantener la Seguridad Informática Interna actualmente operativa en la agencia principal de Caja Huancayo.					
	3	Cambiar la Seguridad Informática Interna por otra basada en otra tecnología distinta a las anteriores.					

D) FICHA DE VALIDACIÓN DE INSTRUMENTO DE RECOLECCIÓN DE DATOS POR CRITERIO DE JUECES

I. DATOS GENERALES

1.1. Apellidos y nombres del juez: …….
……....

1.2. Título y/o Grado académico: ……...

1.3. Institución de estudios superiores: ……....

1.4. Cargo e institución donde labora: ……
……

1.5. Título de la investigación: ……...
……....

1.6. Apellidos y nombres de los tesistas:
……
……
…….

II. ASPECTO DE LA VALIDACIÓN

ÍTEMS	SI	NO	SUGERENCIAS
1. Las preguntas persiguen fines del objetivo general.			
2.Las preguntas persiguen los fines del objetivo específico.			
3.Las preguntas abarcan variables e indicadores.			
4. Los ítems permiten medir el problema de la investigación.			
5.Los términos utilizados son claros y comprensibles.			
6. El grado de dificultad o complejidad es aceptable.			
7. Los ítems permiten contrastar la hipótesis de la investigación.			
8. Los reactivos siguen un orden lógico.			

9. Se deben considerar otros ítems.			
10. Los ítems despiertan ambigüedad en el encuestado.			

III. CALIFICACIÓN GLOBAL (Ubique el coeficiente de validez obtenido en el intervalo respectivo y marque con un aspa en el cuadro asociado**)**

CATEGORÍA	INTERVALO
Desaprobado ☐	0 – 3
Observado ☐	4 – 7
Aprobado ☐	8 – 10

Fecha: …. /…. /…..

_____

Firma del Juez

Anexo 2. Prueba de Funcionalidad de la solución de Cisco ISE Versión 3.1. en la Agencia Principal de la Caja Huancayo

La evidencia fotográfica constituye una forma de dar cuenta del trabajo de campo realizado durante la ejecución de una investigación...

En lo que prosigue y como parte de la Galería Fotográfica, se presentan imágenes recopiladas durante el trabajo de campo realizado en la agencia principal de Caja Huancayo ubicada en Calle Real N° 341-343, Huancayo, Junín – Perú.

Caja Huancayo con sus 33 años de vida institucional, continúa creciendo de manera sostenible, posicionándose como una empresa sólida y con una fuerte presencia de marca a nivel del sistema microfinanciero, al cierre del año 2021 Caja Huancayo contaba con 183 oficinas distribuidas a nivel nacional.

Figura 1: Vista exterior de la Agencia Principal de la Caja Huancayo.

Fuente: Fotografiado propio.

Figura 2: Ubicación de los equipos switch’es C9300 del 4to piso de la Agencia Principal de la Caja Huancayo

Fuente: Fotografiado Propio

Figura 3: Ubicación de los equipos switch’es C9300 del Sótano de la Agencia Principal de la Caja Huancayo

Fuente: Fotografiado Propio

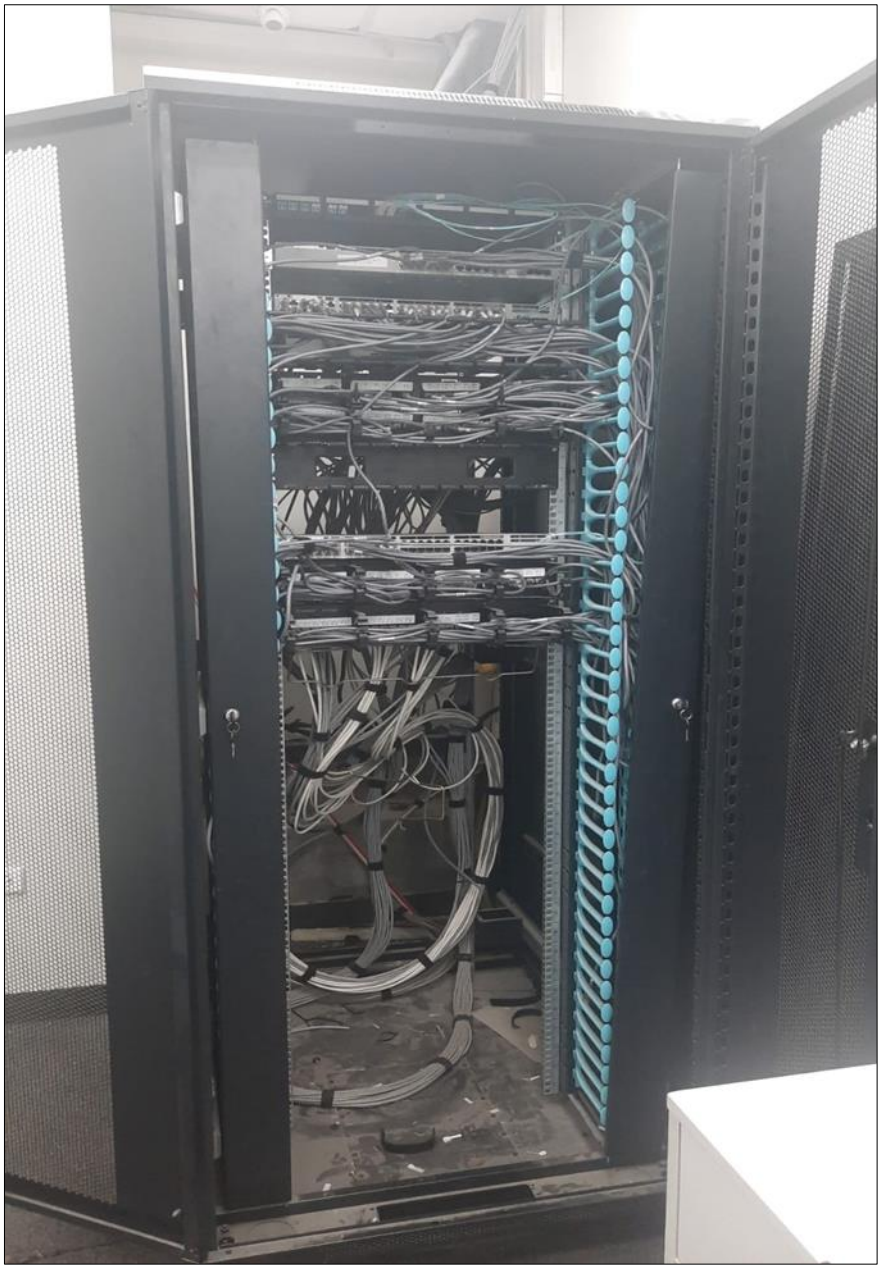


Figura 4: Ubicación de los equipos switch’es C9300 del 3er Piso de la Agencia Principal de la Caja Huancayo

Fuente: Fotografiado Propio

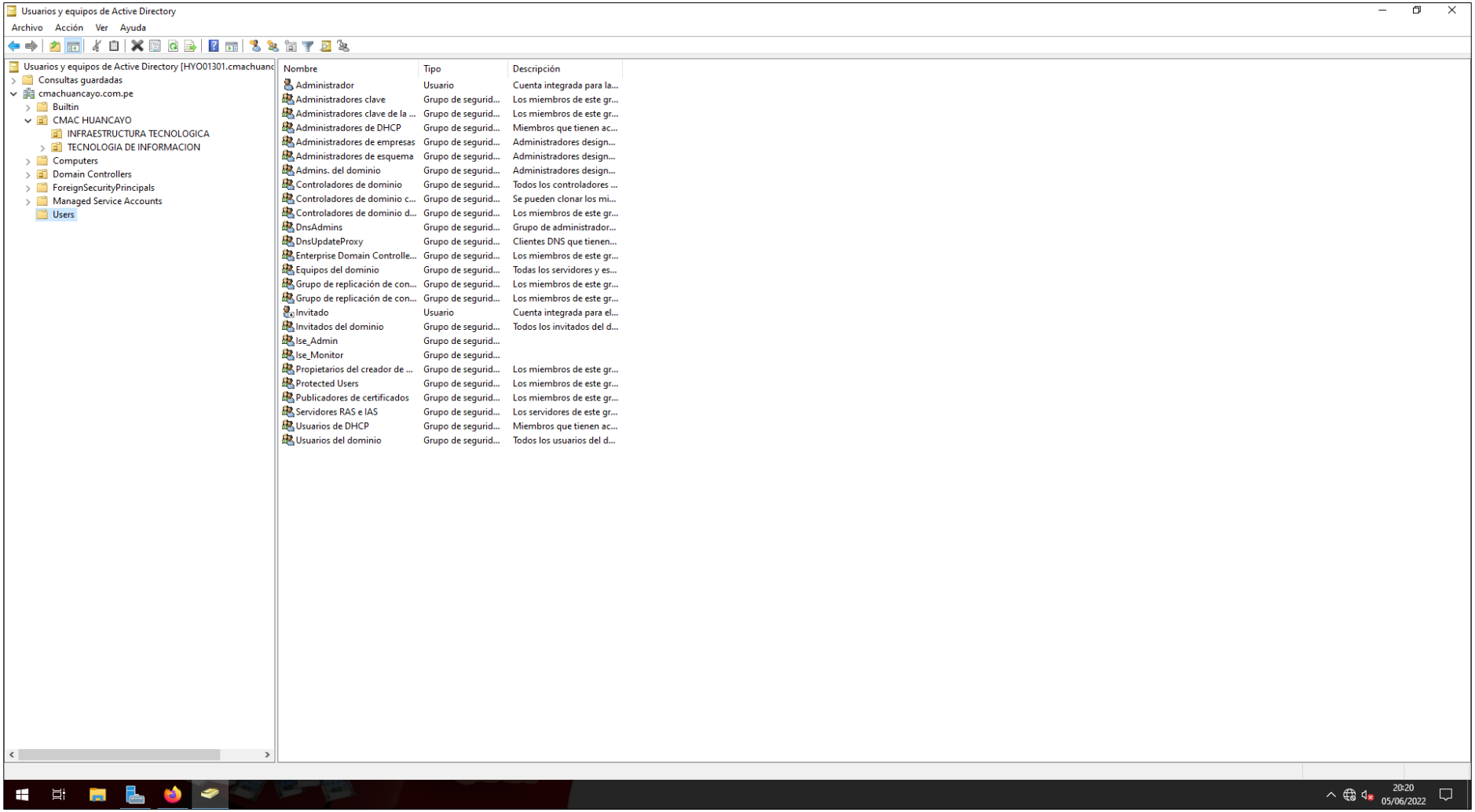


Figura 5: Estructura del Directorio Activo de la CAJA HUANCAYO.

Fuente: Fotografiado propio.

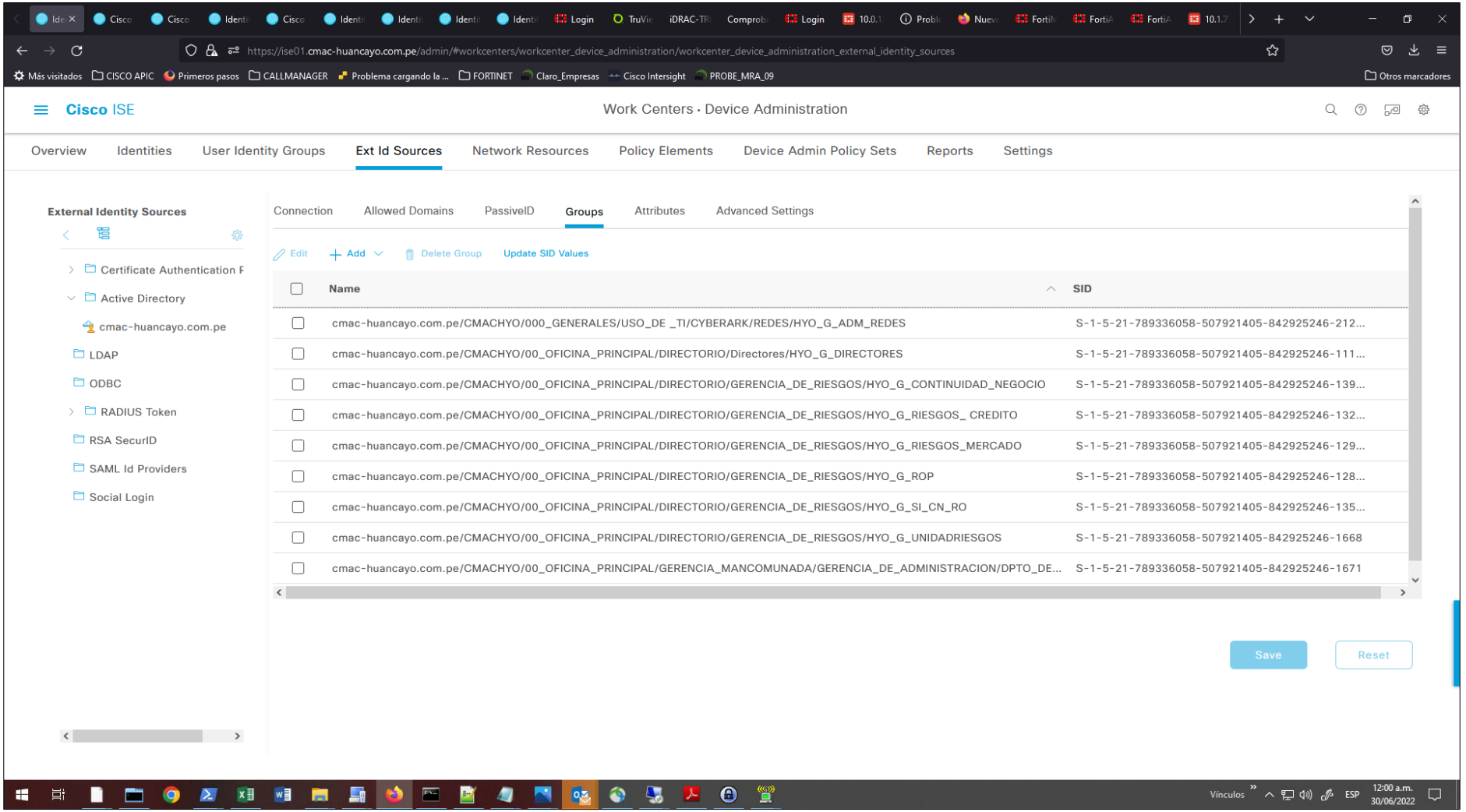


Figura 6: Conexión con el servidor de Directorio Activo en donde se procede a extraer los grupos del Directorio Activo.

Fuente: Fotografiado propio.

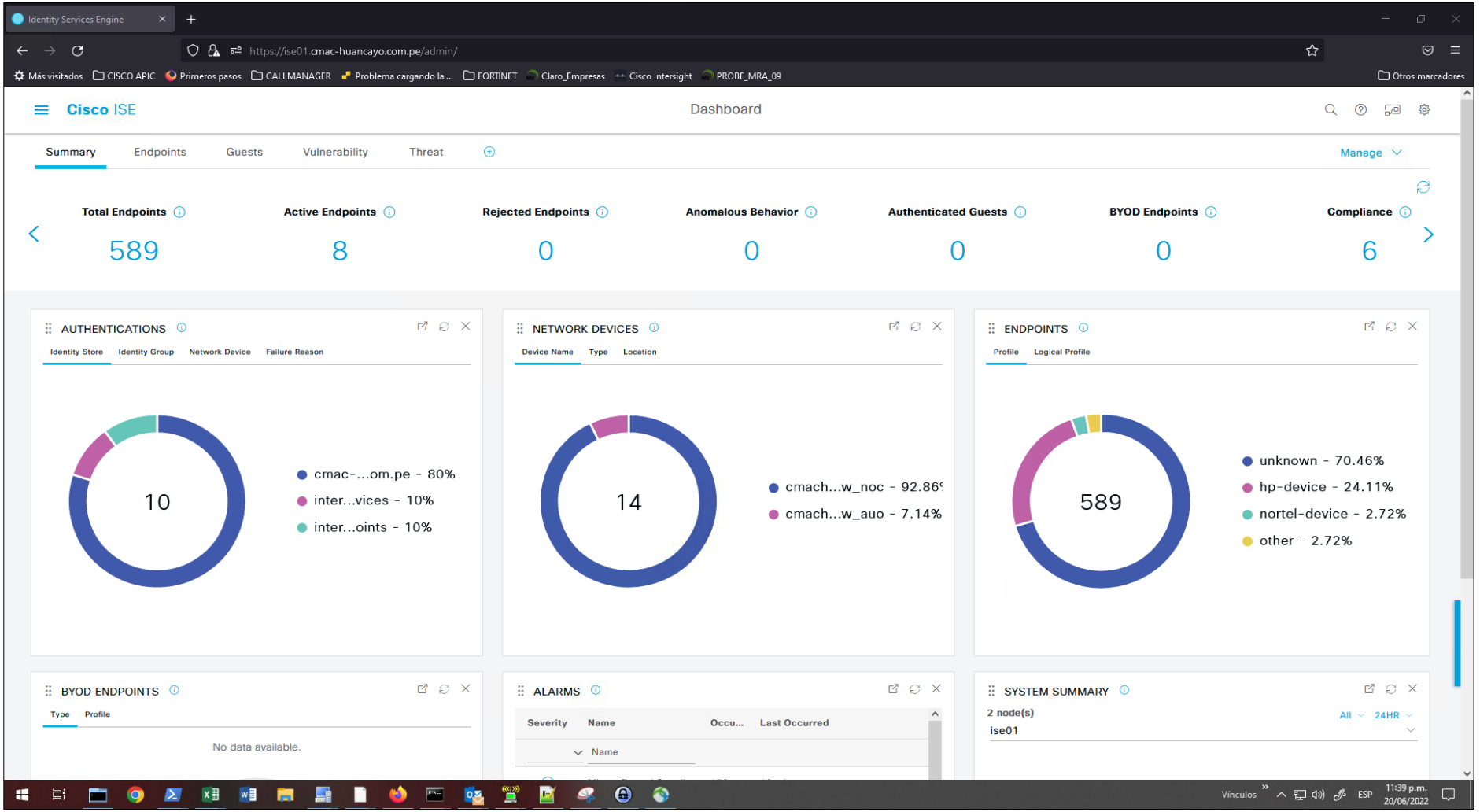


Figura 7: Dashboard principal de la solución CISCO ISE 3.1

Fuente: Fotografiado propio.

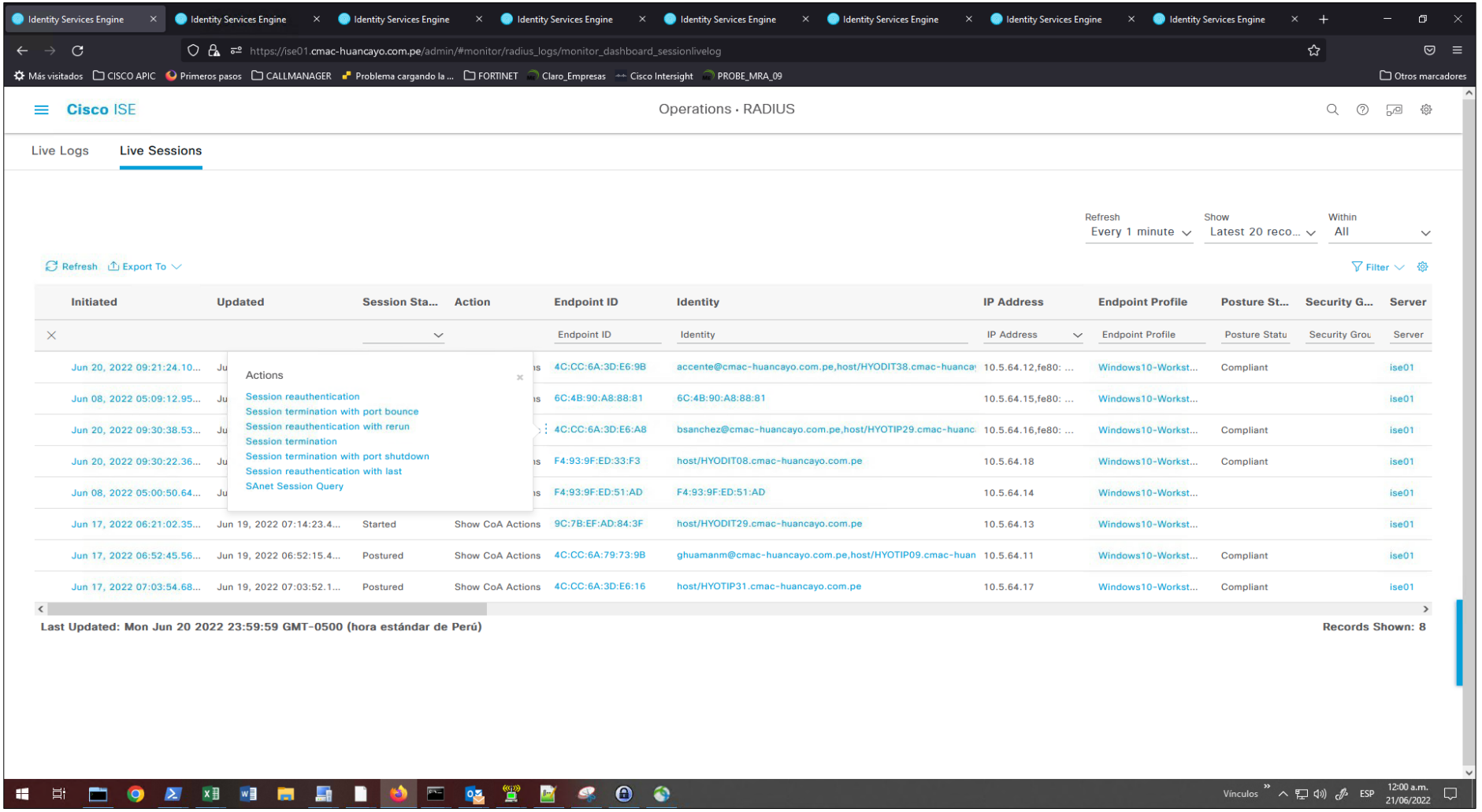


Figura 8: Los equipos autenticados de presentarse cualquier problema que ponga en riesgo, pueden ser finalizados por medio del método COA (Change of Authorization)

Fuente: Fotografiado propio.

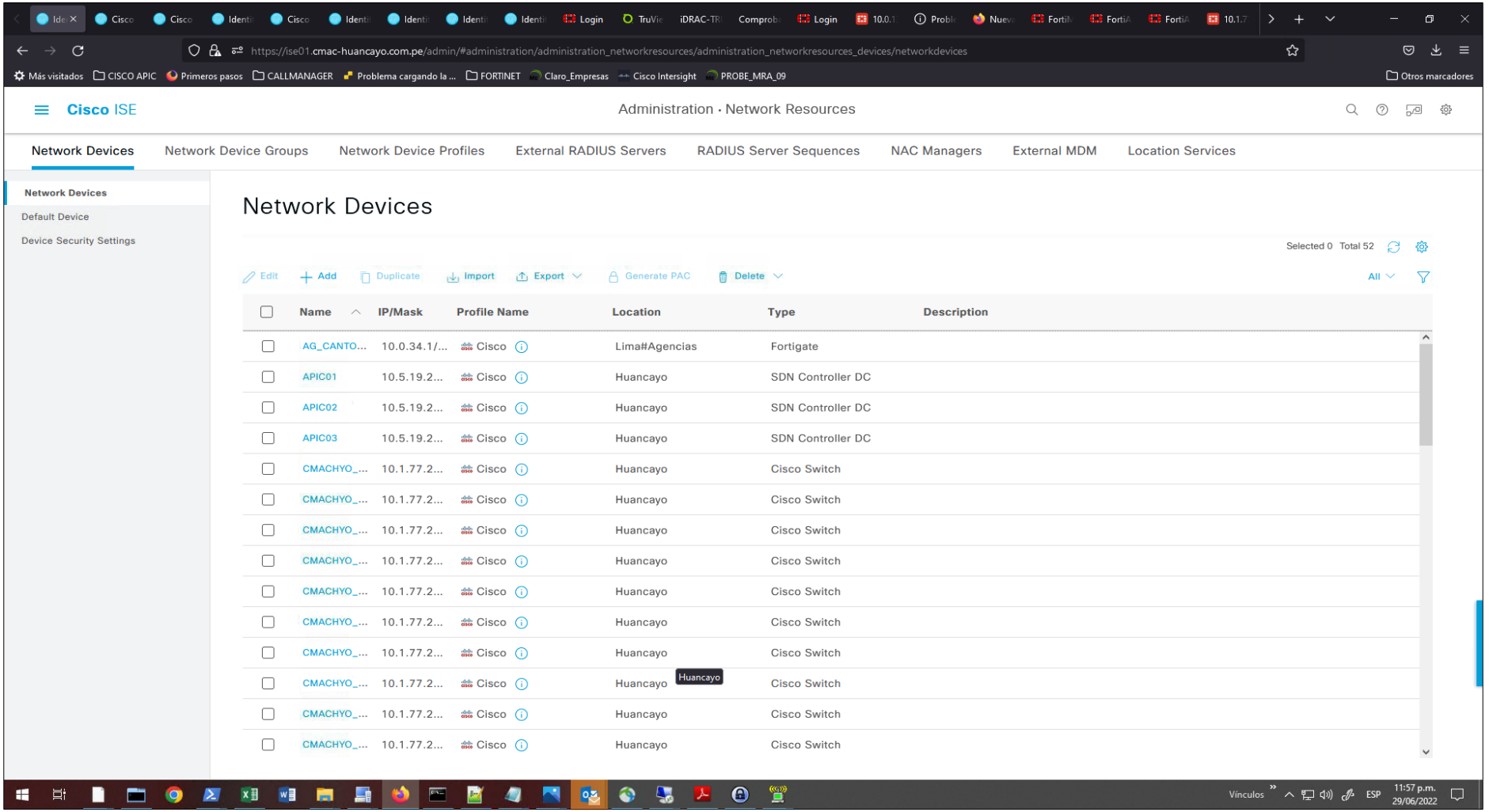


Figura 9: Relación de equipos para la autenticación por TACACS, RADIUS y SNMP

Fuente: Fotografiado propio.

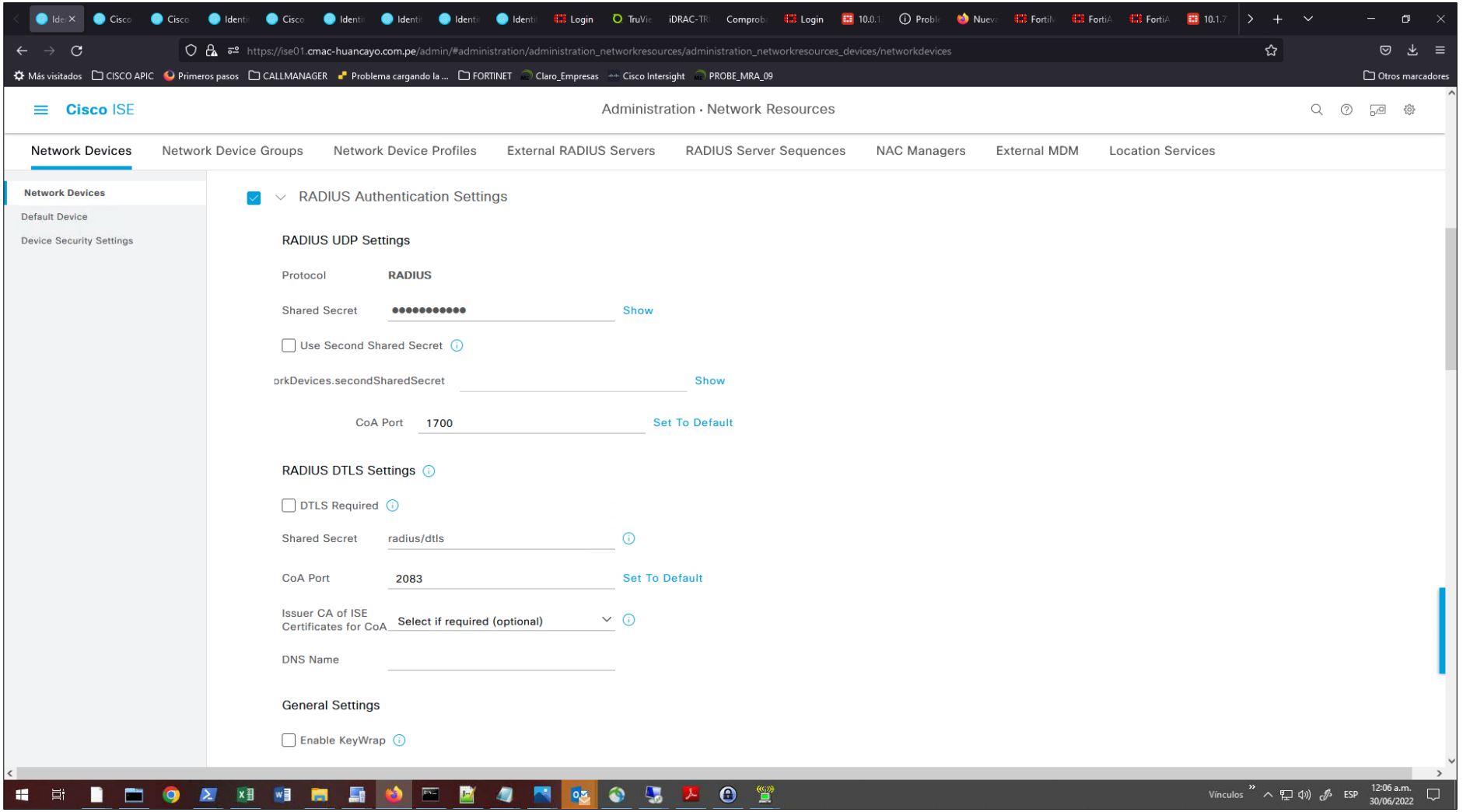


Figura 10: Configuración de un dispositivo para la autenticación por medio del protocolo RADIUS

Fuente: Fotografiado propio.

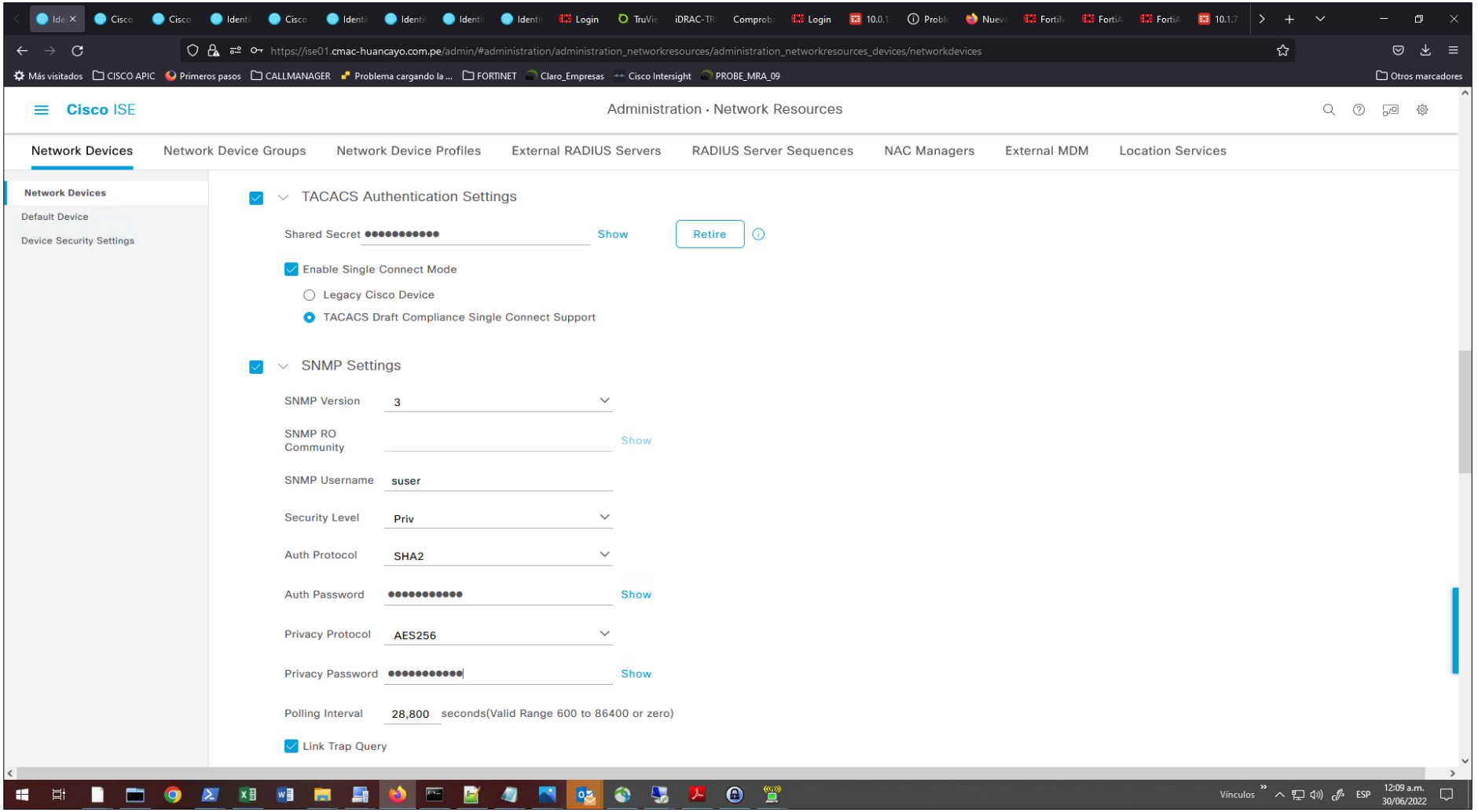
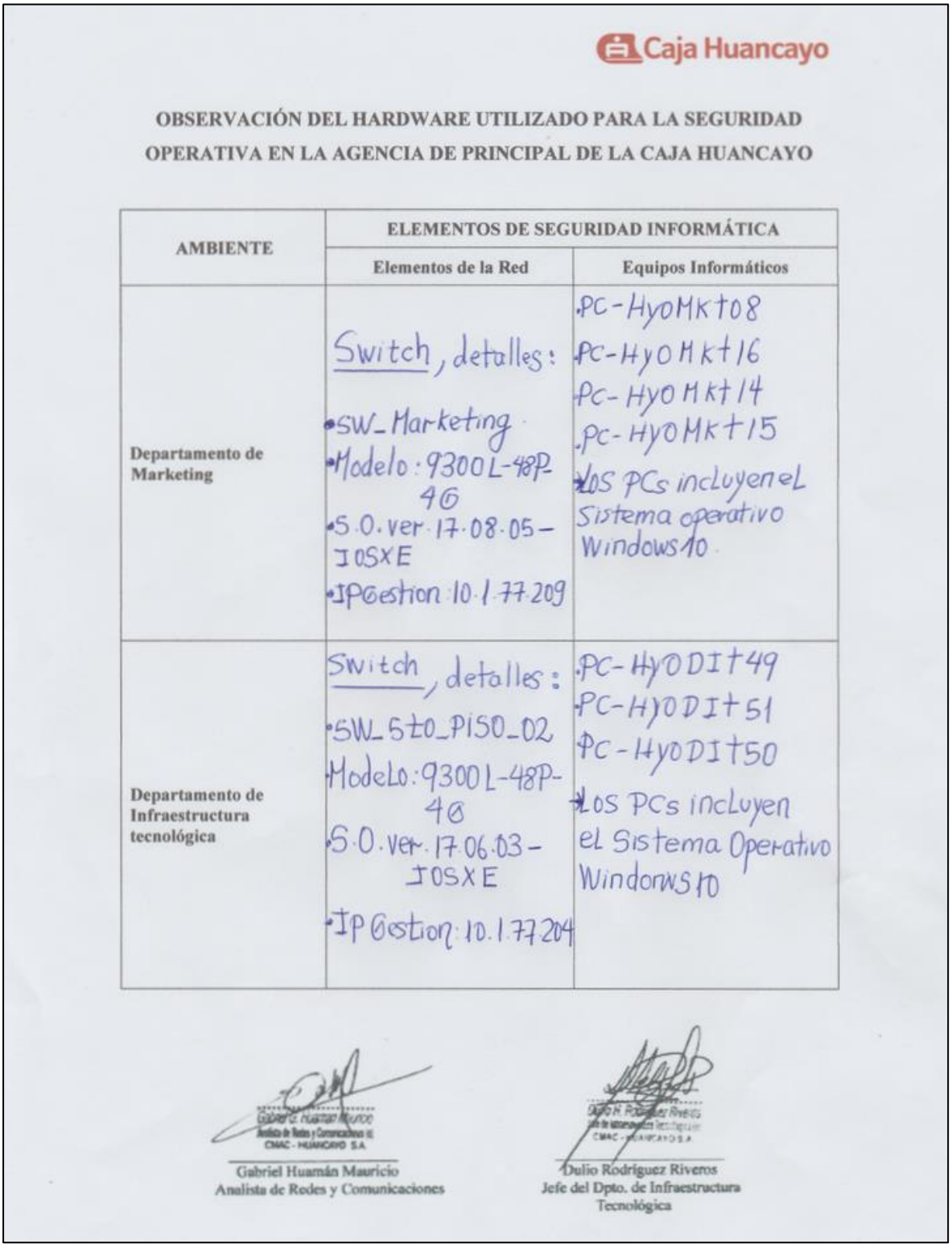


Figura 11: Configuración de un dispositivo para la autenticación por el protocolo TACACS y el protocolo SNMP

Fuente: Fotografiado propio.

Anexo 3. Resultado de la Guía de Observación

.



Caja Huancayo

OBSERVACIÓN DEL HARDWARE UTILIZADO PARA LA SEGURIDAD OPERATIVA EN LA AGENCIA DE PRINCIPAL DE LA CAJA HUANCAYO

AMBIENTE	ELEMENTOS DE SEGURIDAD INFORMÁTICA	
	Elementos de la Red	Equipos Informáticos
Departamento de Marketing	Switch, detalles: •SW_Marketing •Modelo: 9300L-48P-4G •S.O. ver 17.08.05 – IOSXE •IPGestion 10.1.77.209	•PC-HyOMkt08 •PC-HyOMkt16 •PC-HyOMkt14 •PC-HyOMkt15 →Los PCs incluyen el Sistema operativo Windows 10
Departamento de Infraestructura tecnológica	Switch, detalles: •SW_5to_PISO_02 •Modelo: 9300L-48P-4G •S.O. ver. 17.06.03 – IOSXE •IP Gestion: 10.1.77.204	•PC-HyODIt49 •PC-HyODIt51 •PC-HyODIt50 →Los PCs incluyen el Sistema Operativo Windows 10

Gabriel Huamán Mauricio
Analista de Redes y Comunicaciones

Julio Rodríguez Riveros
Jefe del Dpto. de Infraestructura Tecnológica

Anexo 4. Resultado de la Guía de Entrevista

Caja Huancayo

ENTREVISTA AL JEFE DE ÁREA DE INFRAESTRUCTURA TECNOLÓGICA DE LA AGENCIA DE PRINCIPAL DE LA CAJA HUANCAYO

3.1. Preguntas referidas al sistema actual, Red LAN, implementado.

a. ¿Cuál es la velocidad para los enlaces para las agencias de Caja Huancayo?

Actualmente Caja Huancayo, cuenta con un ancho de banda de 10 megas por agencia

b. ¿Qué características de seguridad en la RED LAN se encuentra implementado actualmente?

Caja Huancayo cuenta con Firewall interno y Perimetral de la marca Palo Alto, ademas todos los equipos de computo utilizan el antivirus McAfee

3.2. Preguntas referidas a seguridad interna.

a. En lo que va del presente año 2021 ¿Hubo fallas en los Switch Campus o de Acceso?

Si, debido a que algunos equipos se encontraron desfasados, por lo cual no contaba con el soporte del Fabricante.

b. En lo que va del presente año 2021 ¿Hubo ataques en el equipo Wireless Lan Controller y Access Point?

Si, posiblemente pero no se podria evidenciar, debido a que no se cuenta con una solucion que nos alerte.

c. En lo que va del presente año 2021 ¿Hubo ataques al servidor DHCP de tipo MAN IN THE MIDDLE?

Caja Huancayo anualmente realiza pruebas de ethical hacking, donde se pudo evidenciar la existencia de la vulnerabilidad.

d. En lo que va del presente año 2021 ¿Hubo problemas con respecto a la configuración PORT-SECURITY?

Caja Huancayo anualmente realiza pruebas de ethical hacking, donde se pudo evidenciar la existencia de la vulnerabilidad con respecto al PORT-SECURITY

Caja Huancayo

3.3. Preguntas referidas a seguridad interna (Intencionados o Inocentes).

a. ¿Qué tipo de protección se utiliza para evitar el acceso no autorizado de algún dispositivo u usuario a red interna de la CAJA HUANCAYO?

No se cuenta con ninguna solución que permita evitar el acceso no autorizado a la red.

b. ¿Cuentan con alguna plataforma centralizada para la autenticación seguro a través de los protocolos TACACS+ y RADIUS?

No contamos con ninguna solución para la autenticación centralizada, pero si contamos con un servidor de directorio activo

c. En lo que va del presente año 2021 ¿Hubo ataques en la gestión y administración de dispositivos finales por usuarios desconocidos?

No contamos con ninguna solución que nos alerte ataques en la gestion y administración de dispositivos

d. En lo que va del presente año 2021 ¿Hubo ataques por algún tipo de virus de un dispositivo final y que labores hicieron a fin de no comprometer a los demás dispositivos finales?

Si hubo un ataque por un virus y se tomo como medidas preventivas aislar el equipo inpectado de la red interna

e. ¿Cuentan con alguna plataforma de verificación para poder visualizar (que, como, donde y cuando se conecta un dispositivo final a la RED interna de la CAJA HUANCAYO)?

No contamos con ninguna solución que permita la visualización de los usuarios y equipos que se autentican a la red.

Gabriel Huamán Mauricio
Analista de Redes y Comunicaciones

Dulio Rodríguez Riveros
Jefe del Dpto. de Infraestructura Tecnológica

Anexo 5. Resultado del cuestionario por los 10 expertos

ANALÍSIS MEDIANTE JUICIO DE EXPERTOS

I. Presentación.

Nombre y Apellidos: Carlos Eugenio Vilcatoma Ocaña

Grado: Bachiller (Ingeniero de Sistemas)

¡Buen Día!

En la actualidad vengo ejecutando una investigación que tiene como objetivo: "Implementar políticas de seguridad para la Red LAN de Caja Huancayo, basadas en la tecnología informática Cisco ISE (Identity Services Engine)". En ese sentido, como parte de proponer una mejora en la seguridad informática de la agencia principal de Caja Huancayo, es que recurro a usted que cuenta con experiencia en la implementación de las tecnologías CISCO, para que nos brinde su parecer, basado en su juicio como profesional, con respecto a las preguntas que aparecen más abajo.

II. Indicaciones.

Marcar con una equis (X), la calificación que asignaría a cada uno de los ítems del cuestionario, marcando:

A: Excelente.
B: Bueno.
C: Regular.
D: Malo.
E: Pésimo.

III. Cuestionario.

Aspecto Consultado	Propuesta		Calificación				
			A	B	C	D	E
Vulnerabilidad en la protección del conmutador de paquetes (Switch)	1	Cambiar la Seguridad Informática Interna por otra basada en tecnología CISCO ISE.	X				
	2	Mantener la Seguridad Informática Interna actualmente operativa en la agencia principal de Caja Huancayo.		X			
	3	Cambiar la Seguridad Informática Interna por otra basada en otra tecnología distinta a las anteriores.					X
Vulnerabilidad en la protección del punto de acceso (Access Point y WLC – Wireless Lan Controller)	1	Cambiar la Seguridad Informática Interna por otra basada en tecnología CISCO ISE.		X			
	2	Mantener la Seguridad Informática Interna actualmente operativa en la agencia principal de Caja Huancayo.		X			
	3	Cambiar la Seguridad Informática Interna por otra basada en otra tecnología distinta a las anteriores.		X			
Vulnerabilidades en la protección de MAN IN THE MIDDLE	1	Cambiar la Seguridad Informática Interna por otra basada en tecnología CISCO ISE.		X			
	2	Mantener la Seguridad Informática Interna actualmente operativa en la agencia principal de Caja Huancayo.		X			
	3	Cambiar la Seguridad Informática Interna por otra basada en otra tecnología distinta a las anteriores.			X		

Vulnerabilidades en mitigar la cantidad de dispositivos (PORT-SECURITY)	**1**	Cambiar la Seguridad Informática Interna por otra basada en tecnología CISCO ISE.	**X**				
	2	Mantener la Seguridad Informática Interna actualmente operativa en la agencia principal de Caja Huancayo.		**X**			
	3	Cambiar la Seguridad Informática Interna por otra basada en otra tecnología distinta a las anteriores.			**X**		
Políticas de seguridad NAC (Network Access Control)	**1**	Cambiar la Seguridad Informática Interna por otra basada en tecnología CISCO ISE.	**X**				
	2	Mantener la Seguridad Informática Interna actualmente operativa en la agencia principal de Caja Huancayo.		**X**			
	3	Cambiar la Seguridad Informática Interna por otra basada en otra tecnología distinta a las anteriores.		**X**			
Política de seguridad centralizada (TACACS+ y RADIUS)	**1**	Cambiar la Seguridad Informática Interna por otra basada en tecnología CISCO ISE.		**X**			
	2	Mantener la Seguridad Informática Interna actualmente operativa en la agencia principal de Caja Huancayo.			**X**		
	3	Cambiar la Seguridad Informática Interna por otra basada en otra tecnología distinta a las anteriores.			**X**		
Política de seguridad de gestión y administración de dispositivos finales	**1**	Cambiar la Seguridad Informática Interna por otra basada en tecnología CISCO ISE.	**X**				
	2	Mantener la Seguridad Informática Interna actualmente operativa en la agencia principal de Caja Huancayo.		**X**			
	3	Cambiar la Seguridad Informática Interna por otra basada en otra tecnología distinta a las anteriores.	**X**				
Política de Seguridad para visibilidad de la red (Usuarios Microsoft Windows, MAC OS, Linux)	**1**	Cambiar la Seguridad Informática Interna por otra basada en tecnología CISCO ISE.		**X**			
	2	Mantener la Seguridad Informática Interna actualmente operativa en la agencia principal de Caja Huancayo.			**X**		
	3	Cambiar la Seguridad Informática Interna por otra basada en otra tecnología distinta a las anteriores.		**X**			
Política de seguridad basado en el acceso (CABLE, WIRELESS, VPN)	**1**	Cambiar la Seguridad Informática Interna por otra basada en tecnología CISCO ISE.	**X**				
	2	Mantener la Seguridad Informática Interna actualmente operativa en la agencia principal de Caja Huancayo.				**X**	
	3	Cambiar la Seguridad Informática Interna por otra basada en otra tecnología distinta a las anteriores.			**X**		

Carlos E. Vilcatoma O.

Carlos Eugenio Vilcatoma Ocaña

ANALÍSIS MEDIANTE JUICIO DE EXPERTOS

I. Presentación.

Nombre y Apellidos: Matías Esteban Torre Valle

Grado: Bachiller (Ingeniero de Sistemas)

¡Buen Día!

En la actualidad vengo ejecutando una investigación que tiene como objetivo: "Implementar políticas de seguridad para la Red LAN de Caja Huancayo, basadas en la tecnología informática Cisco ISE (Identity Services Engine)". En ese sentido, como parte de proponer una mejora en la seguridad informática de la agencia principal de Caja Huancayo, es que recurro a usted que cuenta con experiencia en la implementación de las tecnologías CISCO, para que nos brinde su parecer, basado en su juicio como profesional, con respecto a las preguntas que aparecen más abajo.

II. Indicaciones.

Marcar con una equis (X), la calificación que asignaría a cada uno de los ítems del cuestionario, marcando:

A: Excelente.
B: Bueno.
C: Regular.
D: Malo.
E: Pésimo.

III. Cuestionario.

Aspecto Consultado	Propuesta		Calificación				
			A	B	C	D	E
Vulnerabilidad en la protección del conmutador de paquetes (Switch)	1	Cambiar la Seguridad Informática Interna por otra basada en tecnología CISCO ISE.		X			
	2	Mantener la Seguridad Informática Interna actualmente operativa en la agencia principal de Caja Huancayo.			X		
	3	Cambiar la Seguridad Informática Interna por otra basada en otra tecnología distinta a las anteriores.			X		
Vulnerabilidad en la protección del punto de acceso (Access Point y WLC – Wireless Lan Controller)	1	Cambiar la Seguridad Informática Interna por otra basada en tecnología CISCO ISE.		X			
	2	Mantener la Seguridad Informática Interna actualmente operativa en la agencia principal de Caja Huancayo.				X	
	3	Cambiar la Seguridad Informática Interna por otra basada en otra tecnología distinta a las anteriores.				X	
Vulnerabilidades en la protección de MAN IN THE MIDDLE	1	Cambiar la Seguridad Informática Interna por otra basada en tecnología CISCO ISE.	X				
	2	Mantener la Seguridad Informática Interna actualmente operativa en la agencia principal de Caja Huancayo.				X	
	3	Cambiar la Seguridad Informática Interna por otra basada en otra tecnología distinta a las anteriores.			X		

Vulnerabilidades en mitigar la cantidad de dispositivos (PORT-SECURITY)	**1**	Cambiar la Seguridad Informática Interna por otra basada en tecnología CISCO ISE.		**X**			
	2	Mantener la Seguridad Informática Interna actualmente operativa en la agencia principal de Caja Huancayo.			**X**		
	3	Cambiar la Seguridad Informática Interna por otra basada en otra tecnología distinta a las anteriores.					**X**
Políticas de seguridad NAC (Network Access Control)	**1**	Cambiar la Seguridad Informática Interna por otra basada en tecnología CISCO ISE.		**X**			
	2	Mantener la Seguridad Informática Interna actualmente operativa en la agencia principal de Caja Huancayo.		**X**			
	3	Cambiar la Seguridad Informática Interna por otra basada en otra tecnología distinta a las anteriores.				**X**	
Política de seguridad centralizada (TACACS+ y RADIUS)	**1**	Cambiar la Seguridad Informática Interna por otra basada en tecnología CISCO ISE.		**X**			
	2	Mantener la Seguridad Informática Interna actualmente operativa en la agencia principal de Caja Huancayo.			**X**		
	3	Cambiar la Seguridad Informática Interna por otra basada en otra tecnología distinta a las anteriores.				**X**	
Política de seguridad de gestión y administración de dispositivos finales	**1**	Cambiar la Seguridad Informática Interna por otra basada en tecnología CISCO ISE.		**X**			
	2	Mantener la Seguridad Informática Interna actualmente operativa en la agencia principal de Caja Huancayo.					**X**
	3	Cambiar la Seguridad Informática Interna por otra basada en otra tecnología distinta a las anteriores.	**X**				
Política de Seguridad para visibilidad de la red (Usuarios Microsoft Windows, MAC OS, Linux)	**1**	Cambiar la Seguridad Informática Interna por otra basada en tecnología CISCO ISE.			**X**		
	2	Mantener la Seguridad Informática Interna actualmente operativa en la agencia principal de Caja Huancayo.				**X**	
	3	Cambiar la Seguridad Informática Interna por otra basada en otra tecnología distinta a las anteriores.			**X**		
Política de seguridad basado en el acceso (CABLE, WIRELESS, VPN)	**1**	Cambiar la Seguridad Informática Interna por otra basada en tecnología CISCO ISE.	**X**				
	2	Mantener la Seguridad Informática Interna actualmente operativa en la agencia principal de Caja Huancayo.		**X**			
	3	Cambiar la Seguridad Informática Interna por otra basada en otra tecnología distinta a las anteriores.			**X**		

Matías Esteban Torre Valle

ANALÍSIS MEDIANTE JUICIO DE EXPERTOS

I. Presentación.

Nombre y Apellidos: Giancarlo Condori Torres

Grado: Magister

¡Buen Día!

En la actualidad vengo ejecutando una investigación que tiene como objetivo: "Implementar políticas de seguridad para la Red LAN de Caja Huancayo, basadas en la tecnología informática Cisco ISE (Identity Services Engine)". En ese sentido, como parte de proponer una mejora en la seguridad informática de la agencia principal de Caja Huancayo, es que recurro a usted que cuenta con experiencia en la implementación de las tecnologías CISCO, para que nos brinde su parecer, basado en su juicio como profesional, con respecto a las preguntas que aparecen más abajo.

II. Indicaciones.

Marcar con una equis (X), la calificación que asignaría a cada uno de los ítems del cuestionario, marcando:

A: Excelente.
B: Bueno.
C: Regular.
D: Malo.
E: Pésimo.

III. Cuestionario.

Aspecto Consultado	Propuesta		Calificación				
			A	B	C	D	E
Vulnerabilidad en la protección del conmutador de paquetes (Switch)	1	Cambiar la Seguridad Informática Interna por otra basada en tecnología CISCO ISE.		X			
	2	Mantener la Seguridad Informática Interna actualmente operativa en la agencia principal de Caja Huancayo.		X			
	3	Cambiar la Seguridad Informática Interna por otra basada en otra tecnología distinta a las anteriores.					X
Vulnerabilidad en la protección del punto de acceso (Access Point y WLC – Wireless Lan Controller)	1	Cambiar la Seguridad Informática Interna por otra basada en tecnología CISCO ISE.		X			
	2	Mantener la Seguridad Informática Interna actualmente operativa en la agencia principal de Caja Huancayo.			X		
	3	Cambiar la Seguridad Informática Interna por otra basada en otra tecnología distinta a las anteriores.		X			
Vulnerabilidades en la protección de MAN IN THE MIDDLE	1	Cambiar la Seguridad Informática Interna por otra basada en tecnología CISCO ISE.			X		
	2	Mantener la Seguridad Informática Interna actualmente operativa en la agencia principal de Caja Huancayo.		X			
	3	Cambiar la Seguridad Informática Interna por otra basada en otra tecnología distinta a las anteriores.				X	

Vulnerabilidades en mitigar la cantidad de dispositivos (PORT-SECURITY)	**1**	Cambiar la Seguridad Informática Interna por otra basada en tecnología CISCO ISE.		**X**			
	2	Mantener la Seguridad Informática Interna actualmente operativa en la agencia principal de Caja Huancayo.					**X**
	3	Cambiar la Seguridad Informática Interna por otra basada en otra tecnología distinta a las anteriores.					**X**
Políticas de seguridad NAC (Network Access Control)	**1**	Cambiar la Seguridad Informática Interna por otra basada en tecnología CISCO ISE.		**X**			
	2	Mantener la Seguridad Informática Interna actualmente operativa en la agencia principal de Caja Huancayo.	**X**				
	3	Cambiar la Seguridad Informática Interna por otra basada en otra tecnología distinta a las anteriores.				**X**	
Política de seguridad centralizada (TACACS+ y RADIUS)	**1**	Cambiar la Seguridad Informática Interna por otra basada en tecnología CISCO ISE.			**X**		
	2	Mantener la Seguridad Informática Interna actualmente operativa en la agencia principal de Caja Huancayo.		**X**			
	3	Cambiar la Seguridad Informática Interna por otra basada en otra tecnología distinta a las anteriores.			**X**		
Política de seguridad de gestión y administración de dispositivos finales	**1**	Cambiar la Seguridad Informática Interna por otra basada en tecnología CISCO ISE.		**X**			
	2	Mantener la Seguridad Informática Interna actualmente operativa en la agencia principal de Caja Huancayo.			**X**		
	3	Cambiar la Seguridad Informática Interna por otra basada en otra tecnología distinta a las anteriores.	**X**				
Política de Seguridad para visibilidad de la red (Usuarios Microsoft Windows, MAC OS, Linux)	**1**	Cambiar la Seguridad Informática Interna por otra basada en tecnología CISCO ISE.		**X**			
	2	Mantener la Seguridad Informática Interna actualmente operativa en la agencia principal de Caja Huancayo.				**X**	
	3	Cambiar la Seguridad Informática Interna por otra basada en otra tecnología distinta a las anteriores.			**X**		
Política de seguridad basado en el acceso (CABLE, WIRELESS, VPN)	**1**	Cambiar la Seguridad Informática Interna por otra basada en tecnología CISCO ISE.	**X**				
	2	Mantener la Seguridad Informática Interna actualmente operativa en la agencia principal de Caja Huancayo.			**X**		
	3	Cambiar la Seguridad Informática Interna por otra basada en otra tecnología distinta a las anteriores.					**X**

Giancarlo Condori Torres

ANALÍSIS MEDIANTE JUICIO DE EXPERTOS

I. Presentación.

Nombre y Apellidos: Juan Diego Gutierrez Amasifuen

Grado: Bachiller (Ingeniero de Sistemas)

¡Buen Día!

En la actualidad vengo ejecutando una investigación que tiene como objetivo: "Implementar políticas de seguridad para la Red LAN de Caja Huancayo, basadas en la tecnología informática Cisco ISE (Identity Services Engine)". En ese sentido, como parte de proponer una mejora en la seguridad informática de la agencia principal de Caja Huancayo, es que recurro a usted que cuenta con experiencia en la implementación de las tecnologías CISCO, para que nos brinde su parecer, basado en su juicio como profesional, con respecto a las preguntas que aparecen más abajo.

II. Indicaciones.

Marcar con una equis (X), la calificación que asignaría a cada uno de los ítems del cuestionario, marcando:

A: Excelente.
B: Bueno.
C: Regular.
D: Malo.
E: Pésimo.

III. Cuestionario.

Aspecto Consultado	Propuesta		Calificación				
			A	B	C	D	E
Vulnerabilidad en la protección del conmutador de paquetes (Switch)	1	Cambiar la Seguridad Informática Interna por otra basada en tecnología CISCO ISE.	X				
	2	Mantener la Seguridad Informática Interna actualmente operativa en la agencia principal de Caja Huancayo.			X		
	3	Cambiar la Seguridad Informática Interna por otra basada en otra tecnología distinta a las anteriores.				X	
Vulnerabilidad en la protección del punto de acceso (Access Point y WLC – Wireless Lan Controller)	1	Cambiar la Seguridad Informática Interna por otra basada en tecnología CISCO ISE.		X			
	2	Mantener la Seguridad Informática Interna actualmente operativa en la agencia principal de Caja Huancayo.		X			
	3	Cambiar la Seguridad Informática Interna por otra basada en otra tecnología distinta a las anteriores.		X			
Vulnerabilidades en la protección de MAN IN THE MIDDLE	1	Cambiar la Seguridad Informática Interna por otra basada en tecnología CISCO ISE.		X			
	2	Mantener la Seguridad Informática Interna actualmente operativa en la agencia principal de Caja Huancayo.				X	
	3	Cambiar la Seguridad Informática Interna por otra basada en otra tecnología distinta a las anteriores.			X		

Vulnerabilidades en mitigar la cantidad de dispositivos (PORT-SECURITY)	**1**	Cambiar la Seguridad Informática Interna por otra basada en tecnología CISCO ISE.	**X**				
	2	Mantener la Seguridad Informática Interna actualmente operativa en la agencia principal de Caja Huancayo.					**X**
	3	Cambiar la Seguridad Informática Interna por otra basada en otra tecnología distinta a las anteriores.				**X**	
Políticas de seguridad NAC (Network Access Control)	**1**	Cambiar la Seguridad Informática Interna por otra basada en tecnología CISCO ISE.	**X**				
	2	Mantener la Seguridad Informática Interna actualmente operativa en la agencia principal de Caja Huancayo.	**X**				
	3	Cambiar la Seguridad Informática Interna por otra basada en otra tecnología distinta a las anteriores.		**X**			
Política de seguridad centralizada (TACACS+ y RADIUS)	**1**	Cambiar la Seguridad Informática Interna por otra basada en tecnología CISCO ISE.	**X**				
	2	Mantener la Seguridad Informática Interna actualmente operativa en la agencia principal de Caja Huancayo.				**X**	
	3	Cambiar la Seguridad Informática Interna por otra basada en otra tecnología distinta a las anteriores.			**X**		
Política de seguridad de gestión y administración de dispositivos finales	**1**	Cambiar la Seguridad Informática Interna por otra basada en tecnología CISCO ISE.		**X**			
	2	Mantener la Seguridad Informática Interna actualmente operativa en la agencia principal de Caja Huancayo.					**X**
	3	Cambiar la Seguridad Informática Interna por otra basada en otra tecnología distinta a las anteriores.	**X**				
Política de Seguridad para visibilidad de la red (Usuarios Microsoft Windows, MAC OS, Linux)	**1**	Cambiar la Seguridad Informática Interna por otra basada en tecnología CISCO ISE.		**X**			
	2	Mantener la Seguridad Informática Interna actualmente operativa en la agencia principal de Caja Huancayo.			**X**		
	3	Cambiar la Seguridad Informática Interna por otra basada en otra tecnología distinta a las anteriores.				**X**	
Política de seguridad basado en el acceso (CABLE, WIRELESS, VPN)	**1**	Cambiar la Seguridad Informática Interna por otra basada en tecnología CISCO ISE.	**X**				
	2	Mantener la Seguridad Informática Interna actualmente operativa en la agencia principal de Caja Huancayo.		**X**			
	3	Cambiar la Seguridad Informática Interna por otra basada en otra tecnología distinta a las anteriores.				**X**	

Juan Diego Gutierrez Amasifuen

ANALÍSIS MEDIANTE JUICIO DE EXPERTOS

I. Presentación.

Nombre y Apellidos: Juan Gabrihel Gabino Perez Gonzales

Grado: Bachiller (Ingeniero de Sistemas)

¡Buen Día!

En la actualidad vengo ejecutando una investigación que tiene como objetivo: "Implementar políticas de seguridad para la Red LAN de Caja Huancayo, basadas en la tecnología informática Cisco ISE (Identity Services Engine)". En ese sentido, como parte de proponer una mejora en la seguridad informática de la agencia principal de Caja Huancayo, es que recurro a usted que cuenta con experiencia en la implementación de las tecnologías CISCO, para que nos brinde su parecer, basado en su juicio como profesional, con respecto a las preguntas que aparecen más abajo.

II. Indicaciones.

Marcar con una equis (X), la calificación que asignaría a cada uno de los ítems del cuestionario, marcando:

A: Excelente.
B: Bueno.
C: Regular.
D: Malo.
E: Pésimo.

III. Cuestionario.

Aspecto Consultado	Propuesta		Calificación				
			A	B	C	D	E
Vulnerabilidad en la protección del conmutador de paquetes (Switch)	1	Cambiar la Seguridad Informática Interna por otra basada en tecnología CISCO ISE.	X				
	2	Mantener la Seguridad Informática Interna actualmente operativa en la agencia principal de Caja Huancayo.			X		
	3	Cambiar la Seguridad Informática Interna por otra basada en otra tecnología distinta a las anteriores.			X		
Vulnerabilidad en la protección del punto de acceso (Access Point y WLC – Wireless Lan Controller)	1	Cambiar la Seguridad Informática Interna por otra basada en tecnología CISCO ISE.	X				
	2	Mantener la Seguridad Informática Interna actualmente operativa en la agencia principal de Caja Huancayo.			X		
	3	Cambiar la Seguridad Informática Interna por otra basada en otra tecnología distinta a las anteriores.		X			
Vulnerabilidades en la protección de MAN IN THE MIDDLE	1	Cambiar la Seguridad Informática Interna por otra basada en tecnología CISCO ISE.		X			
	2	Mantener la Seguridad Informática Interna actualmente operativa en la agencia principal de Caja Huancayo.			X		
	3	Cambiar la Seguridad Informática Interna por otra basada en otra tecnología distinta a las anteriores.			X		

Vulnerabilidades en mitigar la cantidad de dispositivos (PORT-SECURITY)	**1**	Cambiar la Seguridad Informática Interna por otra basada en tecnología CISCO ISE.	**X**				
	2	Mantener la Seguridad Informática Interna actualmente operativa en la agencia principal de Caja Huancayo.			**X**		
	3	Cambiar la Seguridad Informática Interna por otra basada en otra tecnología distinta a las anteriores.		**X**			
Políticas de seguridad NAC (Network Access Control)	**1**	Cambiar la Seguridad Informática Interna por otra basada en tecnología CISCO ISE.	**X**				
	2	Mantener la Seguridad Informática Interna actualmente operativa en la agencia principal de Caja Huancayo.	**X**				
	3	Cambiar la Seguridad Informática Interna por otra basada en otra tecnología distinta a las anteriores.		**X**			
Política de seguridad centralizada (TACACS+ y RADIUS)	**1**	Cambiar la Seguridad Informática Interna por otra basada en tecnología CISCO ISE.	**X**				
	2	Mantener la Seguridad Informática Interna actualmente operativa en la agencia principal de Caja Huancayo.			**X**		
	3	Cambiar la Seguridad Informática Interna por otra basada en otra tecnología distinta a las anteriores.		**X**			
Política de seguridad de gestión y administración de dispositivos finales	**1**	Cambiar la Seguridad Informática Interna por otra basada en tecnología CISCO ISE.			**X**		
	2	Mantener la Seguridad Informática Interna actualmente operativa en la agencia principal de Caja Huancayo.		**X**			
	3	Cambiar la Seguridad Informática Interna por otra basada en otra tecnología distinta a las anteriores.	**X**				
Política de Seguridad para visibilidad de la red (Usuarios Microsoft Windows, MAC OS, Linux)	**1**	Cambiar la Seguridad Informática Interna por otra basada en tecnología CISCO ISE.		**X**			
	2	Mantener la Seguridad Informática Interna actualmente operativa en la agencia principal de Caja Huancayo.		**X**			
	3	Cambiar la Seguridad Informática Interna por otra basada en otra tecnología distinta a las anteriores.			**X**		
Política de seguridad basado en el acceso (CABLE, WIRELESS, VPN)	**1**	Cambiar la Seguridad Informática Interna por otra basada en tecnología CISCO ISE.	**X**				
	2	Mantener la Seguridad Informática Interna actualmente operativa en la agencia principal de Caja Huancayo.			**X**		
	3	Cambiar la Seguridad Informática Interna por otra basada en otra tecnología distinta a las anteriores.		**X**			

Juan Gabrihel Gabino Perez Gonzales

ANALÍSIS MEDIANTE JUICIO DE EXPERTOS

I. Presentación.

Nombre y Apellidos: Daniel Pablo Muñoz Moreno

Grado: Bachiller (Ingeniero de Sistemas)

¡Buen Día!

En la actualidad vengo ejecutando una investigación que tiene como objetivo: "Implementar políticas de seguridad para la Red LAN de Caja Huancayo, basadas en la tecnología informática Cisco ISE (Identity Services Engine)". En ese sentido, como parte de proponer una mejora en la seguridad informática de la agencia principal de Caja Huancayo, es que recurro a usted que cuenta con experiencia en la implementación de las tecnologías CISCO, para que nos brinde su parecer, basado en su juicio como profesional, con respecto a las preguntas que aparecen más abajo.

II. Indicaciones.

Marcar con una equis (X), la calificación que asignaría a cada uno de los ítems del cuestionario, marcando:

A: Excelente.
B: Bueno.
C: Regular.
D: Malo.
E: Pésimo.

III. Cuestionario.

Aspecto Consultado		Propuesta	Calificación				
			A	B	C	D	E
Vulnerabilidad en la protección del conmutador de paquetes (Switch)	1	Cambiar la Seguridad Informática Interna por otra basada en tecnología CISCO ISE.			X		
	2	Mantener la Seguridad Informática Interna actualmente operativa en la agencia principal de Caja Huancayo.				X	
	3	Cambiar la Seguridad Informática Interna por otra basada en otra tecnología distinta a las anteriores.			X		
Vulnerabilidad en la protección del punto de acceso (Access Point y WLC – Wireless Lan Controller)	1	Cambiar la Seguridad Informática Interna por otra basada en tecnología CISCO ISE.			X		
	2	Mantener la Seguridad Informática Interna actualmente operativa en la agencia principal de Caja Huancayo.			X		
	3	Cambiar la Seguridad Informática Interna por otra basada en otra tecnología distinta a las anteriores.				X	
Vulnerabilidades en la protección de MAN IN THE MIDDLE	1	Cambiar la Seguridad Informática Interna por otra basada en tecnología CISCO ISE.		X			
	2	Mantener la Seguridad Informática Interna actualmente operativa en la agencia principal de Caja Huancayo.		X			
	3	Cambiar la Seguridad Informática Interna por otra basada en otra tecnología distinta a las anteriores.		X			

Vulnerabilidades en mitigar la cantidad de dispositivos (PORT-SECURITY)	**1**	Cambiar la Seguridad Informática Interna por otra basada en tecnología CISCO ISE.		**X**			
	2	Mantener la Seguridad Informática Interna actualmente operativa en la agencia principal de Caja Huancayo.			**X**		
	3	Cambiar la Seguridad Informática Interna por otra basada en otra tecnología distinta a las anteriores.			**X**		
Políticas de seguridad NAC (Network Access Control)	**1**	Cambiar la Seguridad Informática Interna por otra basada en tecnología CISCO ISE.			**X**		
	2	Mantener la Seguridad Informática Interna actualmente operativa en la agencia principal de Caja Huancayo.			**X**		
	3	Cambiar la Seguridad Informática Interna por otra basada en otra tecnología distinta a las anteriores.				**X**	
Política de seguridad centralizada (TACACS+ y RADIUS)	**1**	Cambiar la Seguridad Informática Interna por otra basada en tecnología CISCO ISE.		**X**			
	2	Mantener la Seguridad Informática Interna actualmente operativa en la agencia principal de Caja Huancayo.				**X**	
	3	Cambiar la Seguridad Informática Interna por otra basada en otra tecnología distinta a las anteriores.				**X**	
Política de seguridad de gestión y administración de dispositivos finales	**1**	Cambiar la Seguridad Informática Interna por otra basada en tecnología CISCO ISE.			**X**		
	2	Mantener la Seguridad Informática Interna actualmente operativa en la agencia principal de Caja Huancayo.					**X**
	3	Cambiar la Seguridad Informática Interna por otra basada en otra tecnología distinta a las anteriores.		**X**			
Política de Seguridad para visibilidad de la red (Usuarios Microsoft Windows, MAC OS, Linux)	**1**	Cambiar la Seguridad Informática Interna por otra basada en tecnología CISCO ISE.			**X**		
	2	Mantener la Seguridad Informática Interna actualmente operativa en la agencia principal de Caja Huancayo.				**X**	
	3	Cambiar la Seguridad Informática Interna por otra basada en otra tecnología distinta a las anteriores.			**X**		
Política de seguridad basado en el acceso (CABLE, WIRELESS, VPN)	**1**	Cambiar la Seguridad Informática Interna por otra basada en tecnología CISCO ISE.			**X**		
	2	Mantener la Seguridad Informática Interna actualmente operativa en la agencia principal de Caja Huancayo.				**X**	
	3	Cambiar la Seguridad Informática Interna por otra basada en otra tecnología distinta a las anteriores.				**X**	

Daniel Pablo Muñoz Moreno

ANALÍSIS MEDIANTE JUICIO DE EXPERTOS

I. Presentación.

Nombre y Apellidos: Cesar Fidel Saavedra Lopez

Grado: Bachiller (Ingeniero de Sistemas)

¡Buen Día!

En la actualidad vengo ejecutando una investigación que tiene como objetivo: "Implementar políticas de seguridad para la Red LAN de Caja Huancayo, basadas en la tecnología informática Cisco ISE (Identity Services Engine)". En ese sentido, como parte de proponer una mejora en la seguridad informática de la agencia principal de Caja Huancayo, es que recurro a usted que cuenta con experiencia en la implementación de las tecnologías CISCO, para que nos brinde su parecer, basado en su juicio como profesional, con respecto a las preguntas que aparecen más abajo.

II. Indicaciones.

Marcar con una equis (X), la calificación que asignaría a cada uno de los ítems del cuestionario, marcando:

A: Excelente.
B: Bueno.
C: Regular.
D: Malo.
E: Pésimo.

III. Cuestionario.

Aspecto Consultado	Propuesta		Calificación				
			A	B	C	D	E
Vulnerabilidad en la protección del conmutador de paquetes (Switch)	1	Cambiar la Seguridad Informática Interna por otra basada en tecnología CISCO ISE.		X			
	2	Mantener la Seguridad Informática Interna actualmente operativa en la agencia principal de Caja Huancayo.			X		
	3	Cambiar la Seguridad Informática Interna por otra basada en otra tecnología distinta a las anteriores.			X		
Vulnerabilidad en la protección del punto de acceso (Access Point y WLC – Wireless Lan Controller)	1	Cambiar la Seguridad Informática Interna por otra basada en tecnología CISCO ISE.			X		
	2	Mantener la Seguridad Informática Interna actualmente operativa en la agencia principal de Caja Huancayo.			X		
	3	Cambiar la Seguridad Informática Interna por otra basada en otra tecnología distinta a las anteriores.			X		
Vulnerabilidades en la protección de MAN IN THE MIDDLE	1	Cambiar la Seguridad Informática Interna por otra basada en tecnología CISCO ISE.		X			
	2	Mantener la Seguridad Informática Interna actualmente operativa en la agencia principal de Caja Huancayo.		X			
	3	Cambiar la Seguridad Informática Interna por otra basada en otra tecnología distinta a las anteriores.				X	

Vulnerabilidades en mitigar la cantidad de dispositivos (PORT-SECURITY)	**1**	Cambiar la Seguridad Informática Interna por otra basada en tecnología CISCO ISE.		**X**			
	2	Mantener la Seguridad Informática Interna actualmente operativa en la agencia principal de Caja Huancayo.				**X**	
	3	Cambiar la Seguridad Informática Interna por otra basada en otra tecnología distinta a las anteriores.			**X**		
Políticas de seguridad NAC (Network Access Control)	**1**	Cambiar la Seguridad Informática Interna por otra basada en tecnología CISCO ISE.			**X**		
	2	Mantener la Seguridad Informática Interna actualmente operativa en la agencia principal de Caja Huancayo.				**X**	
	3	Cambiar la Seguridad Informática Interna por otra basada en otra tecnología distinta a las anteriores.			**X**		
Política de seguridad centralizada (TACACS+ y RADIUS)	**1**	Cambiar la Seguridad Informática Interna por otra basada en tecnología CISCO ISE.		**X**			
	2	Mantener la Seguridad Informática Interna actualmente operativa en la agencia principal de Caja Huancayo.				**X**	
	3	Cambiar la Seguridad Informática Interna por otra basada en otra tecnología distinta a las anteriores.				**X**	
Política de seguridad de gestión y administración de dispositivos finales	**1**	Cambiar la Seguridad Informática Interna por otra basada en tecnología CISCO ISE.			**X**		
	2	Mantener la Seguridad Informática Interna actualmente operativa en la agencia principal de Caja Huancayo.					**X**
	3	Cambiar la Seguridad Informática Interna por otra basada en otra tecnología distinta a las anteriores.		**X**			
Política de Seguridad para visibilidad de la red (Usuarios Microsoft Windows, MAC OS, Linux)	**1**	Cambiar la Seguridad Informática Interna por otra basada en tecnología CISCO ISE.			**X**		
	2	Mantener la Seguridad Informática Interna actualmente operativa en la agencia principal de Caja Huancayo.				**X**	
	3	Cambiar la Seguridad Informática Interna por otra basada en otra tecnología distinta a las anteriores.					**X**
Política de seguridad basado en el acceso (CABLE, WIRELESS, VPN)	**1**	Cambiar la Seguridad Informática Interna por otra basada en tecnología CISCO ISE.		**X**			
	2	Mantener la Seguridad Informática Interna actualmente operativa en la agencia principal de Caja Huancayo.				**X**	
	3	Cambiar la Seguridad Informática Interna por otra basada en otra tecnología distinta a las anteriores.		**X**			

Cesar Fidel Saavedra Lopez

ANALÍSIS MEDIANTE JUICIO DE EXPERTOS

I. Presentación.

Nombre y Apellidos: Víctor Eduardo Alva Calcina

Grado: Bachiller (Ingeniero de Sistemas)

¡Buen Día!

En la actualidad vengo ejecutando una investigación que tiene como objetivo: "Implementar políticas de seguridad para la Red LAN de Caja Huancayo, basadas en la tecnología informática Cisco ISE (Identity Services Engine)". En ese sentido, como parte de proponer una mejora en la seguridad informática de la agencia principal de Caja Huancayo, es que recurro a usted que cuenta con experiencia en la implementación de las tecnologías CISCO, para que nos brinde su parecer, basado en su juicio como profesional, con respecto a las preguntas que aparecen más abajo.

II. Indicaciones.

Marcar con una equis (X), la calificación que asignaría a cada uno de los ítems del cuestionario, marcando:

A: Excelente.
B: Bueno.
C: Regular.
D: Malo.
E: Pésimo.

III. Cuestionario.

Aspecto Consultado	Propuesta		Calificación				
			A	B	C	D	E
Vulnerabilidad en la protección del conmutador de paquetes (Switch)	1	Cambiar la Seguridad Informática Interna por otra basada en tecnología CISCO ISE.	X				
	2	Mantener la Seguridad Informática Interna actualmente operativa en la agencia principal de Caja Huancayo.		X			
	3	Cambiar la Seguridad Informática Interna por otra basada en otra tecnología distinta a las anteriores.		X			
Vulnerabilidad en la protección del punto de acceso (Access Point y WLC – Wireless Lan Controller)	1	Cambiar la Seguridad Informática Interna por otra basada en tecnología CISCO ISE.	X				
	2	Mantener la Seguridad Informática Interna actualmente operativa en la agencia principal de Caja Huancayo.		X			
	3	Cambiar la Seguridad Informática Interna por otra basada en otra tecnología distinta a las anteriores.			X		
Vulnerabilidades en la protección de MAN IN THE MIDDLE	1	Cambiar la Seguridad Informática Interna por otra basada en tecnología CISCO ISE.		X			
	2	Mantener la Seguridad Informática Interna actualmente operativa en la agencia principal de Caja Huancayo.		X			
	3	Cambiar la Seguridad Informática Interna por otra basada en otra tecnología distinta a las anteriores.		X			

Vulnerabilidades en mitigar la cantidad de dispositivos (PORT-SECURITY)	**1**	Cambiar la Seguridad Informática Interna por otra basada en tecnología CISCO ISE.	**X**				
	2	Mantener la Seguridad Informática Interna actualmente operativa en la agencia principal de Caja Huancayo.				**X**	
	3	Cambiar la Seguridad Informática Interna por otra basada en otra tecnología distinta a las anteriores.			**X**		
Políticas de seguridad NAC (Network Access Control)	**1**	Cambiar la Seguridad Informática Interna por otra basada en tecnología CISCO ISE.	**X**				
	2	Mantener la Seguridad Informática Interna actualmente operativa en la agencia principal de Caja Huancayo.	**X**				
	3	Cambiar la Seguridad Informática Interna por otra basada en otra tecnología distinta a las anteriores.		**X**			
Política de seguridad centralizada (TACACS+ y RADIUS)	**1**	Cambiar la Seguridad Informática Interna por otra basada en tecnología CISCO ISE.		**X**			
	2	Mantener la Seguridad Informática Interna actualmente operativa en la agencia principal de Caja Huancayo.			**X**		
	3	Cambiar la Seguridad Informática Interna por otra basada en otra tecnología distinta a las anteriores.			**X**		
Política de seguridad de gestión y administración de dispositivos finales	**1**	Cambiar la Seguridad Informática Interna por otra basada en tecnología CISCO ISE.			**X**		
	2	Mantener la Seguridad Informática Interna actualmente operativa en la agencia principal de Caja Huancayo.				**X**	
	3	Cambiar la Seguridad Informática Interna por otra basada en otra tecnología distinta a las anteriores.	**X**				
Política de Seguridad para visibilidad de la red (Usuarios Microsoft Windows, MAC OS, Linux)	**1**	Cambiar la Seguridad Informática Interna por otra basada en tecnología CISCO ISE.		**X**			
	2	Mantener la Seguridad Informática Interna actualmente operativa en la agencia principal de Caja Huancayo.			**X**		
	3	Cambiar la Seguridad Informática Interna por otra basada en otra tecnología distinta a las anteriores.			**X**		
Política de seguridad basado en el acceso (CABLE, WIRELESS, VPN)	**1**	Cambiar la Seguridad Informática Interna por otra basada en tecnología CISCO ISE.	**X**				
	2	Mantener la Seguridad Informática Interna actualmente operativa en la agencia principal de Caja Huancayo.		**X**			
	3	Cambiar la Seguridad Informática Interna por otra basada en otra tecnología distinta a las anteriores.		**X**			

Víctor Eduardo Alva Calcina

ANALÍSIS MEDIANTE JUICIO DE EXPERTOS

I. Presentación.

Nombre y Apellidos: Jhon Ronald Castro Leiva

Grado: Bachiller (Ingeniero de Sistemas)

¡Buen Día!

En la actualidad vengo ejecutando una investigación que tiene como objetivo: "Implementar políticas de seguridad para la Red LAN de Caja Huancayo, basadas en la tecnología informática Cisco ISE (Identity Services Engine)". En ese sentido, como parte de proponer una mejora en la seguridad informática de la agencia principal de Caja Huancayo, es que recurro a usted que cuenta con experiencia en la implementación de las tecnologías CISCO, para que nos brinde su parecer, basado en su juicio como profesional, con respecto a las preguntas que aparecen más abajo.

II. Indicaciones.

Marcar con una equis (X), la calificación que asignaría a cada uno de los ítems del cuestionario, marcando:

A: Excelente.
B: Bueno.
C: Regular.
D: Malo.
E: Pésimo.

III. Cuestionario.

Aspecto Consultado	Propuesta		Calificación				
			A	B	C	D	E
Vulnerabilidad en la protección del conmutador de paquetes (Switch)	1	Cambiar la Seguridad Informática Interna por otra basada en tecnología CISCO ISE.	X				
	2	Mantener la Seguridad Informática Interna actualmente operativa en la agencia principal de Caja Huancayo.		X			
	3	Cambiar la Seguridad Informática Interna por otra basada en otra tecnología distinta a las anteriores.			X		
Vulnerabilidad en la protección del punto de acceso (Access Point y WLC – Wireless Lan Controller)	1	Cambiar la Seguridad Informática Interna por otra basada en tecnología CISCO ISE.	X				
	2	Mantener la Seguridad Informática Interna actualmente operativa en la agencia principal de Caja Huancayo.			X		
	3	Cambiar la Seguridad Informática Interna por otra basada en otra tecnología distinta a las anteriores.		X			
Vulnerabilidades en la protección de MAN IN THE MIDDLE	1	Cambiar la Seguridad Informática Interna por otra basada en tecnología CISCO ISE.	X				
	2	Mantener la Seguridad Informática Interna actualmente operativa en la agencia principal de Caja Huancayo.			X		
	3	Cambiar la Seguridad Informática Interna por otra basada en otra tecnología distinta a las anteriores.			X		

Vulnerabilidades en mitigar la cantidad de dispositivos (PORT-SECURITY)	**1**	Cambiar la Seguridad Informática Interna por otra basada en tecnología CISCO ISE.	**X**				
	2	Mantener la Seguridad Informática Interna actualmente operativa en la agencia principal de Caja Huancayo.				**X**	
	3	Cambiar la Seguridad Informática Interna por otra basada en otra tecnología distinta a las anteriores.		**X**			
Políticas de seguridad NAC (Network Access Control)	**1**	Cambiar la Seguridad Informática Interna por otra basada en tecnología CISCO ISE.	**X**				
	2	Mantener la Seguridad Informática Interna actualmente operativa en la agencia principal de Caja Huancayo.	**X**				
	3	Cambiar la Seguridad Informática Interna por otra basada en otra tecnología distinta a las anteriores.				**X**	
Política de seguridad centralizada (TACACS+ y RADIUS)	**1**	Cambiar la Seguridad Informática Interna por otra basada en tecnología CISCO ISE.	**X**				
	2	Mantener la Seguridad Informática Interna actualmente operativa en la agencia principal de Caja Huancayo.			**X**		
	3	Cambiar la Seguridad Informática Interna por otra basada en otra tecnología distinta a las anteriores.			**X**		
Política de seguridad de gestión y administración de dispositivos finales	**1**	Cambiar la Seguridad Informática Interna por otra basada en tecnología CISCO ISE.		**X**			
	2	Mantener la Seguridad Informática Interna actualmente operativa en la agencia principal de Caja Huancayo.		**X**			
	3	Cambiar la Seguridad Informática Interna por otra basada en otra tecnología distinta a las anteriores.	**X**				
Política de Seguridad para visibilidad de la red (Usuarios Microsoft Windows, MAC OS, Linux)	**1**	Cambiar la Seguridad Informática Interna por otra basada en tecnología CISCO ISE.		**X**			
	2	Mantener la Seguridad Informática Interna actualmente operativa en la agencia principal de Caja Huancayo.		**X**			
	3	Cambiar la Seguridad Informática Interna por otra basada en otra tecnología distinta a las anteriores.			**X**		
Política de seguridad basado en el acceso (CABLE, WIRELESS, VPN)	**1**	Cambiar la Seguridad Informática Interna por otra basada en tecnología CISCO ISE.	**X**				
	2	Mantener la Seguridad Informática Interna actualmente operativa en la agencia principal de Caja Huancayo.			**X**		
	3	Cambiar la Seguridad Informática Interna por otra basada en otra tecnología distinta a las anteriores.		**X**			

Jhon Ronald Castro Leiva

ANALÍSIS MEDIANTE JUICIO DE EXPERTOS

I. Presentación.

Nombre y Apellidos: Harry Eduardo Aroni Palacios

Grado: Bachiller (Ingeniero de Sistemas)

¡Buen Día!

En la actualidad vengo ejecutando una investigación que tiene como objetivo: "Implementar políticas de seguridad para la Red LAN de Caja Huancayo, basadas en la tecnología informática Cisco ISE (Identity Services Engine)". En ese sentido, como parte de proponer una mejora en la seguridad informática de la agencia principal de Caja Huancayo, es que recurro a usted que cuenta con experiencia en la implementación de las tecnologías CISCO, para que nos brinde su parecer, basado en su juicio como profesional, con respecto a las preguntas que aparecen más abajo.

II. Indicaciones.

Marcar con una equis (X), la calificación que asignaría a cada uno de los ítems del cuestionario, marcando:

A: Excelente.
B: Bueno.
C: Regular.
D: Malo.
E: Pésimo.

III. Cuestionario.

Aspecto Consultado	Propuesta		Calificación				
			A	B	C	D	E
Vulnerabilidad en la protección del conmutador de paquetes (Switch)	1	Cambiar la Seguridad Informática Interna por otra basada en tecnología CISCO ISE.		X			
	2	Mantener la Seguridad Informática Interna actualmente operativa en la agencia principal de Caja Huancayo.		X			
	3	Cambiar la Seguridad Informática Interna por otra basada en otra tecnología distinta a las anteriores.			X		
Vulnerabilidad en la protección del punto de acceso (Access Point y WLC – Wireless Lan Controller)	1	Cambiar la Seguridad Informática Interna por otra basada en tecnología CISCO ISE.		X			
	2	Mantener la Seguridad Informática Interna actualmente operativa en la agencia principal de Caja Huancayo.			X		
	3	Cambiar la Seguridad Informática Interna por otra basada en otra tecnología distinta a las anteriores.					X
Vulnerabilidades en la protección de MAN IN THE MIDDLE	1	Cambiar la Seguridad Informática Interna por otra basada en tecnología CISCO ISE.		X			
	2	Mantener la Seguridad Informática Interna actualmente operativa en la agencia principal de Caja Huancayo.					X
	3	Cambiar la Seguridad Informática Interna por otra basada en otra tecnología distinta a las anteriores.			X		

Vulnerabilidades en mitigar la cantidad de dispositivos (PORT-SECURITY)	**1**	Cambiar la Seguridad Informática Interna por otra basada en tecnología CISCO ISE.		**X**			
	2	Mantener la Seguridad Informática Interna actualmente operativa en la agencia principal de Caja Huancayo.			**X**		
	3	Cambiar la Seguridad Informática Interna por otra basada en otra tecnología distinta a las anteriores.			**X**		
Políticas de seguridad NAC (Network Access Control)	**1**	Cambiar la Seguridad Informática Interna por otra basada en tecnología CISCO ISE.			**X**		
	2	Mantener la Seguridad Informática Interna actualmente operativa en la agencia principal de Caja Huancayo.		**X**			
	3	Cambiar la Seguridad Informática Interna por otra basada en otra tecnología distinta a las anteriores.					**X**
Política de seguridad centralizada (TACACS+ y RADIUS)	**1**	Cambiar la Seguridad Informática Interna por otra basada en tecnología CISCO ISE.			**X**		
	2	Mantener la Seguridad Informática Interna actualmente operativa en la agencia principal de Caja Huancayo.			**X**		
	3	Cambiar la Seguridad Informática Interna por otra basada en otra tecnología distinta a las anteriores.				**X**	
Política de seguridad de gestión y administración de dispositivos finales	**1**	Cambiar la Seguridad Informática Interna por otra basada en tecnología CISCO ISE.			**X**		
	2	Mantener la Seguridad Informática Interna actualmente operativa en la agencia principal de Caja Huancayo.				**X**	
	3	Cambiar la Seguridad Informática Interna por otra basada en otra tecnología distinta a las anteriores.		**X**			
Política de Seguridad para visibilidad de la red (Usuarios Microsoft Windows, MAC OS, Linux)	**1**	Cambiar la Seguridad Informática Interna por otra basada en tecnología CISCO ISE.			**X**		
	2	Mantener la Seguridad Informática Interna actualmente operativa en la agencia principal de Caja Huancayo.				**X**	
	3	Cambiar la Seguridad Informática Interna por otra basada en otra tecnología distinta a las anteriores.			**X**		
Política de seguridad basado en el acceso (CABLE, WIRELESS, VPN)	**1**	Cambiar la Seguridad Informática Interna por otra basada en tecnología CISCO ISE.	**X**				
	2	Mantener la Seguridad Informática Interna actualmente operativa en la agencia principal de Caja Huancayo.			**X**		
	3	Cambiar la Seguridad Informática Interna por otra basada en otra tecnología distinta a las anteriores.		**X**			

Harry Eduardo Aroni Palacios

Anexo 6. Evidencia de acta de consentimiento de autorización de Caja Huancayo

Caja Huancayo

(10/04/2022 - Huancayo)

Dulio Rodríguez Riveros
Jefe de Infraestructura Tecnológica)
CAJA HUANCAYO
Calle Real 341 – 343 Huancayo
(064) 481000

Asunto: ACTA DE CONSENTIMIENTO PARA LA PROPUESTA DE IMPLEMENTACIÓN DE POLÍTICAS DE SEGURIDAD EN LA RED LAN DE CAJA HUANCAYO CON CISCO ISE (IDENTITY SERVICES ENGINE)

Por medio de la presente, yo, Gabriel Gregorio Huamán Mauricio identificado con DNI 46895664 con domicilio en: Jr. Chiclayo 101 el Tambo, otorgo la presente carta de consentimiento para la propuesta de Implementación de políticas de seguridad en la red LAN de Caja Huancayo con CISCO ISE (Identity Services Engine).

El único fin de dicho consentimiento es para poder realizar mi tesis y proponer la implementación para mejorar las políticas de seguridad en la RED LAN de la Caja Huancayo con CISCO ISE.

Sin más por el momento, agradezco la atención prestada la presente Acta, quedando a sus órdenes para cualquier, duda, aclaración o comentario que pudiese surgir de la información aquí presentada.

Reciba un cordial saludo,
Atentamente,

Gabriel Huamán Mauricio
Analista de Redes y Comunicaciones

Dulio Rodríguez Riveros
Jefe del Dpto. de Infraestructura Tecnológica

Anexo 7. Resolución S.B.S. Nº504-2021 (motivo de la implementación)

Resolución S.B.S.

Nº 504-2021

La Superintendenta de Banca, Seguros y Administradoras Privadas de Fondos de Pensiones

Artículo 8. Función de Seguridad de Información y Ciberseguridad

8.1. Son responsabilidades de la función de seguridad de la información y ciberseguridad:

a) Proponer el Plan estratégico del SGSI-C y desarrollar los planes operativos.
b) Implementar y manejar las operaciones diarias necesarias para el funcionamiento efectivo del SGSI-C.
c) Implementar procesos de autenticación para controlar el acceso a la información y sistema que utilice la empresa, y a los servicios que provea.
d) Informar al Comité de Riesgos periódicamente sobre los riesgos que enfrenta la empresa en materia de seguridad de información y ciberseguridad.
e) Informar sobre los incidentes de seguridad de la información al Comité de Riesgos o CSIC, según los lineamientos que este establezca, y a las entidades gubernamentales que lo requieran de acuerdo con la normativa vigente.
f) Evaluar las amenazas de seguridad en las estrategias de continuidad del negocio que la empresa defina y proponer medidas de mitigación de riesgos, así como informar al Comité de Riesgos o CSIC.
g) En general realizar lo necesario para dar debido cumplimiento a lo dispuesto en el presente Reglamento.

8.2. Las empresas deben implementar la función de seguridad de la información y ciberseguridad. Además deben contar con un equipo de trabajo multidisciplinario de manejo de incidentes de ciberseguridad, el cual debe estar capacitado para implementar el plan y los procedimientos para gestionarlos, conformado por representantes de las áreas que permitan prever en ellos los aspectos legales, técnicos y organizacionales, de forma consistente con los requerimientos del programa de ciberseguridad establecidos en este Reglamento.

8.3. Las empresas comprendidas en el régimen simplificado, deben contar con una función de seguridad de la información y ciberseguridad, que cumpla por lo menos con los literales a), e), f) y g) del párrafo 8.1 del presente artículo.

Anexo 8. Resultados de la ficha de validación del instrumento por 3 expertos

FICHA DE VALIDACIÓN DE INSTRUMENTO DE RECOLECCIÓN DE DATOS POR CRITERIO DE JUECES

I. DATOS GENERALES

1.1. Apellidos y nombres del juez: Ing. Henry Iván Crisostomo Ullico

1.2. Título y/o Grado académico: Ingeniero de Sistemas e informática

1.3. Institución de estudios superiores: Universidad Continental

1.4. Cargo e institución donde labora: Supervisor de redes de transporte

1.5. Título de la investigación: Propuesta de implementación de políticas de seguridad basado en cisco ISE (Identity Services Engine) en la Red LAN de Caja Huancayo.

1.6. Apellidos y nombres de los tesistas:

- Gabriel Gregorio Huaman Mauricio.
- Geanlee Ronald Rojas Marcelo.
- John Kennedy Rojas Marcelo.

II. ASPECTO DE LA VALIDACIÓN

ÍTEMS	SI	NO	SUGERENCIAS
1. Las preguntas persiguen fines del objetivo general.	X		
2. Las preguntas persiguen los fines del objetivo específico.	X		
3. Las preguntas abarcan variables e indicadores.	X		
4. Los ítems permiten medir el problema de la investigación.	X		
5. Los términos utilizados son claros y comprensibles.	X		
6. El grado de dificultad o complejidad es aceptable.	X		
7. Los ítems permiten contrastar la hipótesis de la investigación.	X		
8. Los reactivos siguen un orden lógico.	X		
9. Se deben considerar otros ítems.		X	
10. Los ítems despiertan ambigüedad en el encuestado.		X	

III. CALIFICACIÓN GLOBAL (Ubique el coeficiente de validez obtenido en el intervalo respectivo y marque con un aspa en el cuadro asociado)

CATEGORÍA		INTERVALO
Desaprobado	☐	0 – 3
Observado	☐	4 – 7
Aprobado	X	8 – 10

Fecha: 31 / 12 / 2022

Firma del Juez

FICHA DE VALIDACIÓN DE INSTRUMENTO DE RECOLECCIÓN DE DATOS POR CRITERIO DE JUECES

I. DATOS GENERALES

1.1. Apellidos y nombres del juez: .De Rojas Galván Iván.....
.....

1.2. Título y/o Grado académico: .....Ingeniero Electrónico.....

1.3. Institución de estudios superiores: .Universidad Ricardo Palma.....

1.4. Cargo e institución donde labora: ..Jefe de Proyectos / Telefonica Ingenieria de Seguridad.....

1.5. Título de la investigación: Propuesta de implementación de políticas de seguridad basado en cisco ISE (Identity Services Engine) en la Red LAN de Caja Huancayo.

1.6. Apellidos y nombres de los tesistas:
- Gabriel Gregorio Huaman Mauricio.
- Geanlee Ronald Rojas Marcelo.
- John Kennedy Rojas Marcelo.

II. ASPECTO DE LA VALIDACIÓN

ÍTEMS	SI	NO	SUGERENCIAS
1. Las preguntas persiguen fines del objetivo general.	x		
2. Las preguntas persiguen los fines del objetivo específico.	x		
3. Las preguntas abarcan variables e indicadores.	x		
4. Los ítems permiten medir el problema de la investigación.	x		
5. Los términos utilizados son claros y comprensibles.	x		
6. El grado de dificultad o complejidad es aceptable.	x		
7. Los ítems permiten contrastar la hipótesis de la investigación.	x		
8. Los reactivos siguen un orden lógico.	x		
9. Se deben considerar otros ítems.		x	
10. Los ítems despiertan ambigüedad en el encuestado.		x	

III. CALIFICACIÓN GLOBAL (Ubique el coeficiente de validez obtenido en el intervalo respectivo y marque con un aspa en el cuadro asociado)

CATEGORÍA		INTERVALO
Desaprobado	☐	0 – 3
Observado	☐	4 – 7
Aprobado	x	8 – 10

Fecha: 28/12/2022 …./…./…..

IVAN REYNALDO
DE ROJAS GALVAN
INGENIERO ELECTRONICO
Reg. CIP Nº 177383

Firma del Juez

FICHA DE VALIDACIÓN DE INSTRUMENTO DE RECOLECCIÓN DE DATOS POR CRITERIO DE JUECES

I. DATOS GENERALES

1.1. Apellidos y nombres del juez: RODRIGUEZ RIVEROS, DULIO HECTOR

1.2. Título y/o Grado académico: INGENIERO DE SISTEMAS

1.3. Institución de estudios superiores: UNCP

1.4. Cargo e institución donde labora: CHAC - HUANCAYO S.A. JEFE DE INFRAESTRUCTURA TECNOLÓGICA

1.5. Título de la investigación: Propuesta de implementación de políticas de seguridad basado en cisco ISE (Identity Services Engine) en la Red LAN de Caja Huancayo.

1.6. Apellidos y nombres de los tesistas:

- Gabriel Gregorio Huaman Mauricio.
- Geanlee Ronald Rojas Marcelo.
- John Kennedy Rojas Marcelo.

II. ASPECTO DE LA VALIDACIÓN

ÍTEMS	SI	NO	SUGERENCIAS
1. Las preguntas persiguen fines del objetivo general.	X		
2. Las preguntas persiguen los fines del objetivo específico.	X		
3. Las preguntas abarcan variables e indicadores.	X		
4. Los ítems permiten medir el problema de la investigación.	X		
5. Los términos utilizados son claros y comprensibles.	X		
6. El grado de dificultad o complejidad es aceptable.	X		
7. Los ítems permiten contrastar la hipótesis de la investigación.	X		
8. Los reactivos siguen un orden lógico.	X		
9. Se deben considerar otros ítems.		X	
10. Los ítems despiertan ambigüedad en el encuestado.		X	

III. CALIFICACIÓN GLOBAL (Ubique el coeficiente de validez obtenido en el intervalo respectivo y marque con un aspa en el cuadro asociado)

CATEGORÍA		INTERVALO
Desaprobado	☐	0 – 3
Observado	☐	4 – 7
Aprobado	☒	8 – 10

Fecha: 30/12/2022

Dulio H. Rodriguez Riveros
Jefe de Infraestructura Tecnológica (e)
CHAC - HUANCAYO S.A.

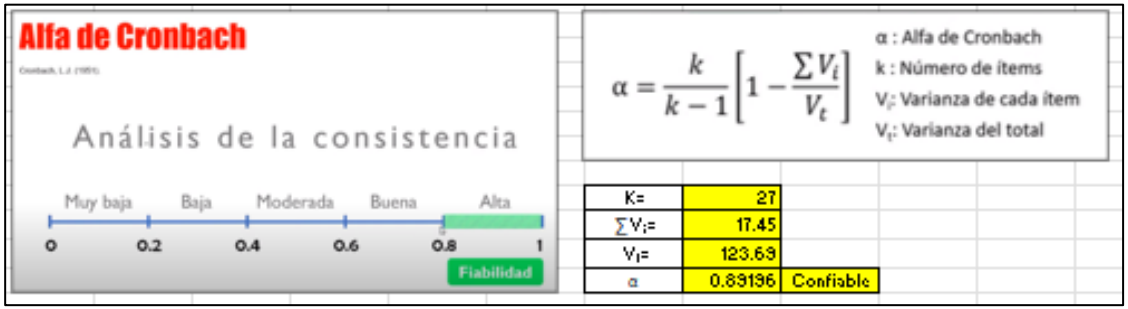
Firma del Juez

Anexo 9. Resultado de la confiabilidad del instrumento

	Calificacion de propuestas																									
Sujetos	P1	P2	P3	P4	P5	P6	P7	P8	P9	P10	P11	P12	P13	P14	P15	P16	P17	P18	P19	P20	P21	P22	P23	P24	P25	P26	P27
Juez 1	A	B	E	B	B	B	B	B	C	A	B	C	A	B	B	B	C	C	A	B	A	B	C	B	A	D	C
Juez 2	B	C	C	B	D	D	A	D	C	B	C	E	B	B	D	B	C	D	B	E	A	C	D	C	A	B	C
Juez 3	B	B	E	B	C	B	C	B	D	B	E	E	B	A	D	C	B	C	B	C	A	B	D	C	A	C	E
Juez 4	A	C	D	B	B	B	B	D	C	A	E	D	A	A	B	A	D	C	B	E	A	B	C	D	A	B	D
Juez 5	A	C	C	A	C	B	B	C	C	A	C	B	A	A	B	A	C	B	C	B	A	B	B	C	A	C	B
Juez 6	C	D	C	C	C	D	B	B	B	B	C	C	C	C	D	B	D	D	C	E	B	C	D	C	C	D	D
Juez 7	B	C	C	C	C	C	B	B	D	B	D	C	C	D	C	B	D	D	C	E	B	C	D	E	B	D	B
Juez 8	A	B	B	A	B	C	B	B	B	A	D	C	A	A	B	B	C	C	C	D	A	B	C	C	A	B	B
Juez 9	A	B	C	A	C	B	A	C	C	A	D	B	A	A	D	A	C	C	B	B	A	B	B	C	A	C	B
Juez 10	B	B	C	B	C	E	B	E	C	B	C	C	C	B	E	C	C	D	C	D	B	C	D	C	A	C	B

	Calificacion de propuestas																											
Sujetos	P1	P2	P3	P4	P5	P6	P7	P8	P9	P10	P11	P12	P13	P14	P15	P16	P17	P18	P19	P20	P21	P22	P23	P24	P25	P26	P27	
Juez 1	5	4	1	4	4	4	4	4	3	5	4	3	5	4	4	4	3	3	5	4	5	4	3	4	5	2	3	103
Juez 2	4	3	3	4	2	2	5	2	3	4	3	1	4	4	2	4	3	2	4	1	5	3	2	3	5	4	3	85
Juez 3	4	4	1	4	3	4	3	4	2	4	1	1	4	5	2	3	4	3	4	3	5	4	2	3	5	3	1	86
Juez 4	5	3	2	4	4	4	4	2	3	5	1	2	5	5	4	5	2	3	4	1	5	4	3	2	5	4	2	93
Juez 5	5	3	3	5	3	4	4	3	3	5	3	4	5	5	4	5	3	4	3	4	5	4	4	3	5	3	4	106
Juez 6	3	2	3	3	3	2	4	4	4	4	3	3	3	3	2	4	2	2	3	1	4	3	2	3	3	2	2	77
Juez 7	4	3	3	3	3	3	4	4	2	4	2	3	3	2	3	4	2	2	3	1	4	3	2	1	4	2	4	78
Juez 8	5	4	4	5	4	3	4	4	4	5	2	3	5	5	4	4	3	3	3	2	5	4	3	3	5	4	4	104
Juez 9	5	4	3	5	3	4	5	3	3	5	2	4	5	5	2	5	3	3	4	4	5	4	4	3	5	3	4	105
Juez 10	4	4	3	4	3	1	4	1	3	4	3	3	3	4	1	3	3	2	3	2	4	3	2	3	5	3	4	82
	0.44	0.44	0.84	0.49	0.36	1.09	0.29	1.09	0.4	0.25	0.84	1.01	0.76	0.96	1.16	0.49	0.36	0.41	0.44	1.61	0.21	0.24	0.61	0.56	0.41	0.6	1.09	123.69
	V_i = Varianza de cada ítem																											V_t = Varianza total

TOTAL



K=	27	
$\sum V_i$=	17.45	
V_t=	123.69	
α	0.89196	Confiable

Anexo 10. Aprobación de estandarización en la marca Cisco para los equipos de comunicaciones y solución de telefonía

Memorandum N° 02244-2021-G-CMACHYO

DE	:	GERENCIA MANCOMUNADA CMAC-HUANCAYO S.A.
A	:	RODRIGUEZ RIVEROS, DULIO HECTOR JEFE DE INFRAESTRUCTURA TECNOLOGICA (E)
ASUNTO	:	**APROBACIÓN DE ESTANDARIZACION EN LA MARCA CISCO PARA LOS EQUIPOS DE COMUNICACIONES Y SOLUCIÓN DE TELEFONIA**
REFERENCIA	:	Informe N° 00051-2021-DIT-CMACHYO Informe N° 00166-2021-DAL-CMACHYO
FECHA	:	Huancayo, martes 23 de febrero del 2021

Considerando lo indicado en el Informe N° 00051-2021-DIT-CMACHYO (23.02.21) y considerando la opinión del departamento de Asesoría Legal mediante Informe N° 00166-2021-DAL-CMACHYO (23.02.21), por el presente se comunica que, en Comité de Gerencia mediante **Acuerdo N° 0297-2021 (23.02.21)** se acordó aprobar la estandarización de la marca Cisco para equipos de comunicaciones Switch, Router o Gateway de Voz, Servidores físicos y virtuales para telefonía IP, Teléfonos IP y herramientas de administración y gestión tales como: Cisco Prime Infraestructure, Cisco DNA (Digital Network Architectura), Cisco ISE (Identity Services Engine), Cisco SDN (Redes definidas por Software) y Cisco ACI y APIC.

Por lo que se encarga, proceder según corresponda.

Atentamente,

Firmado por:

VALDIVIA MORAN,VICTOR ANDRES
GERENTE DE OPERACIONES Y FINANZAS
24/02/2021 09:34:58 a.m.

NUÑEZ PORRAS,JOSE MARIA
GERENTE DE ADMINISTRACION
24/02/2021 09:42:51 a.m.

C.c. :

ESPINOZA ORTIZ, CAROLINA LISSET
JEFE DE LOGISTICA
MEDINA VILCAPOMA, ROGER JHONATAN
ASISTENTE DE LOGISTICA (E)
MENDOZA CABALLERO, ENRIQUE
SUB JEFE DE INFRAESTRUCTURA TECNOLOGICA
HUALLULLO PRIETO, PAUL
ASISTENTE DE REDES Y COMUNICACIONES (E)