



**UNIVERSIDAD NACIONAL DE CHIMBORAZO
FACULTAD DE INGENIERÍA
CARRERA DE SISTEMAS Y COMPUTACIÓN**

**GUÍA DE IMPLEMENTACIÓN DE POLÍTICAS DE CONTROL PARA MITIGAR
LOS CIBERATAQUES BASADOS EN EL MODELO CARDING EN LA COAC
“RIOBAMBA LTDA.”**

Trabajo de titulación para optar al título de Ingeniera en Sistemas y Computación

Autor:

Paredes Díaz, Karen Valeria

Tutor:

PhD. Lorena Paulina Molina Valdiviezo

Riobamba, Ecuador. 2022

PÁGINA DE ACEPTACIÓN

Los miembros del Tribunal de Graduación del proyecto de investigación de título:
**GUÍA DE IMPLEMENTACIÓN DE POLÍTICAS DE CONTROL PARA MITIGAR
LOS CIBERATAQUES BASADOS EN EL MODELO CARDING EN LA COAC
“RIOBAMBA LTDA”** presentado por la Srta. Karen Valeria Paredes Díaz, dirigido por
PhD. Lorena Paulina Molina Valdiviezo.

Una vez escuchada la defensa oral y revisado el informe final del proyecto de investigación
con fines de graduación escrito en el cual se ha constatado el cumplimiento de las
observaciones realizadas, remite la presente para el uso y custodia en la biblioteca de la
Facultad de Ingeniería de la UNACH.

Para constancia de lo expuesto firman:



Firmado electrónicamente por:
**LORENA PAULINA
MOLINA
VALDIVIEZO**

Ph.D. Lorena Molina
TUTORA



Firmado electrónicamente por:
**ANA ELIZABETH
CONGACHA AUSHAY**

Ing. Anita Congacha
MIEMBRO DEL TRIBUNAL



Firmado electrónicamente por:
**FERNANDO
TIVERIO MOLINA
GRANJA**

Ing. Fernando Molina
MIEMBRO DEL TRIBUNAL

DERECHOS DE AUTORIA

Yo, Karen Valeria Paredes Díaz, con cedula de ciudadanía 172358731-5, autora del trabajo de investigación titulado: **Guía de implementación de políticas de control para mitigar los ciberataques basados en el modelo Carding en COAC “Riobamba Ltda.”** Certifico que la producción, ideas, opiniones, criterios, contenidos y conclusiones expuestas son de mí exclusiva responsabilidad.

A sí mismo, cedo a la Universidad Nacional de Chimborazo, en forma no exclusiva, los derechos para su uso, comunicación pública, distribución, divulgación y/o reproducción total o parcia, por medio físico o digital; en esta cesión se entiende que el cesionario no podrá obtener beneficios económicos. La posible reclamación de terceros respecto de los derechos de autora de la obra referida será de mi entera responsabilidad; librando a la Universidad Nacional de Chimborazo de posibles obligaciones.

En Riobamba. 28 de marzo de 2022



Karen Valeria Paredes Díaz
172358731-5
Autora

AGRADECIMIENTO

En primera instancia quiero agradecer a Dios por la vida y por darme la oportunidad de culminar con éxito mi carrera del cual me siento tan orgullosa.

Mil gracias a mis padres por ser los principales promotores en mi carrera, por haberme proporcionado la mejor educación y lecciones de vida, enseñándome que con esfuerzo, trabajo y constancia todo se consigue.

Agradezco mucho por la ayuda de mis maestros, compañero y en especial a mi tutora Ing. Lorena Molina que con su ayuda y conocimiento fue posible realizar esta investigación.

Karen Valeria Paredes Díaz

DEDICATORIA

Esta tesis se la dedico de manera muy especial al forjador de mi camino, a mi padre celestial Jehová Dios que me dio la capacidad y la inteligencia para llegar hacer profesional, me levanto en mis continuos tropiezos, al creador de mis amados padres Pablo Paredes Viteri y Ligia Patricia Díaz quienes siempre me apoyaron incondicionalmente en la parte moral y económica para poder cumplir con mi meta, gracias a ellos por confiar y creer en mí.

A mi amado hijo Jair quien ha sido el motor y razón de mi vida fuente de motivación para poder superarme cada día y tener un futuro mejor.

A Danny de quien no me arrepiento de haberle conocido, a su lado aprendí muchas cosas, conociendo mi lado tierno, loco y sincero he incluso despertando en mi mucha ilusión, pero enseñándome que jamás se para de aprender, la vida nunca para de enseñar. Comprendiendo que las cosas que van a ser para uno el mismo destino las guarda hasta que lleguemos a ellas con mucho esfuerzo.

Y finalmente a mis amigos quien sin esperar nada a cambio compartieron sus conocimientos, alegrías y tristezas y a todas aquellas personas y familiares quienes durante esta etapa de educación estuvieron apoyándome y así logrando que este sueño se haga realidad.

Karen Valeria Paredes Díaz

ÍNDICE GENERAL

AGRADECIMIENTO
DEDICATORIA.....
RESUMEN
INTRODUCCIÓN	14
CAPITULO I.....	16
1. PLANTEAMIENTO DEL PROBLEMA.....	16
1.1 Problema y justificación.....	16
1.2. Objetivos	17
Objetivo General	17
Objetivos Específicos	17
CAPITULO II	18
2. MARCO TEÓRICO	18
2.1. Seguridad Informática	18
2.2. Riesgos informáticos	18
2.3. Ciberataque	18
2.4. Tipos de Ataques	19
2.4.1. Acceso físico.....	19
2.4.2. Interceptación de comunicaciones:	19
2.4.3. Denegaciones de servicio:.....	19
2.4.4. Intrusiones	20
2.5. Ciberseguridad	20
2.6. Seguridad de la información	21
2.7. Riesgos y amenazas de la ciberseguridad	21
2.8. Carding	22
2.8.1. Metodologías empleadas para el Carding.....	22
2.8.1.2. El phishing	22

2.8.1.3. Malware rootkit	22
2.8.1.4. El Skimming	23
2.8.1.5. BINS	23
2.8.1.6. Cash-Out	23
2.9. Vulnerabilidad.....	24
2.10. Métodos de seguridad para mitigar el fraude	24
2.10.1. Autenticación multifactor para mitigar el fraude	24
2.10.2. Aplicación de normas PCI-DSS (Payment Card Industry Data Security Standard)	24
2.10.3. Seguridad de la Información.....	25
2.10.4. Estándares Internacionales.....	25
2.10.5. ISO / IEC 27001	25
2.10.6. Estimación de riesgos.....	26
2.10.7. Sistema de Gestión de la Seguridad de la Información.	26
2.10.8. Tratamiento de riesgos.	26
2.10.9. Aceptación de riesgos.	29
2.10.10. Comunicación de riesgos.	31
2.10.11. Monitoreo y revisión de riesgos.	32
2.11. Sector financiero	33
2.12. Metodología ENISA.....	34
2.12.1. Objetivos de seguridad.....	34
2.13. Metodología APCERT	35
2.13.1. Objetivos de seguridad.....	36
CAPITULO III.....	37
3. METODOLOGIA.....	37
3.1. Tipo de Estudio	37
3.1.1. Según el objeto de estudio	37
3.1.2. Según el nivel de conocimiento.....	37
3.2. Según el método a utilizar	37
3.3. Procedimientos.....	38
3.3.1. Técnica de investigación	38
3.3.2. Instrumento de Recolección de datos.....	38

3.4. Procesamiento y análisis	38
3.4.1. Parámetros de las metodologías ENISA y APCERT	39
3.4.1.1. Metodología ENISA.....	39
3.4.1.2. Metodología APCERT	41
3.5. Comparaciones de metodologías	42
3.6. Procedimiento de trabajo:	46
CAPITULO IV	48
4. ANÁLISIS Y RESULTADOS	48
5. CONCLUSIONES Y RECOMENDACIONES	63
5.1. Conclusiones	63
5.2. Recomendaciones	64
6. BIBLIOGRAFÍA	65
ANEXOS	70
ANEXO A.....	70
ENTREVISTA.....	70
ANEXO B.....	78
ENCUESTA	78
ANEXO C.....	79
MATRIZ DE EVALUACION DE INSTRUMENTOS EVALUADOS POR EXPERTOS EN SEGURIDAD.....	79
1.1. SEGURIDAD FÍSICA	2
1.1.1. Hardware y Software.....	2
1.1.2. Áreas de trabajo	2
1.2. CONTROL DE ACCESO FÍSICO A OFICINAS Y ZONAS RESTRINGIDAS.....	2
1.2.1. INSTALACIONES	2
1.3. CONTROL DE APLICACIONES EN ESTACIONES DE TRABAJO	3
1.4. CONTROL DE DATOS EN LAS APLICACIONES.....	3
1.5. SEGURIDAD LÓGICA	3

1.5.1. ASPECTOS GENERALES.....	3
1.5.2. IDENTIFICACIÓN DE USUARIOS.....	4
1.6. AUTENTICACIÓN EN LA RED	4
1.7. PASSWORD.....	4
1.8. LA INFORMACIÓN	5
1.8.1. POLITICAS GENERALES	5
1.9. EL CORREO ELECTRÓNICO	5
1.10. SEÑALES POR ATAQUES DE CARDING	5
1.11. COMO PROTEGERSE DEL CARDING.....	6

ÍNDICE DE TABLAS

TABLA 1 COMPARACIÓN CATEGORÍA HARDWARE	43
TABLA 2 COMPARACIÓN CATEGORÍA SOFTWARE.....	43
TABLA 3 MEDIDAS DE CONTROL	44
TABLA 4 MARCO DE CONTROLES	45
TABLA 5 COMPARACIÓN DE LAS DOS METODOLOGÍAS	60

ÍNDICE DE FIGURAS

FIGURA 1	COPIAS DE SEGURIDAD	48
FIGURA 2	CONTROL DE PERSONAL EXTERNO E INTERNO.....	49
FIGURA 3	PERFILES DE USUARIO.....	50
FIGURA 4	CONTROL DE SOFTWARE INSTALADOS	51
FIGURA 5	APLICACIONES PARA DETERMINAR RIESGOS DE SEGURIDAD....	52
FIGURA 6	EQUIPOS PROTEGIDOS EN LA EMPRESA	53
FIGURA 7	PROTECCIÓN DE LOS DATOS.....	54
FIGURA 8	CONTROLES DE ACCESO.....	55
FIGURA 9	POLÍTICAS EN LOS EQUIPOS INFORMÁTICOS	56
FIGURA 10	IDENTIFICACIÓN DE RIESGOS INFORMÁTICOS	57

RESUMEN

En la actualidad los ataques informáticos no ven el tamaño de la organización o la importancia del negocio al momento en que desean perjudicar, con el avance tecnológico han descubierto métodos de ataques para cometer sus propósitos maliciosos provocando enormes pérdidas y gastos en las organizaciones e instituciones financieras.

Por consiguiente, el presente trabajo de tesis tiene como objetivo el desarrollo de una guía de implementación de políticas de control para mitigar los ciberataques basados en el modelo Carding en la COAC “Riobamba Ltda.”

Durante esta investigación se recopiló información importante sobre los parámetros de las metodologías ENISA y APCERT para su posterior comparación logrando determinar la más adecuada para el desarrollo de la guía y como técnica de recolección de información la encuesta y la entrevista, esta última aplicada al personal del área de sistemas de la institución. Después de aplicar las técnicas de recolección de información se obtuvo un 40% en relación con la identificación y análisis de los riesgos, por otra parte, en la entrevista realizada al directivo se evidenció que en el departamento de tecnología presenta un 21% de efectividad en los planes de ciberseguridad lo que afectaría de forma significativa en los riesgos asociados al modelo Carding. Con respecto a la comparación realizada entre metodologías, se obtuvo una puntuación para ENISA de 19 puntos, representando un 95% de los criterios evaluados, a diferencia de APCERT que obtuvo una puntuación de 15 puntos que representan un 75%, por lo tanto, se emplea la metodología ENISA, en este se detallan los pasos para reducir los posibles ataques basados en el modelo Carding.

Palabras Clave: Ataques informáticos, carding, riesgos, seguridad informática, vulnerabilidades.

ABSTRACT

At present, computer attacks do not see the size of the organization or the importance of the business at the time they want to harm, with technological advances they have discovered attack methods to commit their malicious purposes, causing enormous losses and expenses in organizations and financial institutions.

Therefore, this thesis work aims to develop a control policy implementation guide to mitigate cyberattacks based on the model Carded in the COAC “Riobamba Ltda.”

During this investigation, important information was collected on the parameters of the ENISA and APCERT methodologies for their subsequent comparison, determining the most appropriate for the development of the guide and as a technique for collecting information, the survey and the interview, the latter applied to the staff of the systems area of the institution. After applying the information collection techniques, 40% was obtained in relation to the identification and analysis of risks, on the other hand, in the interview with the director, it was shown that in the technology department, the results are 21% effective. cybersecurity plans, which would significantly affect the risks associated with the Carding model. With regard to the comparison made between methodologies, a score of 19 points was obtained for ENISA, representing 95% of the evaluation criteria, a difference for APCERT, which obtained a score of 15 points, which represents 75%, therefore, uses the ENISA methodology, it details the steps to reduce possible attacks based on the Carding model.

Keywords: Computer attacks, cards, risks, computer security, vulnerabilities.



Firmado electrónicamente por:
DIANA CAROLINA
CHAVEZ GUZMAN

Reviewed by:

Lcda. Diana Chávez

English Professor.

c.c. 065003795-5

INTRODUCCIÓN

Actualmente los sistemas informáticos se emplean en diversas áreas, tanto en el ámbito laboral como de entretenimiento para realizar tareas de forma automatizada y eficiente. Sin embargo, existen grupos que utilizan diferentes mecanismos para fines inapropiados y poco éticos, ya sea tratando de incursionar en el sistema sin autorización aprovechando brechas de inseguridad o engañando a los usuarios difundiendo información engañosa para obtener datos que les permita ingresar sin permiso a los sistemas, esto ocasiona vulnerabilidades facilitando los ataques, tanto con el objetivo de sustraer datos e información sensible, bloqueo de sistemas, envíos de información alarmante o falsa.

Es por ello, por lo que se ha convertido en algo imperativo el disponer de un plan de emergencias frente a posibles ataques, ya que no solo pueden inhabilitar sistemas sino también afectar la credibilidad de la institución generando posibles pérdidas a nivel económico de la misma (Freire, 2017).

Por otra parte, en el contexto financiero, se han presentado ataques en los últimos años en renombradas instituciones internacionales como, por ejemplo, State Bank of India, JPMorgan Chase, BBVA Bancomer, Toronto-Dominion Bank y Poste Italiane Sp A. (Banco Posta) causando cuantiosas pérdidas monetarias. Los fraudes con tarjetas son problemas a nivel global debido a las vulnerabilidades existentes que ocasionan desconfianza al usuario para el uso de estos dispositivos por otra parte genera pérdida de credibilidad sobre las instituciones financieras. Muchos de estos ataques son provocados por hackers y en otras por individuos con algún conocimiento técnico al respecto (Freire, 2017).

El problema es tan extenso que existen iniciativas de las empresas afectadas y del estado para realizar campañas informativas con el propósito de mantener a sus clientes al tanto de esta problemática y les permita realizar sus operaciones de forma segura. En base a lo

expuesto anteriormente, se requiere investigar tanto el ámbito nacional como internacional acerca de las modalidades de este tipo de crímenes cibernéticos y que afectan el país y los cuales se encuentran vinculados con el Carding (Duran, 2020).

Por lo anteriormente expuesto, se considera de gran importancia generar una guía a través de esta investigación que proporcione los mecanismos idóneos para mitigar los ciberataques basados en el modelo Carding dentro del COAC.

Este documento obedece a la siguiente estructura: en el Capítulo I se aborda el planteamiento del problema y los objetivos generales y específicos respectivamente, seguidamente en el Capítulo II se desarrolla el marco teórico, se aborda los conceptos y definiciones relacionadas con las variables en estudio. Asimismo, el capítulo III se plantea la metodología y se detalla el tipo de enfoque, así como de investigación a implementar. Posteriormente, en el Capítulo IV se encuentra el análisis y resultados y finalmente se exhiben las conclusiones y recomendaciones a las que se llegaron el análisis.

CAPITULO I

1. PLANTEAMIENTO DEL PROBLEMA

1.1 Problema y justificación

Muchos sistemas informáticos en la actualidad están conectados entre sí para ofrecer una gran variedad de servicios disponibles en todo momento, obteniendo acceso a bibliotecas digitales, información, noticias, inclusive se pueden realizar transmisiones en vivo denominadas streaming la cual es posible a través de diversas plataformas como Skype, Goto Meeting o Webex, es por ello, que gracias a la innovación digital las organizaciones y usuarios en general, efectúan diariamente un importante número de transacciones electrónicas financieras por medio de diferentes canales determinados por las entidades de comercio.

Actualmente se disponen de diversos instrumentos para mitigar y controlar las transacciones de índole engañoso. Sin embargo, la inexperiencia de los modus operandi se vuelve el aliado del criminal cibernético para alcanzar sus propósitos, ya que a través de prácticas poco ortodoxas logran afectar a los usuarios (Duran, 2020).

La COAC es una de las instituciones financieras que ofrece servicios a través del internet y en la cual podría ser vulnerada su seguridad, por tal motivo se ha visto conveniente realizar un estudio con el objetivo de desarrollar una guía de políticas de control financiero para mitigar los posibles ataques basándose en el modelo Carding, logrando de esta manera estar prevenir un supuesto caso de ataque cibernético.

1.2. Objetivos

Objetivo General

Desarrollar una guía de implementación de políticas de control para mitigar los ciberataques basados en el modelo Carding en la COAC.

Objetivos Específicos

- Determinar las generalidades y principales características relacionadas con el modelo Carding.
- Detallar las formas más recurrentes de vulneración de la seguridad mediante el modelo Carding.
- Analizar las diferentes clases de metodologías del Carding para la elaboración de políticas de control para mitigar los ciberataques basados en el modelo Carding.

CAPITULO II

2. MARCO TEÓRICO

2.1. Seguridad Informática

Proceso de establecer y observar un conjunto de estrategias, políticas y procedimientos para prevenir daño, alteración o sustracción los recursos informáticos de una organización y también garantizar el correcto funcionamiento de esos instrumentos (Jaramillo & Riofrío, 2015).

2.2. Riesgos informáticos

Quiroz y Macias (2017), indican que estos son amenazas que pueden ocurrir en una instancia determinada a través de vulnerabilidades que encuentran dentro de los sistemas los atacantes en un momento determinado.

2.3. Ciberataque

Es una operación indebida de carácter ilegal a través de medios informáticos que pretende causar daños a la infraestructura de sistemas de una organización o particular. Por otra parte, estos actos delictivos en muchas ocasiones no están establecidos como faltas en las leyes de algunos países (Reddy, Adepu, Mishra, & Mathur, 2021).

En este sentido, los sistemas informáticos están compuestos por cierta cantidad de componentes que permiten su correcto funcionamiento, entre ellos, electricidad, hardware, sistema operativo, aplicaciones, datos, red, usuarios y en particular los ataques se pueden realizar incursión en cada eslabón de esta cadena, aprovechando las vulnerabilidades que el atacante explote (Aguirre, 2017).

2.4. Tipos de Ataques

Según Machín y Gazapo (2016) existen varios tipos de ataques, entre los cuales se destacan:

2.4.1. Acceso físico

El bandido tiene acceso a las instalaciones:

- Interrupción del suministro eléctrico, su objetivo es generar daño físico a los equipos, causando fallas en el sistema eléctrico.
- Apagado manual del equipo se realiza de forma presencial y busca la pérdida de información.
- Vandalismo.
- Robo de disco duro.
- Monitoreo de red, con el propósito de descubrir vulnerabilidades.

2.4.2. Interceptación de comunicaciones:

El atacante busca recopilar la información de acceso y de esta forma tener ingreso no restringido al sistema.

- Secuestro de sesión, robo de perfiles o de identidad del usuario.
- Falsificación de identificación, a través de phishing, simular la identidad de un usuario o de una página.
- Redireccionamiento o alteración de mensajes, se usa para realizar ataques tipo troyano, simulando ser un correo de confianza.

2.4.3. Denegaciones de servicio:

Ataque a un sistema computarizado, así como a una red provocando que un recurso o servicio sea interrumpido e imposibilitando su acceso a sus verdaderos usuarios. Su propósito es impedir el normal funcionamiento de un servicio.

Es un ataque a un sistema de computadoras o red que causa que un servicio o recurso sea inaccesible a los usuarios legítimos. Su objetivo es interrumpir el funcionamiento normal de un servicio, sus principales ataques son producidos a través de:

- Aprovechamiento de los enflaquecimientos del protocolo TCP/IP.
- Aprovechamiento de las fragilidades del software del servidor.

2.4.4. Intrusiones

Según Freire (2017), es un ataque el cual busca dar acceso a personal no autorizado a un sistema informático, otorgándole privilegios de administrador o incluso acceder a información reservada.

- Análisis de puertos: una técnica que los hackers emplean para encontrar las debilidades de un equipo o de una red. Si bien esta técnica no es un ataque en realidad, los hackers la usan para detectar qué puertos están abiertos en un dispositivo. De acuerdo con la información de los puertos libres, puede obtenerse acceso no autorizado.
- Elevación de privilegios: Este ataque radica en el aprovechamiento de una debilidad de un sistema al transmitir determinada solicitud la cual no ha sido diseñada previamente. Por consiguiente, provoca procedimientos fuera de lo normal logrando el acceso a los sistemas con propiedades administrativas.
- Ataques malintencionados: Estos pueden incluir virus, gusanos, troyanos.

2.5. Ciberseguridad

Según Quiroz y Macías (2017) esta son las políticas, herramientas y directrices que son empleadas para resguardar un equipo informático de cualquier acción maliciosa de un atacante foráneo que intente acceder a los sistemas tanto empresariales como personales.

Según cifras publicadas de la Unión Internacional de Telecomunicaciones UIT (2020), existen algunas naciones que han marcado la diferencia en la prevención de ataques de ciberseguridad, entre ellos 193 países, cada uno con un rango específico de compromiso para enfrentar posibles ciberataques y Ecuador se encuentra en el sexto puesto de América Latina y ocupa la posición 66 en el listado de los territorios que reflejan dichos datos (Calderón, 2015).

2.6. Seguridad de la información

La seguridad de la información se refiere a la protección de seguridad técnica y de gestión adoptada por el sistema de procesamiento de datos para proteger el hardware, software y los datos de la computadora contra daños, alteraciones o exposición debido a razones accidentales o maliciosas (Conrad, Misenar, & Feldman, 2017).

2.7. Riesgos y amenazas de la ciberseguridad

El sistema de información es utilizado generalmente por un cierto rango de usuarios y la información. Por ello, en cada sistema de información se diseñan funciones de gestión de usuarios y se establecen permisos. Estas medidas pueden fortalecer la seguridad del sistema hasta cierto punto. Sin embargo, todavía existen algunos problemas en las aplicaciones prácticas. Por ejemplo, la función de administración de la autoridad del usuario de algunos sistemas de aplicación es demasiado simple para implementar un control de autoridad más detallado de manera flexible, cada sistema de aplicación no tiene una administración unificada de usuarios, lo cual es muy inconveniente de usar y no puede garantizar la administración efectiva y la seguridad de la cuenta (Quiroz & Macias, 2017).

2.8. Carding

Se refiere al uso no autorizado de la información de la cuenta de la tarjeta de crédito y débito para comprar bienes y servicios de manera fraudulenta. Sin embargo, en los últimos años, este término ha evolucionado, para incluir una variedad de actividades relacionadas con el robo y el uso fraudulento de números de cuenta de tarjeta de crédito y débito, asimismo, en el Carding se incluye el pirateo informático, phishing, cobro de números de cuenta robados, esquemas de reenvío y fraude en subastas en internet (Freire, 2017).

Adicionalmente, el generalizado uso de tarjetas de crédito y débito proporciona un objetivo importante para el fraude ya que es un mercado en constante crecimiento y porque los tipos de tarjetas que se utilizan solo contienen una banda magnética o emplean un chip y tecnología de firma, en lugar de la tecnología de chip y número de identificación personal (PIN) que es una tecnología relativamente nueva (Yadav, Jain, & Kumar, 2021).

2.8.1. Metodologías empleadas para el Carding

Entre las metodologías más empleadas para el Carding tenemos las siguientes:

2.8.1.2. El phishing

Es la forma más común que usan los estafadores para obtener información de tarjetas de crédito. Este método implica configurar malware y promover al objetivo para que descargue un archivo malicioso, una vez que se inyecta el malware, los piratas informáticos obtienen acceso al número de identificación bancaria del objetivo, las contraseñas y otros detalles relevantes (Halga, Agrafiotis, & Nurse, 2020).

2.8.1.3. Malware rootkit

Son un tipo de malware que están diseñados para pasar inadvertido, estos proporcionan a los mal intencionados la propiedad de controlar remotamente los sistemas (Halga, Agrafiotis, & Nurse, 2020).

Por otra parte, los rootkits pueden sujetar una serie de herramientas, que van desde programas que aprueban a los piratas informáticos robar sus contraseñas hasta módulos que les facilitan el robo de su tarjeta de crédito o información bancaria en línea. Los rootkits también pueden brindar a los piratas informáticos la capacidad de subvertir o deshabilitar el software de seguridad y rastrear las teclas que toca, lo que facilita que los delincuentes roben su información personal (Shalaginov, Dyrkolbotn, & Alazab, 2021).

2.8.1.4. El Skimming

Es un tipo de robo de tarjetas de crédito en el que los delincuentes utilizan un pequeño dispositivo para robar información de la tarjeta de crédito en una transacción de tarjeta de crédito o débito legítima, su funcionamiento es a través del dispositivo que captura y almacena todos los detalles en la banda magnética de la tarjeta, esta franja contiene el número de la tarjeta de crédito, la fecha de vencimiento y el nombre completo del titular de la tarjeta, por lo que los ladrones manipulan los datos robados para realizar cargos fraudulentos, ya sea en línea o con una tarjeta de crédito falsificada (Rachavelias, 2019).

2.8.1.5. BINS

Es el número de identificación bancaria el cual se refiere al conjunto inicial de cuatro a seis números que aparecen en una tarjeta de pago. Este conjunto de números identifica la institución que emite la tarjeta y es clave en el proceso de hacer coincidir las transacciones con el emisor de la tarjeta de crédito. El sistema de numeración se aplica a tarjetas de crédito, tarjetas de cargo, tarjetas prepagas, tarjetas de regalo, tarjetas de débito, tarjetas prepagas y tarjetas de beneficios electrónicas (ANSI, 2021).

2.8.1.6. Cash-Out

Radica en la sustracción de cuentas PayPal, saldos de tarjetas de regalo, cuentas bancarias en línea y valores de Western Union (Shalaginov, Dyrkolbotn, & Alazab, 2021).

2.9. Vulnerabilidad

Desde un punto de vista tecnológico, la vulnerabilidad, consiste en una debilidad encontrada en cierto hardware, software o procedimiento, que faculta usuarios sin autorización a efectuar acciones no permitidas. De acuerdo con información del UIT (2020) el 46% de los sitios web contienen vulnerabilidades consideradas de alto riesgo, mientras que el 87% contienen vulnerabilidades de gravedad media. Además, se destaca que, aunque las debilidades de inyección SQL están disminuyendo ligeramente, otras amenazas se muestran en aumento, por lo tanto, determinar las vulnerabilidades de un sitio o aplicación es un paso necesario para poder establecer mecanismos de seguridad que permitan prevenir ataque, o incluso implementar políticas más de seguridad más globales (Ayyagari, 2020).

2.10. Métodos de seguridad para mitigar el fraude

2.10.1. Autenticación multifactor para mitigar el fraude

La autenticación multifactor (MFA) es un sistema de seguridad que implementa múltiples autenticaciones para verificar la racionalidad de una transacción, el propósito de MFA es establecer una defensa multinivel que dificulta el acceso de personas no autorizadas a sistemas o redes informáticas (Aleksandr, y otros, 2018).

2.10.2. Aplicación de normas PCI-DSS (Payment Card Industry Data Security Standard)

Según Security Standards Council, (2016) la PCI es una normativa internacional aplicada al pago con tarjetas para la seguridad de los datos con el propósito de brindar protección a los tarjetahabientes y sus operaciones en la institución financiera y resguardando la información de personas no autorizadas, lo que es la estrategia primordial para mitigar los posibles fraudes contra los clientes, dichas normativas fueron creada por las principales organizaciones globales expendedoras de tarjetas de crédito y las cuales establecieron el

PCI Security Standards Council (PCI -SSC), entre ellas tenemos, MasterCard Worldwide y Visa International. American Express, Discover Financial Services, JCB (latam.mastercard, 2020).

El estándar PCI-DSS está conformado por 12 parámetros recopilados en seis propósitos de seguimiento general (latam.mastercard, 2020).

- Establecer y preservar redes seguras.
- Resguardar los datos del tarjetahabiente.
- Incorporar sistemas de pruebas de vulnerabilidad
- Establecer procedimientos robustos de control de acceso.
- Supervisar y verificar incursiones a la red periódicamente.

2.10.3. Seguridad de la Información

Según la ISO/IEC 27000 (2021), la seguridad de la información gira en torno a la protección y el procesamiento de la información almacenada electrónicamente, por lo que la seguridad de la información es la confidencialidad, integridad y disponibilidad de la información protegida por las medidas adecuadas. (ISO/IEC 27000, 2021).

2.10.4. Estándares Internacionales.

La ISO/IEC 27000 (2021), es la familia de normas de sistemas de gestión de seguridad de la información, denominada "ISO27K", es desarrollada por la Organización Internacional para la estandarización (ISO) y la personalización conjunta de la Comisión Electrotécnica Internacional (IEC). Esta serie de estándares se deriva de la práctica y presenta recomendaciones para la gestión de la seguridad de la información y gestiona, controla los riesgos en el campo de los sistemas de gestión de la seguridad de la información.

2.10.5. ISO / IEC 27001.

Es un estándar internacional, describe cómo construir, auditar y verificar de forma independiente un sistema de gestión de seguridad de la información. Esto le permite

proteger de manera más efectiva la seguridad de toda la información financiera y confidencial, reduciendo así la posibilidad de uso ilegal o no autorizado (ISO - ISO/IEC 27001, 2021).

2.10.6. Estimación de riesgos.

Según Conrad et al. (2017), la estimación de riesgos es un proceso que engloba la detección de los recursos que utiliza un sistema de gestión de seguridad, sus amenazas y vulnerabilidades a los que se encuentran sometidos, así como la probabilidad de que ocurran, es por ello por lo que un proyecto de seguridad tiene como propósito controlar la seguridad de los activos de información los cuales pueden gestionarse a través de los siguiente:

- Identificación de los peligros.
- Análisis de vulnerabilidades.
- Cálculo del riesgo.

2.10.7. Sistema de Gestión de la Seguridad de la Información.

Un sistema de gestión de seguridad de la información (SGSI) forma parte de un sistema global de gestión, el cual está fundamentado en el análisis de riesgos para, monitorear, establecer, implementar, operar, mantener, revisar y mejorar la salvaguarda de los activos de información para concretar los objetivos del negocio, esta definición, descrita en la norma ISO/IEC 27001 (2021), enmarca el SGSI en el contexto del modelo Planear-Hacer-Verificar-Actuar (Snedaker & Rima, 2014).

2.10.8. Tratamiento de riesgos.

El rápido crecimiento de los ataques contra los sistemas de redes informáticas y el alto costo de las contramedidas de seguridad disponibles han favorecido metodologías estructuradas de alto nivel con el objetivo de evaluar el estado de seguridad de dichos sistemas y seleccionar la más conveniente medida de defensa. Por tanto, la integración de las

cuestiones de seguridad en la actividad empresarial de organizaciones ha sido un desafío importante desde varias décadas (Fennelly & Perry, 2017).

Uno de los primeros enfoques de gestión de riesgos fue desarrollado en 1979 por Campbell quien desarrolló una metodología estructurada basada en un conjunto de conceptos tales como el análisis de vulnerabilidad, análisis de amenazas, análisis de riesgo e implementación de control. Summers (1997), propuso un método similar basado en cuatro pasos:

- Análisis de activos: identificación de activos y asignación de valores.
- Identificación de amenazas y vulnerabilidades.
- Cálculo de la expectativa de pérdida anual para cada amenaza.
- Salvaguardar de los activos.

Por otra parte, además, las metodologías de gestión de riesgos se pueden dividir en dos categorías: enfoques ascendentes y enfoques descendentes. El enfoque de abajo hacia arriba consiste en seleccionar a priori la amenaza residual, por ejemplo, el grado de protección del sistema, e implementar las contramedidas que permitan alcanzarlo. La estimación de contingencia de arriba hacia abajo define las tareas programadas que están destinadas a reducir las exposiciones identificadas. Algunos ejemplos de estas tareas incluyen, entre otros, identificación de vulnerabilidades, mitigación de contingencia, monitoreo del estado del sistema y evaluación de peligros (Summers, 1997).

Es por ello que, la Gestión de Riesgos ha sido un punto focal de interés tanto para instituciones gubernamentales como para investigadores. Esto resultó en el desarrollo de muchos estándares, pautas y modelos que contribuyeron consistentemente al avance de este campo. Los trabajos más importantes relacionados con la Gestión de Riesgos tenemos a los estándares ISO y el modelo de enfoque Octave (Katsikas, 2013).

Sin embargo, la evaluación de vulnerabilidades, activos y amenazas críticas operacionalmente (OCTAVE) ha sido desarrollada conjuntamente por la Universidad Carnegie Mellon y el Instituto de Ingeniería de Software. Es un método autodirigido que se basa en un equipo pequeño, llamado equipo de análisis, que incluye tanto al personal de negocios como de tecnología de la información. El proceso OCTAVE se ha estructurado con respecto a las distintas categorías de resultados que podría ser alcanzado por este equipo. Principalmente, se han considerado tres tipos de productos; datos organizacionales, datos tecnológicos y datos de análisis como mitigación de riesgos (Snedaker & Rima, 2014).

En comparación con de la evaluación típica centrada en la tecnología, OCTAVE se focaliza en el riesgo organizacional y los problemas estratégicos relacionados con la práctica, equilibrando el riesgo operativo, las prácticas de seguridad y la tecnología. OCTAVE utiliza un enfoque basado en talleres de tres fases que permite a los trabajadores de la empresa reunir una imagen completa los requerimientos de seguridad de los datos de la organización. Estas fases según Snedaker & Rima (2014), se describen a continuación:

1. Establecer perfiles de riesgos fundamentados en activos: esta es una estimación de los aspectos organizativos. El grupo de trabajo de observación establece los activos dentro de la empresa y lo que se hace actualmente para protegerlos. Luego, el equipo determina los activos que son relevantes para la empresa (activos críticos) y define los requisitos de seguridad correspondientes. Finalmente, identifica las amenazas a cada activo crítico y crea un perfil de contingencia para ese activo. Cabe mencionar que los perfiles de amenazas se derivan del concepto de árbol de eventos.

2. Identificar las vulnerabilidades de la infraestructura: esta es una valoración de la arquitectura de la información que el equipo de trabajo designado para el análisis de la infraestructura de tecnología de la información es el encargado de la búsqueda de debilidades que puedan aprovecharse para obtener acceso no autorizado a la información o para interrumpir el procesamiento de la información. Por otra parte, estas vulnerabilidades incluyen:
 - Aquellas que son inherentes al diseño o especificación del hardware o software del sistema,
 - Aquellas que ocurren por una implementación defectuosa de software o hardware de un diseño satisfactorio y
 - Aquellas que provienen de la configuración del sistema o error de administración.
3. Desarrollar planes y estrategias de seguridad: los riesgos se analizan en esta fase. La información generada por las evaluaciones organizacionales y de infraestructura de información (Fases 1 y 2) se analiza para identificar los riesgos para la empresa y evaluar las amenazas en función de su impacto en la misión de la organización. Luego, se crea un perfil de riesgo para cada activo crítico. Además, se desarrolla una táctica de defensa para la organización y procedimientos de mitigación que abordan los riesgos de mayor prioridad.

2.10.9. Aceptación de riesgos.

La ausencia del riesgo no es realmente una estrategia de mitigación porque aceptar un riesgo no reduce su efecto. Sin embargo, la aceptación de riesgos es una opción legítima en la gestión de riesgos. Hay varias razones por las que las empresas pueden optar por la

acquiescencia del riesgo en determinadas situaciones. La razón más común es que el costo de otras opciones de gestión de riesgos, como evitar o limitar, puede superar el costo del riesgo en sí. No hay ningún beneficio en gastar \$ 100,000 para evitar un riesgo de \$ 10,000. En los casos en que el costo supera al beneficio, la mayoría de las organizaciones optan por aceptar un riesgo en lugar de gastar tiempo o dinero en mitigarlo (Snedaker & Rima, 2014). Por lo tanto, aceptar un riesgo a veces se denomina opción de, no hacer nada. Este puede ser un concepto familiar para aquellos que estén familiarizados con los fundamentos de la gestión de proyectos. A medida que desarrolle estrategias, debe considerar las implicaciones de no hacer nada. Esta puede ser una forma de asegurarse de que está tomando las medidas adecuadas porque si considera las implicaciones de aceptar el riesgo, puede observarse las posibles consecuencias y compararlas con otras opciones (Fennelly & Perry, 2017).

Por el contrario, el costo de la aceptación del riesgo es muy bajo al principio, pero después de una interrupción del negocio, el costo puede ser significativamente más alto que otras estrategias de gestión de amenazas. La empresa puede estar dispuesta a ahorrar dinero hoy sabiendo que tendrá un gasto desproporcionadamente grande más adelante si se produce una interrupción del negocio (Fennelly & Perry, 2017).

Al mismo tiempo, las pequeñas empresas pueden adoptar la postura de que no pueden permitirse evitar, limitar o transferir el riesgo y, por lo tanto, aceptan el riesgo por defecto. Esta es una vista limitada y no debería ser la posición predeterminada en esta planificación. La aceptación del riesgo debe evaluarse junto con las otras opciones para determinar las implicaciones, las acciones apropiadas y los costos de varias estrategias de mitigación. La aceptación del riesgo es la opción menos costosa a corto plazo y, a frecuentemente, la opción más costosa a largo plazo en caso de que ocurra un evento (Snedaker & Rima, 2014).

2.10.10. Comunicación de riesgos.

Una vez que se ha aceptado el plan de gestión de riesgos, debe llevarse a cabo con disciplina las actividades de control que están enfocadas a asegurar que el plan de gestión de riesgos se esté ejecutando correctamente y cumpliendo sus objetivos. El progreso se mide contra el plan de gestión de riesgos, y los recursos asignados a las actividades de riesgo se verifican para ver si se están utilizando correctamente. Por ejemplo, asegurando que los recursos efectivos se mantengan para verdaderos propósitos de contingencia, en lugar de ser utilizados como fuente de fondos de funcionamiento normales (Fennelly & Perry, 2017).

Las actividades que se están realizando para gestionar cada riesgo se revisan periódicamente junto con las actividades de seguimiento, al igual que el nivel de riesgo. Si el esfuerzo de reducción o eliminación de riesgos no avanza tan bien como se esperaba, se toman acciones para remediar la situación. Del mismo modo, parte de la actividad de control es garantizar que el plan de acción tenga tiempo suficiente para entrar en vigor. Los cambios prematuros en el curso de acción pueden ser más perjudiciales que no gestionar los riesgos en absoluto (Snedaker & Rima, 2014).

Las actividades de control de la gestión de riesgos también se centran en comunicar y regularizar la realización de los programas de trabajo de amenazas con las actividades organizativas existentes. Es clave que lo que está sucediendo en la forma de gestionar el riesgo se comunique a otras actividades del proyecto y al cliente si es necesario. Sin embargo, es probable que muchos de los riesgos traspasen los límites de la organización; por ejemplo, un riesgo puede afectar al departamento de software, al departamento de ingeniería de sistemas, al departamento de finanzas y a la administración de subcontratos de proveedores. Cada grupo tendrá que cooperar si se quiere gestionar adecuadamente el riesgo (Snedaker & Rima, 2014).

Además, las acciones que representan cambios del plan de actividades organizacionales no relacionadas con el riesgo deben comunicarse a quienes ejecutan los planes de acción del riesgo para garantizar que los planes no se vean comprometidos y que no se creen nuevas fuentes de riesgo. Esta comunicación de las actividades de riesgo del proyecto debe ser a un área lo más amplia posible (Calderón, 2015).

Finalmente, se dedicará una cantidad significativa de actividad de control a resolver problemas de conflictos de asignación de recursos. Dado que todos los recursos del proyecto son finitos, cualquier cambio en la asignación puede tener un efecto perjudicial en otra persona del proyecto. Por lo tanto, es importante que los recursos se reasignen de manera adecuada y con el mayor efecto posible para reducir la cantidad de fricción organizacional interna que puede desarrollarse. También se debe comunicar el fundamento de la reasignación (Fennelly & Perry, 2017).

2.10.11. Monitoreo y revisión de riesgos.

La actividad final de gestión de riesgos es el seguimiento y monitoreo del estado de riesgo individual y a nivel de proyecto. Los riesgos de alta prioridad se rastrean de cerca para detectar alteraciones en su nivel de riesgo. Los indicadores de amenazas definidos anteriormente brindan advertencias tempranas de cambios significativos que pueden estar ocurriendo. Los riesgos como grupo también se sopesan como un todo para determinar si ha cambiado el nivel general de riesgo del proyecto (Summers, 1997).

Durante la actividad de planificación, las exposiciones que no se gestionan activamente se colocan en una lista de vigilancia general. Se trata de riesgos que se han aceptado tal cual o para los que se ha elaborado un plan de contingencia. Periódicamente, estos riesgos se revisan para ver si sus probabilidades, consecuencias o tiempos han cambiado o, para aquellos que tienen un plan de contingencia, si se ha excedido el referente de riesgo, lo que significa que es ahora y el momento para que el plan de contingencia entre en

funcionamiento. Además, es importante que, periódicamente se comprueban nuevas fuentes de riesgo, especialmente en los entornos de interés ajenos al proyecto, como el entorno empresarial externo. Los eventos externos pueden cambiar los supuestos, objetivos, limitaciones o expectativas, y mientras más pronto sean detectadas, existirán más opciones para ser abordados. Por lo tanto, los objetivos, supuestos o restricciones del proyecto también se revisan formalmente para determinar si han cambiado de alguna manera. Por otra parte, las revisiones de los objetivos, los supuestos y las limitaciones del proyecto también pueden ocurrir lentamente y no se noten a menos que se verifiquen formalmente (Fennelly & Perry, 2017).

Parte del esfuerzo de monitoreo tiene como objetivo capturar las lecciones aprendidas para referencias futuras, también llamados, proyectos midstream, actuales y futuros. La información de riesgo recopilada durante el curso del proyecto es una excelente fuente de información histórica y actual que puede permitir que un nuevo miembro del equipo del proyecto o especialmente un nuevo gerente de proyecto comprenda rápidamente el estado actual del proyecto (Snedaker & Rima, 2014).

La información de las lecciones aprendidas también es útil para que se utilicen en proyectos similares y para que puedan evitar los mismos errores o, si dependen del resultado de ese proyecto, para comprender los riesgos y las implicaciones de ese trabajo para que puedan tomar las medidas adecuadas por sí mismos. Las lecciones aprendidas no solo deben referirse a los riesgos en sí mismos, sino también a la eficacia del proceso de análisis y gestión de riesgos en sí (Fennelly & Perry, 2017).

2.11. Sector financiero

El sector financiero a nivel mundial es por excelencia, una actividad económica en que la innovación y el uso de las tecnologías de información son fundamentales. Un ejemplo de ello es el uso de tarjetas de crédito, el cual representa un medio de pago muy extendido en

el mundo entero, estos métodos sufren frecuentemente de diversos tipos de ataques informáticos, lo cual puede ocasionar daños y alteraciones en la información, tanto de los clientes como en los datos que se resguardan dentro de la institución (Jaramillo & Riofrío, 2015).

Esto conlleva a un gran problema, ya que actualmente la información se ha convertido en uno de los activos más importantes de las organizaciones y al verse afectada puede causar daños económicos irreparables (Freire, 2017).

La detección y evaluación de las vulnerabilidades en el sector financiero, ayudará a mejorar la seguridad informática en la COAC y al conocer cuáles son sus falencias en cuanto a ataques más comunes, con el fin de revisar las políticas de control y seguridad establecidas en la institución, atenuar los ciberataques, basados en el modelo Carding para mejor posibles ataques desde el internet.

2.12. Metodología ENISA

La Agencia Europea de Seguridad de las Redes y la Información (ENISA) es una agencia dedicada a lograr un alto nivel común de ciberseguridad en toda Europa y establecida en 2004 y reforzada por la Ley de Ciberseguridad de la UE. Esta, mejora la confiabilidad de los productos, servicios y procesos de TIC con esquemas de certificación de ciberseguridad, coopera con los Estados miembros además de los organismos de la UE y ayuda a Europa a prepararse para los retos cibernéticos del mañana (ENISA, 2021).

2.12.1. Objetivos de seguridad

Según ENISA (2021) entre los objetivos principales se tienen los siguientes:

- Documentar y registrar los incidentes de agresiones o vulneraciones que se puedan presentar en instituciones a nivel de infraestructura y de redes, para su posterior informe a la agencia y demás autoridades.

- Proporcionar asesoría y apoyo entorno a los objetivos establecidos al Parlamento Europeo, comisión y organismos referentes.
- Impulsar la colaboración entre agentes relacionados con el sector como, por ejemplo, universidades, empresas y organizaciones, las cuales colaboran en la difusión de información acerca de ataques o vulneraciones que estén ocurriendo, para solventar la problemática sin afectaciones al ente afectado.
- Recomendación de buenas prácticas para solventar incidentes de forma oportuna y para garantizar buena operatividad.
- Supervisión en el control y elaboración de normas para servicios y productos de seguridad.
- Colaboración internacional para el control de la seguridad cibernética.

2.13. Metodología APCERT

El Equipo Técnico de Respuesta a Emergencias de la Red Nacional de Computadoras de China (APCERT) es un centro técnico de ciberseguridad no gubernamental, sin fines de lucro con un equipo de coordinación clave para la comunidad de respuesta ante emergencias de ciberseguridad de China, asimismo, se esfuerza por mejorar la postura de seguridad cibernética de la nación y salvaguardar la seguridad de la infraestructura de información crítica (APCERT, 2021).

Al mismo tiempo, al aprovechar su plataforma de detección de seguridad de internet, monitorea de manera proactiva las amenazas e incidentes de ciberseguridad para la infraestructura de información crítica, como la red financiera, industrial y móvil, también descubre amenazas e incidentes al compartir información con socios nacionales e internacionales y recibir informes de incidentes de usuarios en el país y en el extranjero a través de la línea directa, correo electrónico y sitio web (APCERT, 2021).

2.13.1. Objetivos de seguridad

Según APCERT (2021) entre los objetivos principales se tienen los siguientes:

- Apoyo sobre incidentes de ciberseguridad con el propósito de solventarlos.
- Apoyo sobre vulnerabilidades de ciberseguridad que aún no son del dominio público.
- Apoyo sobre amenazas de ciberseguridad y su temprana detección.
- Disponibilidad las 24 horas los 365 días.
- Informar los medios para establecer contacto a través de SMS, correo electrónico, entre otros.

CAPITULO III

3. METODOLOGIA

3.1. Tipo de Estudio

3.1.1. Según el objeto de estudio

El tipo de investigación puede catalogarse documental, por cuanto se estudió y analizó tesis de varios investigadores, así como material en línea, relacionado con el tema de la investigación, que permitirán ser aplicados en la empresa COAC. De esta manera, se buscó determinar relaciones, vínculo en el texto, argumentaciones ante la situación presente del conocimiento en el área de estudio, para fundamentar a través de material documental para alcanzar el entendimiento.

3.1.2. Según el nivel de conocimiento

Con respecto al tipo de investigación que se desarrolló en este trabajo, puede clasificarse como descriptiva, ya que se estudió la realidad dentro del COAC, a través de la descripción de su entorno, realizando un análisis previo acerca de las vulnerabilidades y riesgos que puedan presentarse dentro de la organización.

3.2. Según el método a utilizar

En el caso de este estudio se aplicó el método inductivo, ya que se obtuvieron conclusiones globales a partir de indicios individuales y está compuesto por fases, entre ellas, la investigación de los sucesos para su exploración, la codificación y el estudio de esos hechos.

3.3. Procedimientos

3.3.1. Técnica de investigación

En esta investigación se utilizó la técnica de observación y como técnica de recolección de información la encuesta y la entrevista. En este sentido, se logró encuestar a diversos trabajadores de la COAC, en este caso Auditores, Oficiales de Cumplimiento, Gerentes de la Empresa, personal de las áreas de Operaciones, Organización y Procesos y finalmente el Departamento de Prevención de Fraudes, con los cuales se recopiló información de la existencia de casos de estudio y se aplicó un muestreo por conveniencia debido al limitado acceso que se tiene de la información.

3.3.2. Instrumento de Recolección de datos

En esta investigación se aplicó como instrumento el cuestionario y la guía de entrevista. En este sentido, el instrumento estuvo compuesto por una serie de preguntas, de múltiples opciones, en el que los participantes tuvieron la libertad de responder de manera independiente las preguntas. Se aplicó una escala de medición de Likert, esta escala de medición demanda que los consultados señalen el grado de consentimiento o discrepancia con las afirmaciones planteadas en relación con el tema de investigación. Con relación a la escala esta tiene cinco (5) categorías de respuesta, que van de “Totalmente de acuerdo” a “Totalmente en desacuerdo”

3.4. Procesamiento y análisis

Para esta investigación el procedimiento se realizó de la siguiente manera, primero se procesó la información dispersa o desordenada de los datos recolectados de la población, con el propósito de obtener los datos del trabajo de campo y luego se generaron los resultados ya agrupados y ordenados. Dicha cita, aportó información relevante para esta investigación ya que en el enfoque cuantitativo fue necesario para determinar el tipo de

procedimiento utilizado basado en el tipo de instrumento seleccionado para la recolección de datos, aplicado a los trabajadores del área de sistemas en la COAC. En relación con el enfoque cuantitativo aplicado a esta investigación, se empleó el análisis cuantitativo de los datos a través de una computadora, por lo tanto, se usó un programa estadístico para lograr la tabulación de los resultados procesados.

Por otra parte, se estableció el análisis de dos metodologías para extraer los distintos elementos que conforman cada una de ellas con el propósito de utilizar los parámetros seleccionados para la creación de la guía de políticas de control.

3.4.1. Parámetros de las metodologías ENISA y APCERT

En la presente investigación se establecieron los siguientes elementos derivados de ambas metodologías, las cuales serán analizadas para establecer cuáles se emplearán en la creación de la guía de políticas de control.

3.4.1.1. Metodología ENISA

Dentro del análisis obtenido por medio de la revisión de literatura de la metodología ENISA, se establecen los siguientes parámetros:

Hardware:

Medios de conexión:

- Enlace de internet.

Herramientas de protección:

- Firewall.

Equipos:

- Estaciones de trabajo.
- Equipos adicionales.

Servidores:

- Correo electrónico.
- Intranet.

Seguridad Física:

- Caja de seguridad para copias de seguridad y almacenamiento de documentos.

Software:

- Sistema de seguimiento de incidentes.
- Herramientas para administrar políticas de seguridad, evaluación de riesgos y planes de contingencia.
- Herramientas de auditoría de seguridad.

Medidas de control:

Medidas preventivas:

- Técnicas.
- Organizativas o administrativas.

Medidas de protección:

- Colectivas.
- Individuales.

Medidas de mitigación:

- Plan de emergencia.
- Planificación de evaluación.
- Sistemas de alerta.

Macro de controles:

- Políticas de seguridad.
- Seguridad física y del entorno.
- Gestión de comunicaciones y operaciones.

- Control de acceso.

Política de seguridad:

- Política de clasificación de información.
- Políticas externas para el acceso de la información.
- Aislamiento de la información.
- Seguridad del internet.
- Notación y tratamiento de incidentes.
- Capacitación.
- Uso de los correos electrónicos.
- Seguridad de la red de computadores.
- Telecomunicaciones de la información.
- Uso de dispositivos móviles.

3.4.1.2. Metodología APCERT

Dentro del análisis obtenido por medio de la revisión de literatura de la metodología APCERT, se establecen los siguientes parámetros:

Hardware:

Medios de conectividad:

- Enlace a internet.

Equipos:

- Estaciones de trabajo.

Servidores:

- Registro de eventos.
- Respaldo de información.

Software:

- Sistemas operativos prioritarios.
- Soporte a varios SO.

Medidas de control:

- Evaluación de riesgos.
- Medidas preventivas.
- Medidas de protección.
- Medidas de mitigación.

Macro controles y políticas de seguridad:

- Identificar, autenticar y autorizar el acceso a los sistemas de información solo a personas autorizadas.
- Identificar al remitente y destinatario de las comunicaciones electrónicas, especialmente correo electrónico.
- Garantizar la disponibilidad de la información y de las aplicaciones.
- Proporcionar el conjunto de medidas organizativas y técnicas de seguridad de la información, que garanticen el cumplimiento de los requisitos legales para la validez y eficacia de los procedimientos administrativos.
- Facilitar la adopción de medidas organizativas y técnicas que aseguren la protección de su información frente a los riesgos propios de los sistemas y aplicaciones informáticas que opere
- Gestión de incidentes de seguridad.
- Auditoría y control de la seguridad.

3.5. Comparaciones de metodologías

Para conformar los parámetros en la investigación, se consideran los siguientes: Software, hardware, equipos, controles y políticas de seguridad. Seguidamente, según la comparación realizada de las dos metodologías ENISA y APCERT, se presentan los siguientes cuadros de comparación, donde se establecen los parámetros de inclusión en la metodología y están representados con una (S) y con una (N) los parámetros que excluye.

Tabla 1 Comparación categoría hardware

Parámetros	ENISA	APCERT
Enlace de internet	S	S
Estaciones de trabajo	S	S
Equipos adicionales	S	N
Servidores	S	S
Seguridad Física	S	N

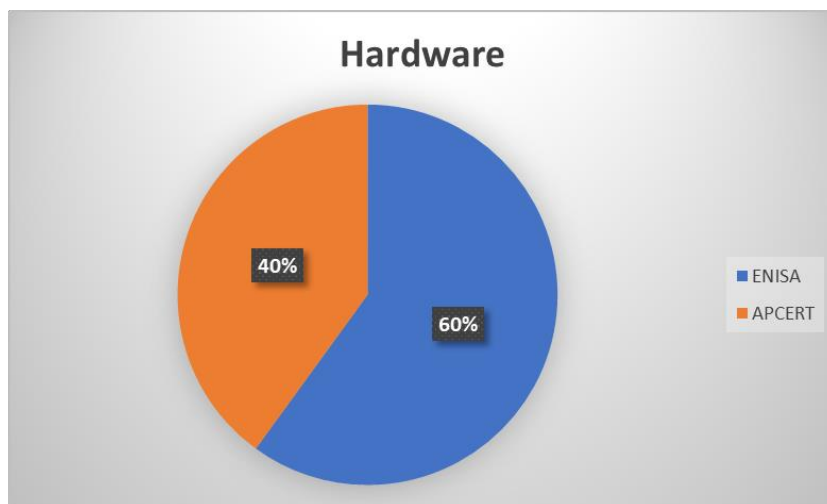


Figura 1 Comparación categoría hardware

Al realizar la comparativa en la categoría hardware, se observa que la metodología ENISA logra cumplir con 6 parámetros, mientras que la metodología APCERT tiene solo 4 parámetros en los que no admite equipos adicionales y seguridad física.

Tabla 2 Comparación categoría software

Parámetros	ENISA	APCERT
Sistema de seguimiento de incidentes	S	S
Herramientas para administrar políticas de seguridad, evaluación de riesgos y planes de contingencia	S	N
Herramientas de auditoría de seguridad	S	N
Multiplataforma	N	S

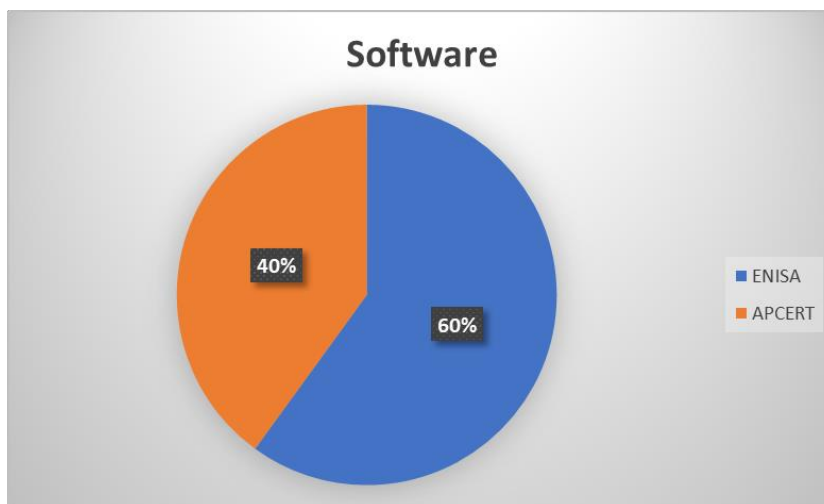


Figura 2 Comparación categoría software

Al realizar la comparativa en la categoría software se observa que la metodología ENISA logra cumplir con 3 parámetros, mientras que la metodología APCERT tiene solo 2 parámetros, en los que no admite herramientas para administrar políticas de seguridad, evaluación de riesgos, planes de contingencia ni herramientas de auditoría de seguridad.

Tabla 3 Medidas de control

Parámetros	ENISA	APCERT
Preventivas	S	S
Protección	S	S
Mitigación	S	S

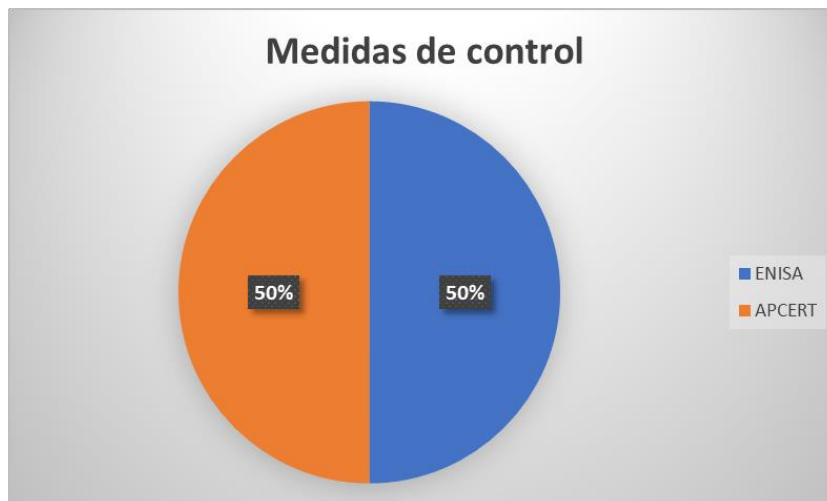


Figura 3 Medidas de control

Al realizar la comparativa en las medidas de control se observa que, ambas metodologías cumplen con todos parámetros, indicando su interés en el control en las áreas de prevención, protección y mitigación.

Tabla 4 Marco de controles

Parámetros	ENISA	APCERT
Políticas de seguridad	S	S
Seguridad física y del entorno	S	S
Gestión de comunicaciones y operaciones	S	S
Control de acceso	s	S
Disponibilidad de la información	S	S
Capacitación	S	N
Auditoría y control de la seguridad	S	S

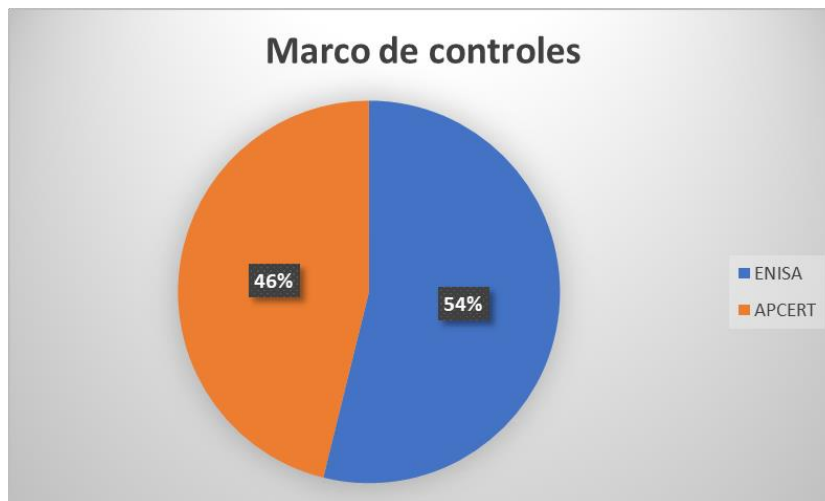


Figura 4 Marco de controles

Al realizar la comparativa en la categoría marco de controles se observa que, la metodología ENISA logra cumplir con 7 parámetros, mientras que la metodología APCERT tiene solo 6 parámetros en el que no admite capacitación.

3.6. Procedimiento de trabajo:

- Revisar el sustento teórico sobre el tema de investigación.
- Analizar los métodos de Carding.
- Investigar la metodología Carding.
- Desarrollo del tema del proyecto.
- Análisis de vulnerabilidades de la seguridad.
- Descripción de los tipos de vulneración de la seguridad mediante el modelo Carding.
- Análisis de las diferentes modalidades de metodologías del Carding para determinar las mejores políticas de control para mitigar los ciberataques basados en el modelo Carding.
- Investigar sobre las metodologías del Carding.
- Estudio de modelos para mitigar los ciberataques.
- Certificación de los instrumentos a través de la matriz de validación.
- Entrevistas y encuestas con los directivos del COAC.
- Análisis de Resultados Obtenidos.
- Estudio de las metodologías del Carding.

- Análisis y comparación de las mesologías ENISA y APCERT.
- Guía de implementación de políticas de control.

CAPITULO IV

4. ANÁLISIS Y RESULTADOS

4.1. Encuesta

A continuación, se presenta el análisis de los resultados obtenidos de las encuestas correspondientes al levantamiento de información en la COAC “Riobamba”.

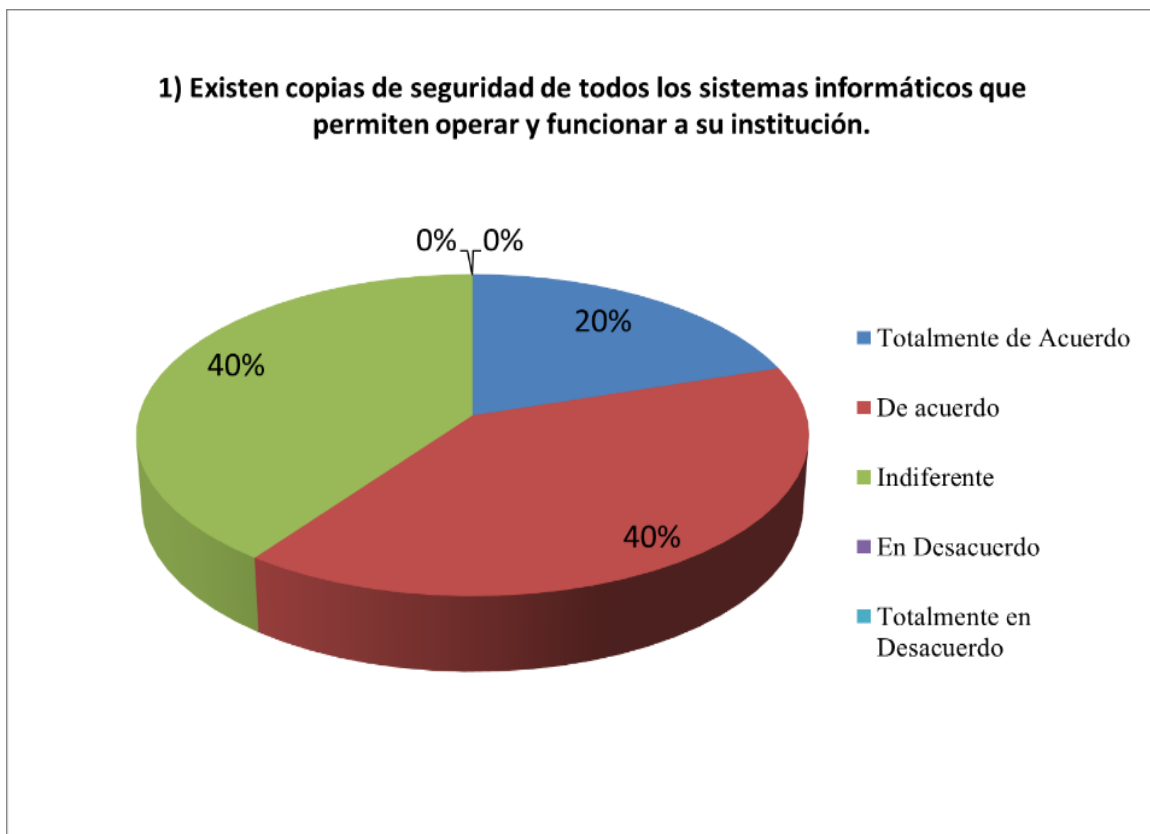


Figura 5 Copias de seguridad

Del grupo de encuestados en relación con las copias de seguridad, el 20% indicó que está totalmente de acuerdo, junto al 40% que manifestó estar de acuerdo, ya que existen copias de seguridad de todos los sistemas informáticos, que permiten operar y funcionar a su institución, mientras, que el 40% restante comento sentirse indiferente.

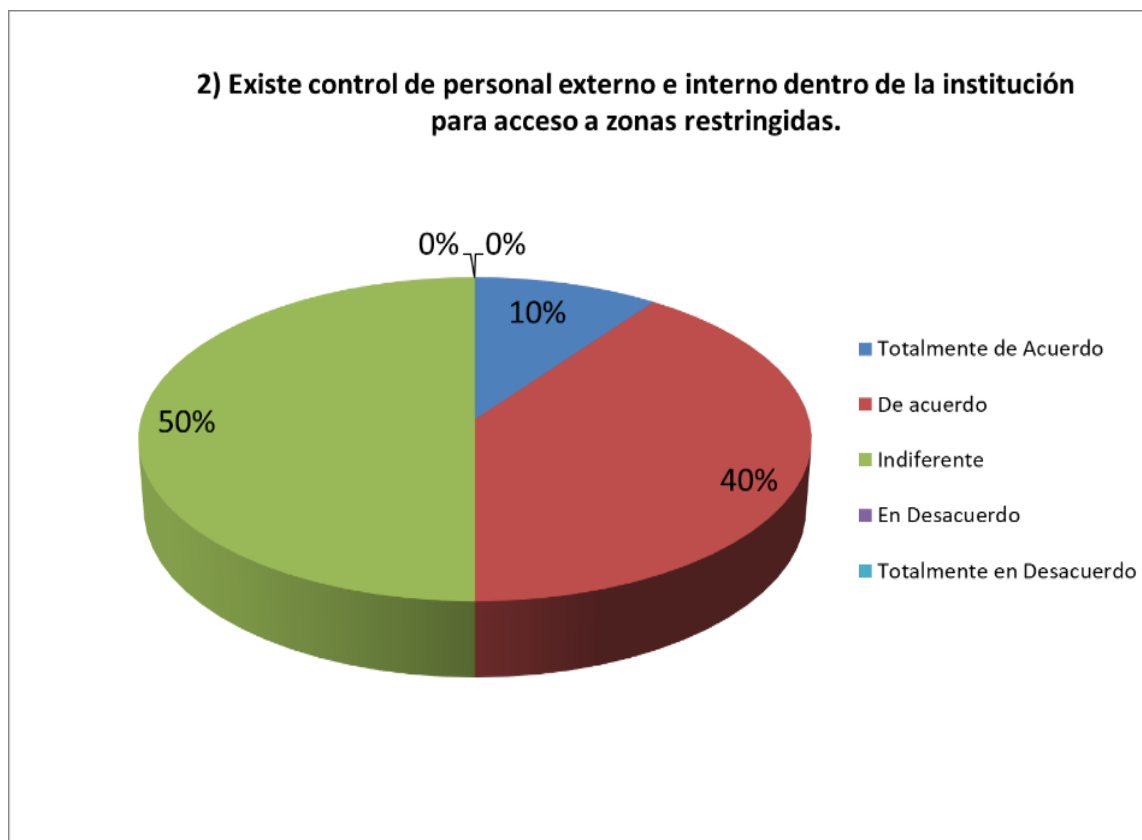


Figura 6 Control de personal externo e interno

Del grupo de encuestados en relación con el control de personal externo e interno, el 10% indicó estar totalmente de acuerdo, 40% que manifestó estar de acuerdo con que existe control de personal externo e interno dentro de la institución, para acceso a zonas restringidas, mientras que el 50% estuvo indiferente ante la consulta.

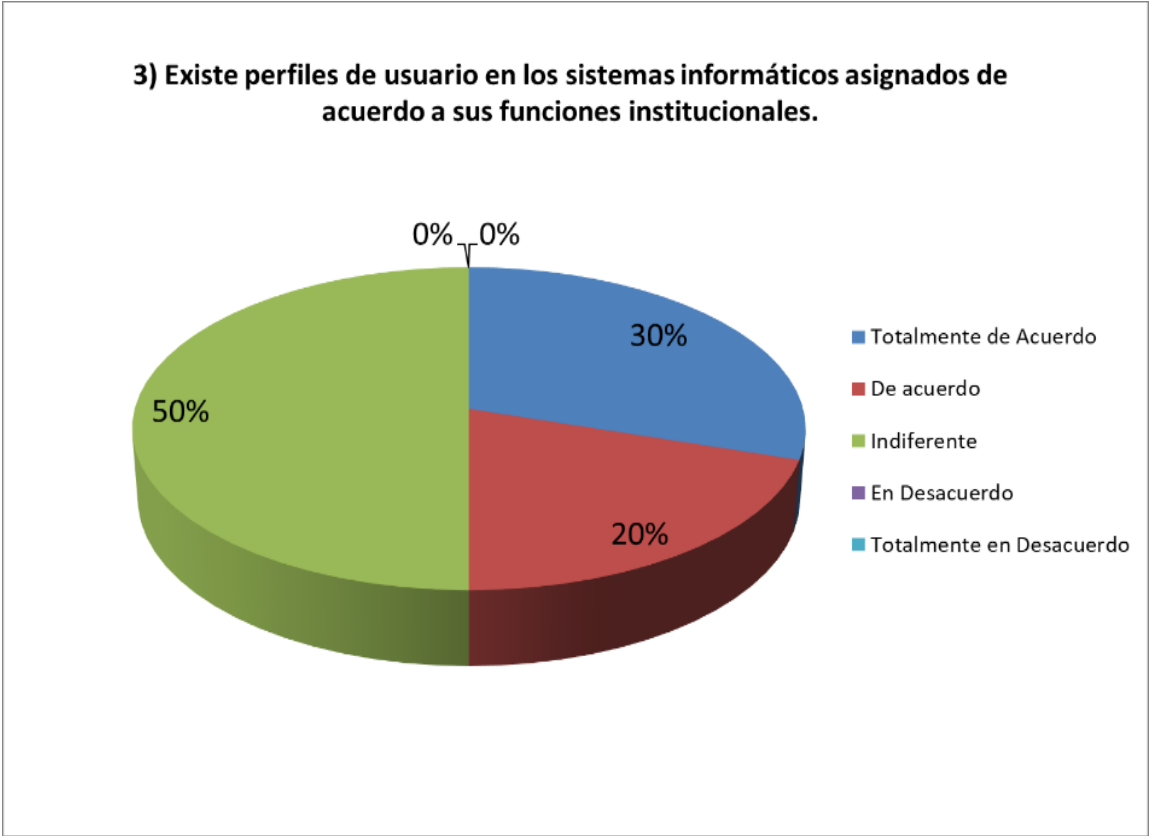


Figura 7 Perfiles de usuario

Del grupo de encuestados en relación con los perfiles de usuario, el 20% indicó estar totalmente de acuerdo, sumado al 30% que manifestó estar de totalmente acuerdo con que existen perfiles de usuario en los sistemas informáticos asignados, de acuerdo con sus funciones institucionales, mientras el 50% indicó indiferente.

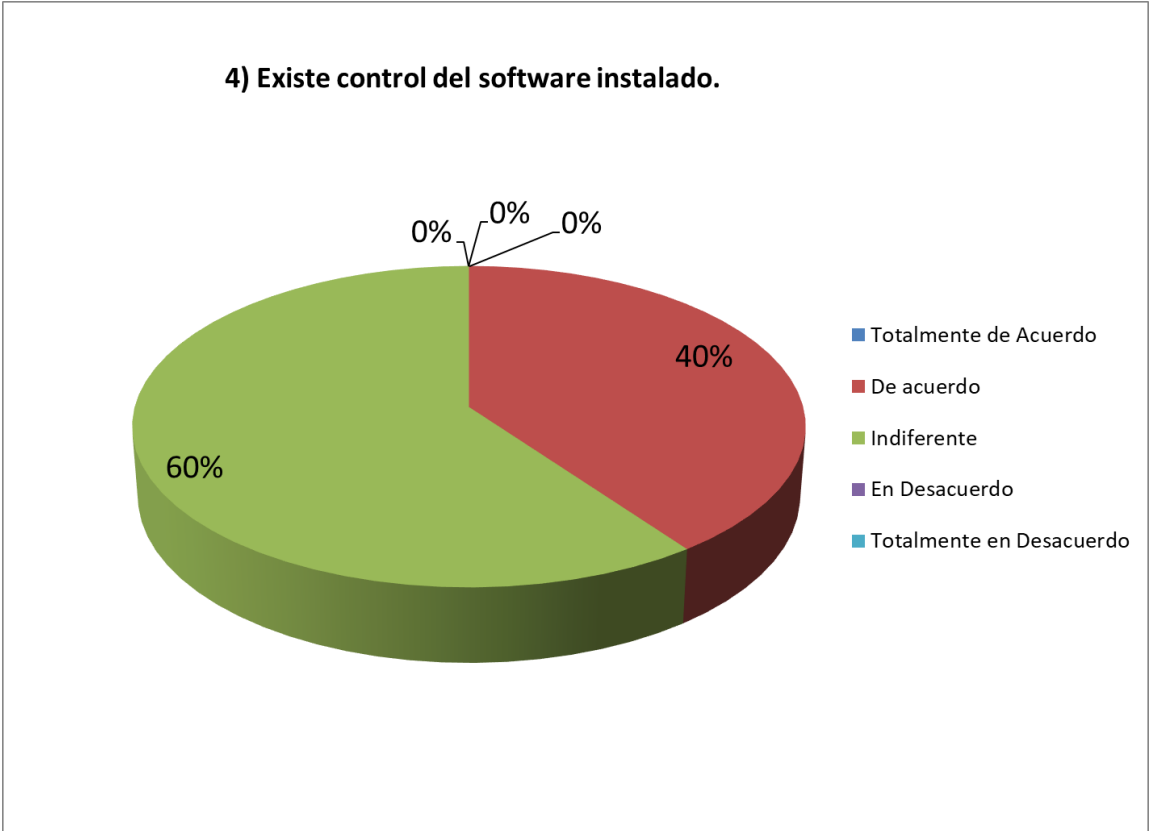


Figura 8 Control de software instalados

Del grupo de encuestados en relación con el control de software instalados, el 60% indicó estar indiferente de que existen controles del software instalado, mientras el 40% manifestó estar de acuerdo.

5) Existe aplicaciones que permitan determinar los riesgos de seguridad o ataques informáticos a los sistemas instalados.

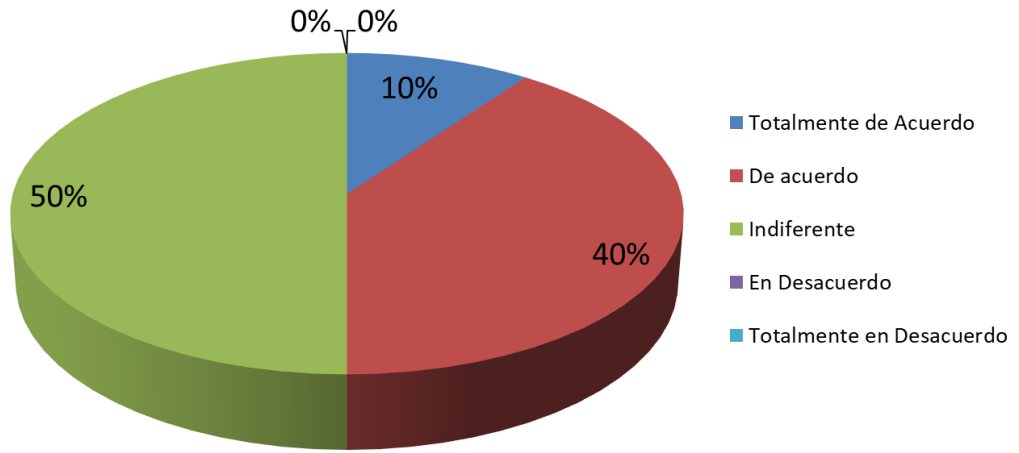


Figura 9 Aplicaciones para determinar riesgos de seguridad

Del grupo de encuestados en relación con las aplicaciones para determinar riesgos de seguridad, el 10% indicó estar totalmente de acuerdo, junto al 40% que manifiesta estar de acuerdo, mientras que el 50% solo indica estar indiferente.

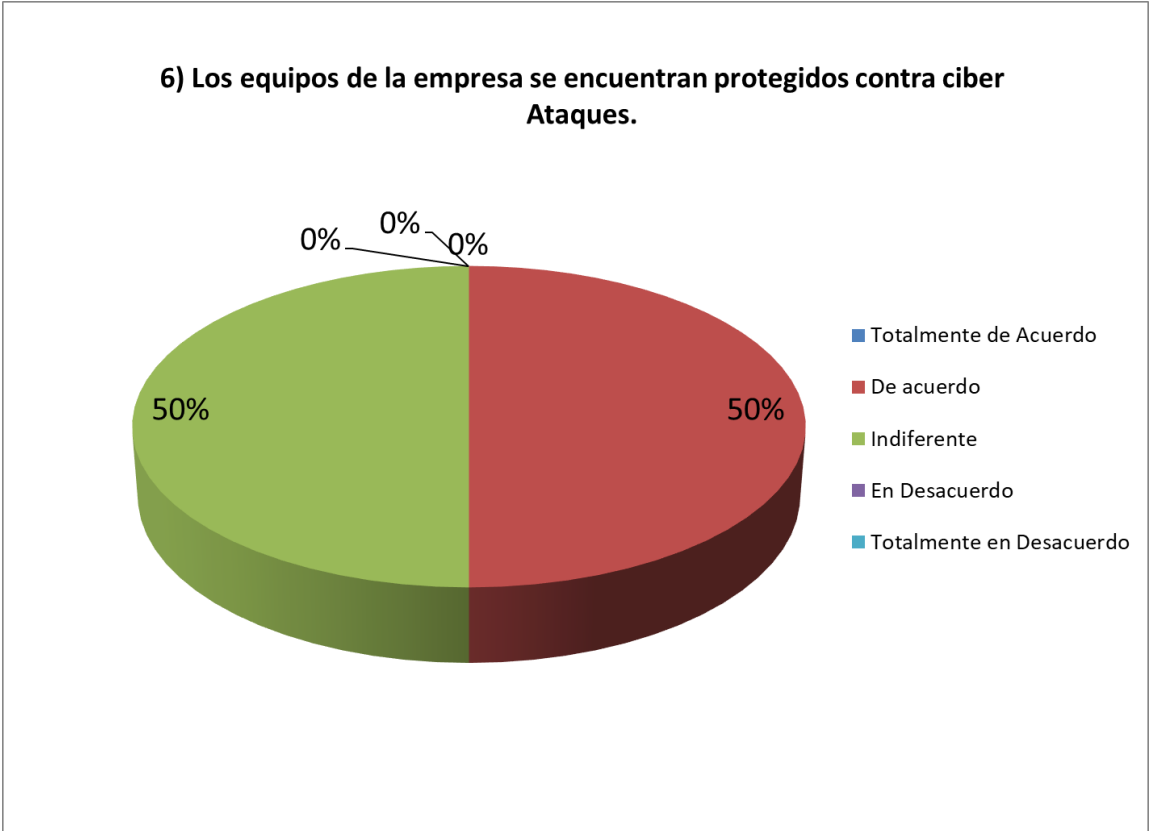


Figura 10 Equipos protegidos en la empresa

Del grupo de encuestados con relación a los equipos protegidos en la empresa, el 50% indicó estar de acuerdo, mientras otro 50% manifestó estar indiferente ante la consulta.

7) La protección de los datos y la información digital son aspectos de seguridad que se debe mejorar.

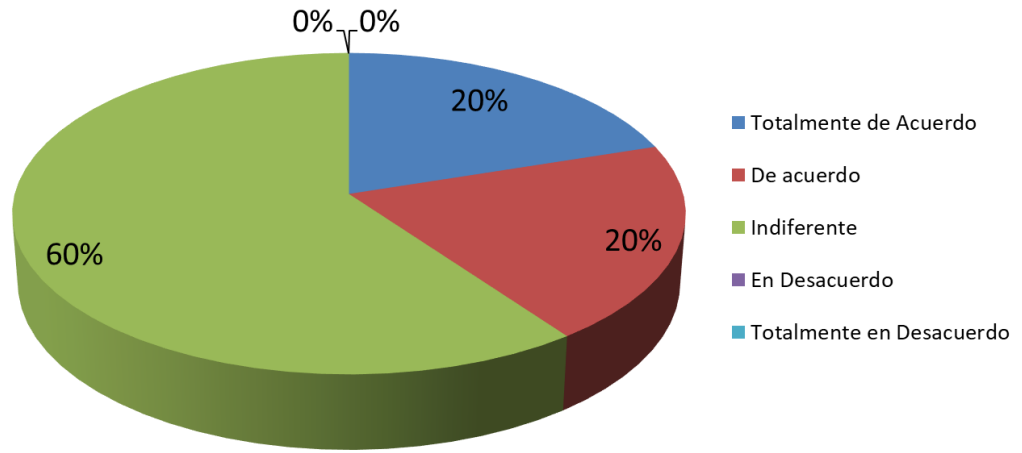


Figura 11 Protección de los datos

Del grupo de encuestados en relación con la protección de los datos, el 20% indica estar totalmente de acuerdo, junto al 20% que manifiesta estar de acuerdo. Por otra parte, el 60% indica estar indiferente.

8) Existe controles de restricción de acceso a los equipos informáticos desplegados en el Datacenter y las otras instalaciones de la empresa.

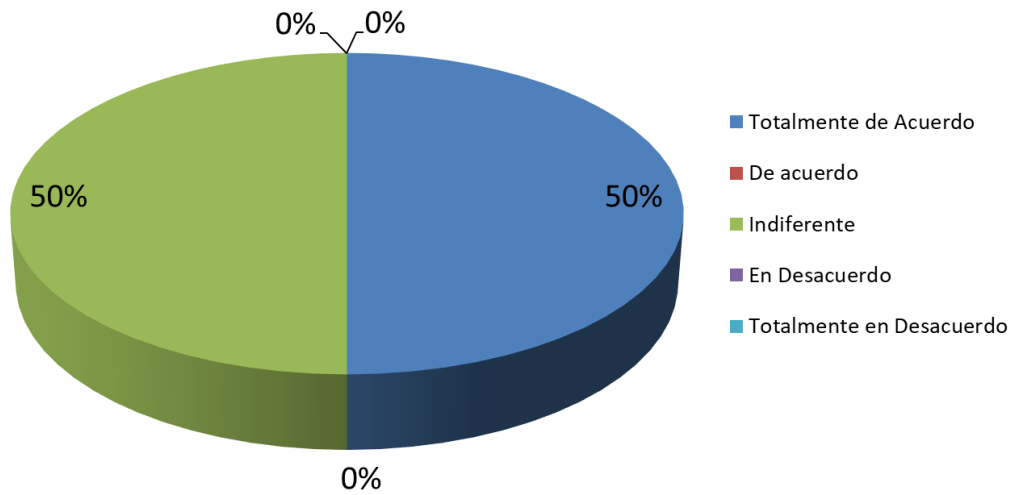


Figura 12 Controles de acceso

Del grupo de encuestados con relación a los controles de acceso, el 50% indicó estar totalmente de acuerdo, mientras el 50% restante manifestó estar indiferente.

9) Existen políticas para la extracción de activos informáticos de la empresa tales como: portátiles, teclados, mouse, accesorios.

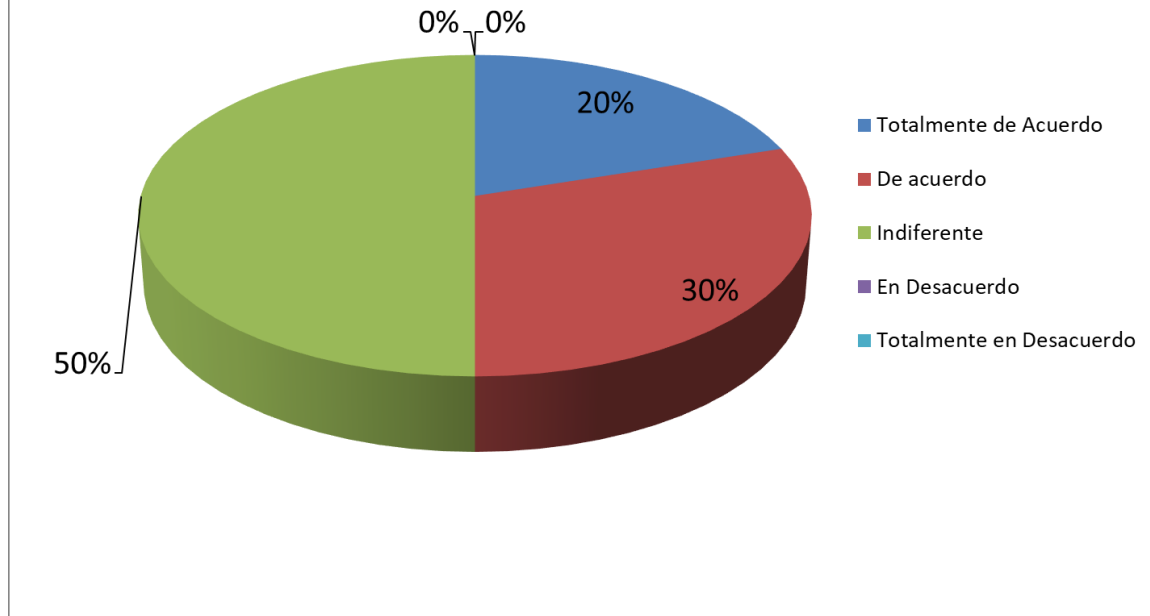


Figura 13 Políticas en los equipos informáticos

Del grupo de encuestados en relación con las políticas en los equipos informáticos, donde el 20% manifestó estar totalmente de acuerdo, sumado al 30% que indicó estar de acuerdo, mientras el 50% indicó estar indiferente.

10) Se identifican y analizan los riesgos de manera oportuna y los resultados se comunican a la alta dirección

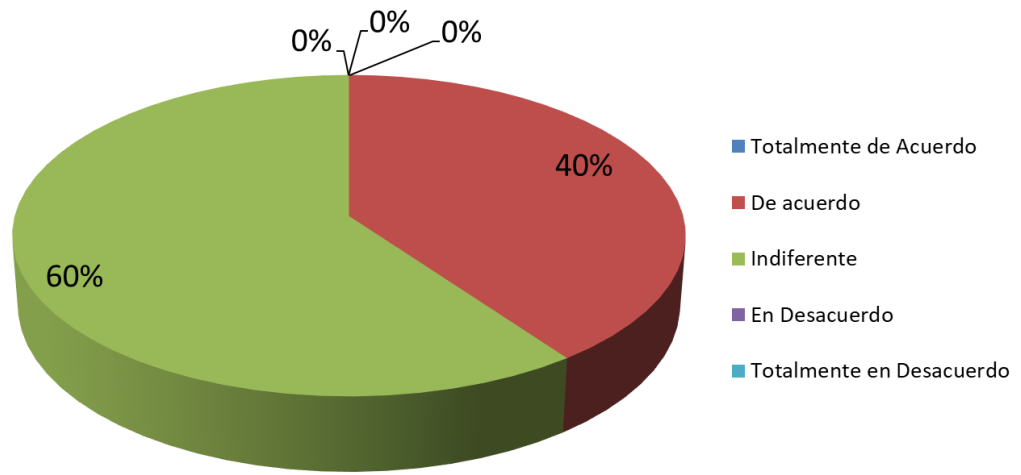


Figura 14 Identificación de riesgos informáticos

Del grupo de encuestados en relación con la identificación de riesgos informáticos, el 60% manifiesta estar indiferente, mientras el 40% indica estar de acuerdo.

4.2. Entrevista

1. Con relación al ítem, aplicaciones y dispositivos extraíbles que se emplean dentro de la institución, se puede determinar lo siguiente:

Según indica el alto directivo del área de tecnología de la información, existen políticas establecidas para controlar estos dispositivos, como el empleo de antivirus, protocolos de implementación de equipos, los cuales se disponen en las diferentes áreas con permisología de acceso a dichos dispositivos, para más detalles ver anexo A de la entrevista.

2. Con relación al ítem, uso adecuado de contraseñas y datos personales, se puede determinar lo siguiente:

Según indica el alto directivo del área de tecnología de la información, existen protocolos en cuanto al suministro de usuarios y contraseñas dentro de la institución, por lo que una vez suministrada estos perfiles a cada empleado es responsabilidad de cada uno de ellos su correcto uso y resguardo, existiendo una sanción por parte de la empresa por uso incorrecto, para más detalles ver anexo A de la entrevista.

3. Con relación al ítem, controles de seguridad, se puede determinar lo siguiente:

Según indica el alto directivo del área de tecnología de la información, la institución cuenta con normas y políticas establecidas para el manejo de la seguridad de cada usuario, además, los responsables directos del cumplimiento son los jefes de cada área, para más detalles ver anexo A de la entrevista.

4. En relación con el ítem, riesgos del uso de wifi públicas, se puede determinar lo siguiente:

Según indica el alto directivo del área de tecnología de la información, se envían al personal publicidades donde se mencionan los riesgos sobre ese tipo de accesos, para más detalles ver anexo A de la entrevista.

5. En relación con el ítem, capacidad del personal para identificar virus/malware, se puede determinar lo siguiente:

Según indica el alto directivo del área de tecnología de la información, el sistema genera una alerta de la cual posteriormente es informada al sistema y esta avisa al departamento correspondiente, para más detalles ver anexo A de la entrevista.

6. En relación con el ítem, presupuesto en ciberseguridad, se puede determinar lo siguiente:

Según indica el alto directivo del área de tecnología de la información, no directamente, está destinado a seguridad y por el momento se tiene un 21% del plan estipulado por la institución, para más detalles ver anexo A de la entrevista.

7. Con relación al ítem, capacidad de los empleados para prevenir errores de seguridad informática, se puede determinar lo siguiente:

Según indica el alto directivo del área de tecnología de la información, no, ya que muchos empleados de la institución evidencian falencias en el tema de la ciberseguridad, para más detalles ver anexo A de la entrevista.

8. Con relación al ítem, planes de prevención de riesgos informáticos, se puede determinar lo siguiente:

Según indica el alto directivo del área de tecnología de la información, si, consiste en tres niveles los cuales son básico, específico y muy completo, para más detalles ver anexo A de la entrevista.

9. Con relación al ítem, riesgos cibernéticos, se puede determinar lo siguiente:

Según indica el alto directivo del área de tecnología de la información, los riesgos cibernéticos se combaten con conocimiento, seguido de inversión, para más detalles ver anexo A de la entrevista.

10. Con relación al ítem, políticas de seguridad en la institución, se puede determinar lo siguiente:

Según indica el alto directivo del área de tecnología de la información, Sí, para más detalles ver anexo A de la entrevista.

11. En relación con el ítem, Vulnerabilidades en los navegadores, se puede determinar lo siguiente:

Según indica el alto directivo del área de tecnología de la información, sí, ya que la ingeniería bajo los navegadores está basada en ingeniería social, lo cual implica conocimiento para ser manejado correctamente, para más detalles ver anexo A de la entrevista.

4.3. Comparación de metodologías

Una vez efectuada la comparación de las metodologías basadas en 4 criterios con sus elementos que lo conforman se logró un puntaje de 19 en la metodología ENISA y esta es la elegida para la realización de la guía de sugerencias y en políticas de control, basadas en el modelo Carding. A continuación, se presentan los distintos elementos que se utilizó para la comparación de las dos metodologías:

Tabla 5 Comparación de los parámetros de las dos metodologías

Metodologías	ENISA	APCERT
Hardware	6	4
Software	3	2
Medidas de control	3	3
Marco de controles	7	6
	19	15

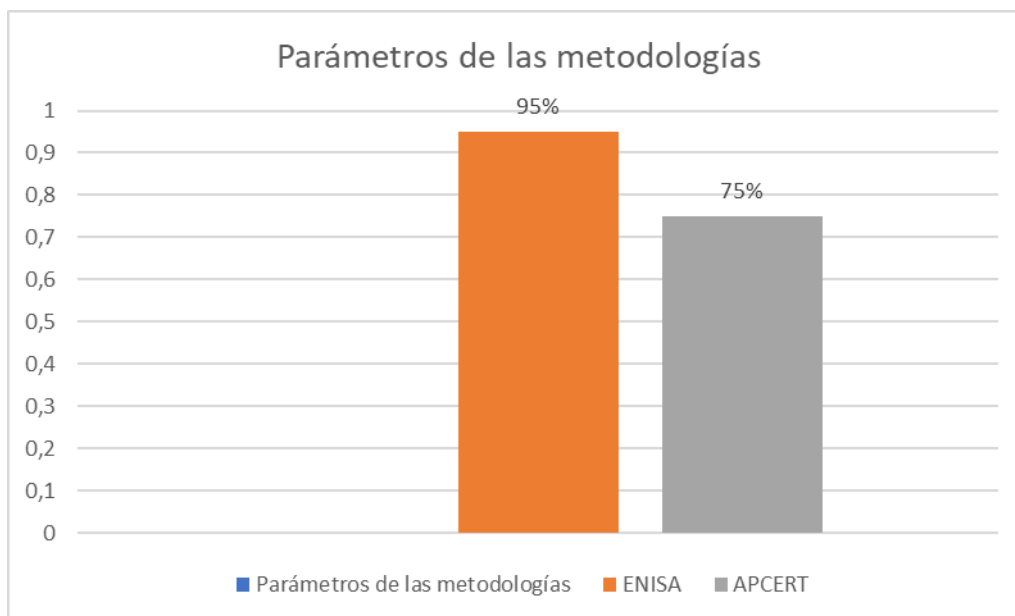


Figura 15 Porcentaje de la comparación de ENISA y APCERT

Al realizar la comparación de los elementos de las dos metodologías se logró determinar en la categoría de hardware para la metodología ENISA, que satisface 6 parámetros dentro del análisis de literatura, al contrario de APCERT que satisface 4 parámetros, en los cuales no considera a equipos adicionales ni seguridad Física.

Al mismo tiempo, en la categoría de software en la metodología ENISA, satisface 3 parámetros, por el contrario de APCERT la cual satisface 2 parámetros, donde no considera las herramientas para administrar políticas de seguridad, evaluación de riesgos ni planes de contingencia, así como tampoco considera a las herramientas de auditoría de seguridad.

Igualmente, en la categoría de medidas de control en las metodologías ENISA y APCERT satisfacen ambas los 3 parámetros analizados.

Posteriormente, en el análisis de la categoría marco de controles en la metodología ENISA satisface 7 parámetros, mientras APCERT satisface 6 parámetros, en el cual no considera la capacitación.

De este modo, luego de realizar la comparación de las metodologías con un total de 19 puntos que representan un 95% para ENISA, esta es la escogida sobre la metodología APCERT que consiguió una puntuación 15 que representan un 75%, por estos resultados, se

procede a la realización de la guía antes mencionada con la metodología ENISA y las metodologías del Carding analizadas, tal como puede observarse en el anexo C.

5. CONCLUSIONES Y RECOMENDACIONES

5.1. Conclusiones

El propósito de esta investigación fue analizar e investigar los métodos más recurrentes del Carding para mitigar los ciberataques en el COAC mediante una guía de políticas de control, por lo que se llega a las siguientes conclusiones que se presentan a continuación:

- A través de las generalidades encontradas en el marco teórico se establecieron las características relacionadas con los modelos del Carding, tales como controlar de forma remota los sistemas, además de contar con habilidades que otorga funciones de indetectabilidad y poseen destrezas en la deshabilitación de software de seguridad. Por lo tanto, los datos encontrados referentes a estos métodos fraudulentos aportaron conocimiento y recursos que posteriormente sirvieron de referencia para dicha investigación evitando posibles ataques tanto internos como externos en las organizaciones.
- Por medio del análisis de las formas más recurrentes del Carding se logró establecer cuáles son las más frecuentes que afectan a las entidades financieras y entre las cuales se observaron el phishing, malware rootkit, Cash-Out y skimming.
- Con el análisis e investigación de las diferentes clases de métodos para mitigar el Carding, se fundamentó a través de la comparación realizada entre metodologías ENISA y APCERT basándose en 4 criterios, entre los que se evaluaron hardware, software, medidas de control y marco de controles, se consideró emplear la metodología ENISA para la elaboración de la guía propuesta, ya que una vez realizado el análisis la misma presentó un 95% de efectividad de sus características y un amplio esquema a ser considerado en función de la seguridad.

5.2. Recomendaciones

- Mantener una capacitación especializada con el personal que tiene acceso a áreas sensibles de la organización, con el propósito de hacer frente ante cualquier ciberataque.
- Realizar publicidades informativas destinadas hacia los clientes, con el fin de informar los métodos por los cuales pueden ser víctimas de ciberataques, para contar con herramientas útiles para estar prevenidos.
- Realizar reuniones mensuales con directivos de otras sucursales, que les permita estar actualizados de los posibles ataques que hayan podido sufrir y que las otras sucursales deberían estar al tanto para estar atentas a cualquier novedad.

6. BIBLIOGRAFÍA

- Aguirre, A. (2017). *Ciberseguridad en Infraestructuras críticas de información*. (Tesis de Post Grado), Universidad de Buenos Aires, Buenos Aires. Obtenido de http://bibliotecadigital.econ.uba.ar/download/tpos/1502-1115_AguirrePonceAA.pdf
- Aleksandr, O., Sergey, B., Niko, M., Sergey, A., Tommi, M., & Yevgeni, K. (2018). Multi-Factor Authentication: A Survey. *Cryptography*, 2(-), 1-31. doi:10.3390/cryptography2010001
- Alvarado, E., & Buitrago, D. (2018). *Sistema de Gestión de Seguridad de la Información (SGSI)*. (Tesis de Pregradp), Universidad Distrital Francisco José de Caldas, Bogotá, Colombia. Obtenido de <https://repository.udistrital.edu.co/bitstream/handle/11349/13418/BuitragoRojasDanielaStefany2018.pdf?sequence=1&isAllowed=y>
- ANSI. (2021). *American National Standards Institute*. Obtenido de <https://www.ansi.org/>
- Ayyagari, R. (1 de 2020). Data breaches and carding. En *The Palgrave Handbook of International Cybercrime and Cyberdeviance* (págs. 939–959). Palgrave Macmillan. doi:10.1007/978-3-319-78440-3_37
- Calderón, L. (2015). Seguridad informática y seguridad de la información. (Tesis). Universidad Piloto de Colombia, Bogotá, Colombia.
- Calderón, L. (2015). *Seguridad informática y seguridad de la información*. Universidad Piloto de Colombia, Bogotá, Colombia.
- Calderón, L. (2015). *Seguridad informática y seguridad de la información*. (Tesis de Pregrado), Universidad Piloto de Colombia, Bogotá, Colombia. Obtenido de <http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/2821/Trabajo%20de%20grado.pdf?sequence=1&isAllowed=y>

- Conrad, E., Misenaar, S., & Feldman, J. (1 de 2017). Domain 1 : Security risk management. En *Eleventh Hour CISSP®* (págs. 1–32). Elsevier. doi:10.1016/b978-0-12-811248-9.00001-2
- Conrad, E., Misenaar, S., & Feldman, J. (1 de 2017). Domain 1 : Security risk management. En *Eleventh Hour CISSP®* (págs. 1–32). Elsevier. doi:10.1016/b978-0-12-811248-9.00001-2
- Duran, J. (2020). *Principales características, modos de perpetración y vulneración de la seguridad informática a través de la modalidad CARDING*. (Tesis Maestria), Universidad Nacional Abierta y a Distancia “UNAD”, Colombia. Obtenido de <https://repository.unad.edu.co/bitstream/handle/10596/34366/jduranpa.pdf?sequence=1&isAllowed=y>
- Duran, J. (28 de Mayo de 2020). *Principales Características, Modos De Perpetración Y Vulneración De La Seguridad Informática A Través De La Modalidad Carding*. (Tesis de pregrado), Universidad Nacional Abierta y a Distancia, Bogotá D.C, Colombia . Obtenido de <https://repository.unad.edu.co/bitstream/handle/10596/34366/jduranpa.pdf?sequence=1&isAllowed=y>
- Faried, F., & Fajardo, F. (2017). *Plan De Contingencia Ante Ciberataques*. (Tesis), Escuela Superior Politécnica Del Litoral, Guayaquil. Obtenido de <https://www.dspace.espol.edu.ec/retrieve/102439/D-106279.pdf>.
- Fennelly, L. J., & Perry, M. A. (1 de 2017). Assessing Risk and Vulnerabilities. En *Physical Security: 150 Things You Should Know* (págs. 79–96). Elsevier. doi:10.1016/b978-0-12-809487-7.00002-4

- Freire, F. (2017). *Plan de contingencia ante ciberataques*. (Tesis de Magister), Escuela Superior Politécnica del Litoral, Guayaquil - Ecuador. Obtenido de <https://www.dspace.espol.edu.ec/retrieve/102439/D-106279.pdf>
- Freire, F. (2017). *Plan de Contingencia ante Ciberataques*. (Tesis Maestría), Escuela Superior Politécnica del Litoral, Guayaquil. Obtenido de <https://www.dspace.espol.edu.ec/xmlui/bitstream/handle/123456789/42124/D-106279.pdf?sequence=-1>
- Halga, L., Agrafiotis, I., & Nurse, J. (2020). Catching the phish: detecting phishing attacks using recurrent neural networks (RNNs). (págs. 219-233). Cham: Springer International Publishing. doi:10.1007/978-3-030-39303-8_17
- Heinemeier, D. (2018). Manual de carding. *hackeruna*, 4.
- Hernández, R., Fernández, C., & Batista, P. (2017). *Metodología de la investigación científica* (7 ed.). Mexico: Mc Graw Hill. Obtenido de <http://observatorio.epacartagena.gov.co/wp-content/uploads/2017/08/metodologia-de-la-investigacion-sexta-edicion.compressed.pdf>
- ISO - ISO/IEC 27001. (2021). *ISO - ISO/IEC 27001 — Information security management*. Obtenido de <https://www.iso.org/isoiec-27001-information-security.html>
- ISO/IEC 27000. (2021). *norma ISO/IEC 27001*. Recuperado el 2021, de <https://www.iso27000.es/iso27000.html>
- ITU. (2020). UIT: Comprometida para conectar el mundo. *UIT: Comprometida para conectar el mundo*, 16. Obtenido de <https://www.itu.int/es/Pages/default.aspx>
http://www.itu.int/dms_pub/itu-s/opb/gen/S-GEN-HLPW-2011-PDF-S.pdf
<https://www.itu.int/es/myitu>

- Jaramillo, C., & Riofrío, J. (2015). *Metodología para realizar la evaluación, detección de riesgos, vulnerabilidades y contramedidas en el diseño e implementación de la infraestructura de la red de la editorial Don Bosco*. (Tesis Pregrado), Universidad Politécnica Salesiana, Cuenca. Obtenido de <https://dspace.ups.edu.ec/handle/123456789/7910>
- Jaramillo, C., & Riofrío, J. (2015). *Metodología para realizar la evaluación, detección de riesgos, vulnerabilidades y contramedidas en el diseño e implementación de la infraestructura de la red de la Editorial Don Bosco, mediante un test de intrusión de caja blanca*. (Tesis Maestría), Universidad Politécnica Salesiana, Cuenca. Obtenido de <http://dspace.ups.edu.ec/handle/123456789/7910>
- Katsikas, S. K. (1 de 2013). Risk Management. En *Computer and Information Security Handbook* (págs. 905–927). Elsevier Inc. doi:10.1016/B978-0-12-394397-2.00053-2
- Katsikas, S. K. (1 de 2016). Risk Management. En *Computer and Information Security Handbook* (págs. 905–927). Elsevier Inc. doi:10.1016/B978-0-12-394397-2.00053-2
- latam.mastercard. (2020). *Cumplimiento del Estándar de Seguridad de Datos PCI Mastercard (DSS)*. Recuperado el 2021, de <https://latam.mastercard.com/es-region-lac/comerciantes/seguridad-y-proteccion/requisitos-y-recomendaciones-de-seguridad/proteccion-de-datos-del-sito-y-pci.html>
- Machín, N., & Gazapo, M. (2016). Cybersecurity as a critical factor for the security of the European Union. *Revista UNISCI*, 2016, 47–68. doi:10.5209/RUNI.53786
- Quiroz, S., & Macias, D. (2017). Seguridad en informática: consideraciones. *Revista Científica Dominio de Las Ciencias*, 3(3), 676-688. Obtenido de <https://dominiodelasciencias.com/ojs/index.php/es/article/view/663>

- Rachavelias, M. (2019). Online financial crimes and fraud committed with electronic means of payment—a general approach and case studies in Greece. (págs. 339-355). n/a: ERA Forum. doi:10.1007/s12027-018-0519-2
- Reddy, V., Adepu, S., Mishra, V., & Mathur, A. (2021). Cybersecurity Cascading effects of cyber-attacks on interconnected critical infrastructure. *Cybersecurity*, 4(1), 1-47. doi:10.1186/s42400-021-00071-z
- Sampieri, R., & Mendoza, C. (2018). *Metodología de la Investigación: las rutas cuantitativa, cualitativa y mixta*. México: Mc Graw Hill.
- Seaman, J. (2020). *PCI DSS*. Berkeley, CA: Apress. doi:10.1007/978-1-4842-5808-8
- Shalaginov, A., Dyrkolbotn, G., & Alazab, M. (2021). Review of the malware categorization in the era of changing cybethreats landscape: common approaches, challenges and future needs., (págs. 71-96). Cham. doi:10.1007/978-3-030-62582-5_3
- Snedaker, S., & Rima, C. (2014). Risk Mitigation Strategy Development. En *Business Continuity and Disaster Recovery Planning for IT Professionals* (págs. 337–367). Elsevier. doi:10.1016/b978-0-12-410526-3.00006-4
- Summers, R. (1997). *Secure computing: threats and safeguards* (Vol. 34). Ohio: McGraw-Hill. doi:10.5860/choice.34-5730
- Urueña, F. (2015). Describir las principales afectaciones de seguridad informática tanto en Colombia. *ieee.es*, 2.
- Yadav, A., Jain, V., & Kumar, A. (2021). Performance analysis of machine learning algorithms in credit card fraud detection. (págs. 319-325). Singapore: Springer Singapore. doi:10.1007/978-981-15-7345-3_26

ANEXOS

ANEXO A

ENTREVISTA

Entrevistado: Alto directivo¹ del área de tecnología de la información de la COAC.

1. ¿Conoce usted las aplicaciones y dispositivos extraíbles que utilizan dentro de la institución? Explique brevemente.

R. Se puede decir que de manera general tenemos controlados todos los externos que ejercen, nuestros dispositivos están conectados a la red interna, tenemos implementado como políticas para cualquier equipo que ingresa o que es de la institución varios esquemas de seguridad ante los cuales tenemos, la plataforma de antivirus que es ESET, donde controlamos la gran parte del tema de estos dispositivos, como también la instalación o protocolo de implementación de equipo que va a cada área donde también se controla o se desvincula o se desactiva los accesos directos a varios procesos, también tenemos claro de que hay ciertas áreas que manejan este tipo de dispositivos, por ende se les mantiene como tipos aislados, con alto riesgo por lo que se les maneja con un cierto perfil de seguridad un poco más alto, de ahí, tenemos que los dispositivos que más manejan son los USB externos y a manera de salida de información tenemos el tema de correos electrónicos que son políticas establecidas por la institución y que asumiéndose el riesgo que se tiene directamente de eso, Por otra parte, existen los manuales operativos, funcionales que tiene que tener el área correspondiente y ser autorizados y aprobados por los directivos por los mandos directivos y también son revisados por los de test de control, por los temas de auditoría y riesgos.

¹ (No se proporcionan sus datos por razones de confidencialidad)

Entrevistadora: es posible que acá o algo o que alguna persona de la institución quiera utilizar estos dispositivos, ustedes les informan anteriormente para ellos poder extraer algún tipo de información o datos.

R. La regla manifiesta o la norma aquí en la institución interna manifiesta, que cualquier persona que ingresa tiene que conocer los procesos y políticas internas de la institución, entre una de esas están las políticas de manejo de equipos y de aplicaciones que tiene la institución.

2. ¿En la institución los empleados hacen un uso adecuado de las contraseñas y datos personales? Explique brevemente.

R. Puedo manifestarle que como usted conoce, la regla que se está haciendo ya normal en el manejo de usuario y password propio en cada una de las aplicaciones, más aún en esta era digital, pero el concepto es que si uno no es responsable de su propio login y su propio password ya es responsabilidad personal, en la institucional lo que si se trata es de comunicar esta responsabilidad que se tiene al manejo de cada clave, existe un área hablando ya del tema central que es el Col financiero de la institución se maneja perfiles con claves de usuario que cada mes se solicita al sistema automáticamente la actualización, ya que cada usuario como tal es asignado cuando así lo amerita mediante el uso, incluso con una autorización formal el cargo que va hacer utilizar donde se le asigna el usuario y la clave, esto ya no está dentro de nuestra área esta manejado por recursos humanos para la asignación de este tipo de accesos de allí como tal el sistema financiero y los sistemas que llamamos prioridad cero manejan clave visual con la idea de que siempre estén actualizando por un periodo de tiempo establecido para manejar la seguridad de allí cada uno es responsable como política e incluso existe reglamento interno donde manifiesta el caso de no utilizar correctamente este tipo de accesos tenga también su sanción.

1. ¿Se realiza un control de la seguridad de todos los usuarios institución? Explique brevemente.

R. Como decía ya más hablando de los temas de los sistemas de alto riesgo que se tiene normado políticas establecidas definidas para el manejo o acceso de tales, entonces entendemos que se manejan correctamente cada cierto periodo auditoría hace un control de este tipo de accesos hasta el momento y revisando cada proceso que haya realizado en este aspecto, con respecto a otros sistemas que son de áreas correspondientes no son considerados de prioridad que son en si llamados, sistemas de apoyo relativamente son responsabilidad de cada uno de los jefes de cada área y el uso, y utilización de este tipo de dispositivos con sus debidos acceso.

Entrevistadora: ¿Cuáles son las áreas que están consideradas como prioridad para la seguridad?

R. Banco financiero, todas las que son aplicaciones directamente institución cooperativa todas las que los socios manejan directamente, esos son todas las que interactúa transaccionalmente con la institución de los socios, puedo enumerarte 4 o tres de momento, por ejemplo, Corp financiero la base central de todas la transacciones institucional, las aplicaciones móviles que son sistemas satélites que hacen posibles transacciones de diferente modo diferente canal, cajeros automáticos podemos decir que es otro tipo de subsistemas, de facturas, de correos electrónicos también, el de accesos a la administración de los antivirus, la administración de Fribur tenemos de todo el sistema diseñado de la tres capas que tenemos implementadas.

Entrevistadora: ¿Que antivirus están utilizando ahora?

R. ESET, toda la plataforma ESET, nosotros manejamos varios.

Entrevistadora: ¿No ha tenido ningún problema?

R. No, es que no hemos tenido, si se han presentado en las capas de seguridad que tenemos pero no han sido de gran impacto, se han logrado controlar a tiempo y se han mitigado relativamente adecuadamente podemos decir, por lo que si hemos tenido ataques, es más muchos de nuestros monitores de ataques, de ciberataques de todo del lado de la plataforma, es a diario, se mantiene un proceso de medida normal que manejamos desde hace tiempo, vamos viendo cómo van creciendo esos relativamente son controlados hasta el momento adecuados digamos, no hemos tenido un ataque bajo estas estas medidas que tenemos de monitoreo de nuestra seguridad vemos que no hemos tenido hasta el momento ataques que pueden ser anormales o procedimientos anormales dentro de este proceso al momento.

4. Según su opinión, ¿Los empleados de la institución conocen los riesgos de uso de redes wifi-públicas? Explique brevemente.

R. Bueno se ha tratado de darle, aquí hay como una red de internet y WhatsApp interno también, se envía correos, se envía publicidades donde se les menciona que tengan cuidado de este tipo de accesos y se les trata de capacitar sobre eso o informar o difundir sobre este tema de que tengan y no sólo esto, varios conceptos de seguridad y su manera de trabajar, sea privada o empresarialmente hablando.

Entrevistadora: ¿Pero los empleados ya han recibido las capacitaciones?

R. No son capacitaciones, como digo son publicidades que se envían para que tomen en cuenta para que se les recuerde generalmente el área de riesgos, hace a veces este tipo de capacitación sobre temas de seguridad y nosotros lo que hacemos es enviarles noticias, informar.

5. Según su criterio, ¿Los empleados de la institución son capaces de identificar un virus/malware? Explique brevemente.

R. Bueno en nuestras redes sí, porque, generalmente les bloquea o les da un alerta como tal y en los cursos electrónicos es un poco más complejo, pero se le ha informado cuando

tengan un mensaje y eso lo conocen los usuarios que manejan correo interno, porque no todos los usuarios manejan un correo interno, aquí se les autoriza dependiendo que área o que funciones están haciendo o que jefe vea como tal necesario la activación de un correo electrónico para tal o cual usuario, en todo caso, todos los usuarios están en conocimiento de cuando llegó un correo nuevo no normal con un mensaje un poco distinto a lo normal, generalmente de un origen no conocido tiene que informar al sistemas, en todo caso, el sistema al momento de que se nos informa, se debe revisar este correo e informa a los procesos o procedimientos a seguir.

Entrevistadora: ¿Pero ustedes se basan mediante un manual o guía o algo para contrarrestar ese problema que ocasiona cuando llega ese correo electrónico?

R. Relativamente, la revisión un poco puntual de que es lo que está sucediendo y es manejado por un soporte en nuestro proveedor de seguridad y en nuestro caso es SERICA y FRIVORE FORTINET, entonces estamos nosotros con ellos contactados y la persona encargada seguridad es el que maneja ese proceso un poco puntual, como él también está encargado de la parte de manejo de los Host, los Spam y todo esos tipos, van cerrando digamos el círculo para ir asegurando mucho mejor este proceso, pero bueno no puedo garantizar de que el 100% de los correos como tal estén sanos, pero bajo las plataformas que estamos mencionando, hasta el momento no hemos tenido inconveniente graves.

6. ¿En la institución se invierte presupuesto en ciberseguridad? Explique brevemente.

R. No como tal, no como directamente hacia los ciberataques, más está destinado a las capas de seguridad que estamos queriendo establecer, asegurar en la institución, la del núcleo, vamos subiendo de aplicación, vamos subiendo de canal estatal, entonces nosotros estamos asegurando es canales, queremos subir y son 7 capas de seguridad las que queremos asegurar y vamos por la tercera y paso a paso vamos saliendo a este nuevo proceso, esta nueva tecnología que estamos hablando de forma digital, hacia el trabajo digital, entonces

poco a poco se van estableciendo cada una de las capas y lo que es necesario y todo lo que es la infraestructura para el sistema de seguridad.

7. Según su opinión, ¿Los empleados de la institución tienen la formación que necesitan para prevenir errores de seguridad informática? Explique brevemente.

R. NO, relativamente no, la gente que sale de las diferentes áreas y por ende generalmente los empleados que ingresan a la institución se les nota un desconocimiento del tema de ciberseguridad, entonces como tal no podemos garantizar que conozcan bastante sobre este tema, aquí se les comienza a informar un poco más sobre eso.

Entrevistadora: Pero imagino que todos aquí en el área de sistemas están capacitados.

R. Con tecnología como siempre sí, pero dice de la institución no puedo asegurar, somos 100 contados y relativamente es difícil saber si existe una falencia en eso, nosotros que somos de tecnología digamos estamos un poco más al tanto de todo este proceso, pero si vamos y le preguntamos a un algún estudiante de administración, algún estudiante es difícil y más aún ahora la juventud está destinada, no le para mucho al tema de la ciberseguridad como tal y eso se ve claramente al manejar los perfiles de Facebook, manejar los términos seguridad.

8. Considera usted que, ¿En la institución se cuenta con un plan de prevención de riesgos informáticos? Explique brevemente.

R. Si, básico, relativamente específico, muy complejo.

9. ¿Cómo se pueden proteger las empresas ante el riesgo de ciberataques? Explique brevemente.

R. Conocimiento, claro está después inversión.

Entrevistadora: ¿Considera usted que la empresa garantiza disponibilidad de sus servicios ante los riesgos del ciberataque?

R. Al momento nosotros tenemos ya un año, casi dos años de experiencia en elevar unos servicios de Internet donde los usuarios ya están realizando transacciones digitales y relativamente si se preparó la institución para este tipo de servicios, al momento podemos decir que estamos a nivel tecnológico asegurados, pero no podemos garantizar, como usted sabe la tecnología varia todos los días, los ataques siguen existiendo de diferente índole, Windows mismo, la otra semana liberó recién una nueva actualización por un tema de un canal abierto por el tema de las impresoras, por un puerto de las impresoras que podrían acceder y se estaban corrigiendo las mismas, entonces no podemos garantizar que todo lo que estemos implementados perita mantener esa seguridad, pero podemos decir que estamos asegurando la transaccionalidad como tal, entonces pienso que la institución al momento garantizar sus servicios como tal, tratando de mantenerse siempre a la parte de todos los cambios que existen y bueno en eso trabajamos.

10. Según su opinión, ¿Existe el desarrollo de políticas de seguridad dentro de la institución? Explique brevemente.

R. Si.


11. Según su opinión, ¿En la institución existe vulnerabilidad de los navegadores de internet? Explique brevemente.


R. Si, en teoría puede ser por desconocimiento de la gente generalmente como esto está basado en una ingeniería social maneja el concepto de venta, de comercialización, entonces al manejar los navegadores se va a encontrar usted con temas de comercialización, por ende, eso implica tener un riesgo no, por manejar estas redes, por que sostiene todo esto el comercio un poco el conocimiento, por un lado, pero todos estaría manejando por el comercio, si uno se mete a la web como tal le llega un mensaje de venta de algo, pues eso entendería yo que el concepto digamos por detrás de todo este proceso y eso implica estar abierto y si se puede hacer eso hay una empresa que vende ese tipo de publicidad que puede

ver eso, pero basado en la inteligencia emocional que tiene incluso una ingeniería social que existe por allí, que trata de averiguar qué es lo que sucede, incluso de los estados de ánimo y todo eso, pero bueno el concepto está allí basado entonces y entendemos que siempre va estar algo abierto por allí para ese proceso, pero la idea es tratar de asegurar el trabajo como tal. como siempre se preguntan sabemos si la seguridad en la casa la utilizamos y porque por desconocimiento, eso es lo que para mi prima en todo y aquí en la institución de ley es un tema bastante nuevo.

Anexo B

ENCUESTA

	UNIVERSIDAD NACIONAL DE CHIMBORAZO FACULTAD DE INGENIERÍA CARRERA DE SISTEMAS Y COMPUTACIÓN						
<p>Estimados(a) participantes: El presente cuestionario tiene como propósito recabar información sobre Guía de implementación de políticas de control para mitigar los ciberataques basados en el modelo Carding en la COAC "Riobamba LTDA.". Este cuestionario consta de una serie de preguntas de múltiples opciones. Al leer cada una de ellas, seleccione la respuesta que sea más fidedigna y confiable. ¡Muchas gracias, por su valiosa colaboración!</p>							
<p>Instrucciones: En las preguntas que se presentan a continuación existen cinco (5) alternativas de respuesta, responda según su apreciación:</p> <ul style="list-style-type: none"> • Señale con una (X) en la casilla correspondiente a su selección. • Asegúrese de marcar una sola alternativa para cada pregunta. • Por favor, no deje ningún ítem sin responder para que exista una mayor confiabilidad en los datos recabados. 							
CUESTIONARIO			RESPUESTAS				
Afirmaciones			Totalmente en Desacuerdo	En desacuerdo	Indiferente	De Acuerdo	Totalmente de Acuerdo
			1	2	3	4	5
1. Existen copias de seguridad de todos los sistemas informáticos que permiten operar y funcionar a su institución.						X	
2. Existe control de personal externo e interno dentro de la institución para acceso a zonas restringidas.						X	
3. Existe perfiles de usuario en los sistemas informáticos asignados de acuerdo a sus funciones institucionales.							X
4. Existe control del software instalado.						X	
5. Existe aplicaciones que permitan determinar los riesgos de seguridad o ataques informáticos a los sistemas instalados.						X	
6. ¿Los equipos de la empresa se encuentran protegidos contra ciber Ataques?						X	
7. ¿La protección de los datos y la información digital son aspectos de seguridad informática que se deberían mejorar?						X	
8. Existe controles de restricción de acceso a los equipos informáticos desplegados en el Datacenter y las otras instalaciones de la empresa.							X
9. Existen políticas para la extracción de activos informáticos de la empresa tales como: portátiles, teclados, mouse, accesorios.						X	
10. Se identifican y analizan los riesgos de manera oportuna y los resultados se comunican a la alta dirección?				X			



Anexo C

MATRIZ DE EVALUACION DE INSTRUMENTOS EVALUADOS POR EXPERTOS EN SEGURIDAD.

MATRIZ DE EVALUACION DEL INSTRUMENTO

DATOS DEL EXPERTO EVALUADOR

Título profesional más alto: Magister en Interconectividad de Redes

Área del conocimiento: TICS

Fecha: 07/06/2021

Objetivo del instrumento: Conocer la pertinencia y objetividad del instrumento de validación para el desarrollar una guía de implementación de políticas de control para mitigar los ciberataques basados en el modelo Carding en la COAC “Riobamba Ltda.”.

Escala de valoración: Escala de 1 a 5 siendo 1 la calificación más baja y 5 la más alta.

Instrucciones: Escriba su valoración bajo cada criterio por pregunta, y de ser necesario una explicación inclúyalo en la casilla de comentario

INSTRUMENTO PARA VALIDAR

INSTRUMENTO DE VALORACION DE LA GUÍA DE IMPLEMENTACIÓN DE POLÍTICAS DE CONTROL PARA MITIGAR LOS CIBERATAQUES BASADOS EN EL MODELO CARDING EN LA COAC “RIOBAMBA LTDA.”

ENCUESTA

Esta encuesta tiene por objetivo conocer su opinión respecto a la estrategia en materia de seguridad de la información para mitigar los ciberataques basados en el modelo Carding y políticas de control establecidas por el COAC “Riobamba Ltda.” que permitan establecer las bases para la creación de la guía de políticas de control más adecuadas.

Agradecemos sus respuestas, la encuesta es anónima y solo será utilizada para los fines indicados.

MATRIZ DE EVALUACION DE LOS INSTRUMENTOS

DATOS DEL EXPERTO EVALUADOR	
Título profesional más alto:	Magister en Interconectividad de Redes
Área del conocimiento:	TICS
Cargo/función:	Docente
Departamento/área:	UNACH – Facultad de Ingeniería
Años de experiencia:	15
Fecha:	07/06/2021

Afirmaciones	VALORACION DE 1 A 5				Comentarios
	Redacción	Pertinencia	Comprensión	Medible	
<p>1.- En la institución existen copias de seguridad de todo el sistema.</p> <p>Totalmente en Desacuerdo En desacuerdo Indiferente De Acuerdo Totalmente de Acuerdo</p>	4	5	4	4	<p>Se sugiere:</p> <p>Existen copias de seguridad de todos los sistemas informáticos que permiten operar y funcionar a su institución</p>
<p>2.- Existe control del personal externo e interno dentro de la institución.</p> <p>Totalmente en Desacuerdo En desacuerdo Indiferente De Acuerdo Totalmente de Acuerdo</p>	4	5	4	4	<p>Se sugiere:</p> <p>Existe control de personal externo e interno dentro de la institución para acceso a zonas restringidas.</p>
<p>3.- En la institución existen usuarios con privilegios acordes a su perfil.</p> <p>Totalmente en Desacuerdo En desacuerdo Indiferente De Acuerdo Totalmente de Acuerdo</p>	5	5	5	5	
<p>4.- Existen vulnerabilidades del personal o del sistema.</p> <p>Totalmente en Desacuerdo En desacuerdo Indiferente De Acuerdo Totalmente de Acuerdo</p>	3	4	4	4	<p>Especifique vulnerabilidades respecto a que parámetro o parámetros</p>
<p>5.- Existen vulnerabilidades del sistema.</p> <p>Totalmente en Desacuerdo En desacuerdo</p>	3	3	3	3	<p>En la pregunta 4 ya se pregunta lo mismo (o del sistema)</p>

Indiferente De Acuerdo Totalmente de Acuerdo					Especifique a que sistema se refiere - Informático - Otro
6.- Existe control del software instalado. Totalmente en Desacuerdo En desacuerdo Indiferente De Acuerdo Totalmente de Acuerdo	5	5	4	4	
7.- Los equipos de la empresa se encuentran protegidos. Totalmente en Desacuerdo En desacuerdo Indiferente De Acuerdo Totalmente de Acuerdo	5	5	4	4	Especificar protegidos respecto a que aspecto o parámetro
8.- La protección de la información es un aspecto de seguridad informática que se debería mejorar. Totalmente en Desacuerdo En desacuerdo Indiferente De Acuerdo Totalmente de Acuerdo	5	5	5	5	
9.- Existen controles de restricción de acceso a los computadores. Totalmente en Desacuerdo En desacuerdo Indiferente De Acuerdo Totalmente de Acuerdo	4	3	5	4	Se sugiere: Existe controles de restricción de acceso a los equipos informáticos desplegados en el Datacenter y las otras instalaciones de la empresa
10.- Existen políticas para la extracción de activos informáticos de la empresa tales como: portátiles, teclados, mouse, accesorios. Totalmente en Desacuerdo En desacuerdo Indiferente De Acuerdo Totalmente de Acuerdo	5	5	5	5	

11.- Se identifican y analizan los riesgos de manera oportuna y los resultados se comunican a la alta dirección. Totalmente en Desacuerdo En desacuerdo Indiferente De Acuerdo Totalmente de Acuerdo	5	5	5	5	
Preguntas	VALORACION DE 1 A 5				Comentarios
	Redacción	Pertinencia	Comprensión	Medible	
1.- ¿Conoce usted las aplicaciones y dispositivos extraíbles que utilizan dentro de la institución?	5	5	5	5	
2.- ¿En la institución los empleados hacen un uso adecuado de las contraseñas y datos personales?	5	5	5	5	
3.- ¿Se realiza un control de la seguridad de todos los usuarios empresariales?	5	5	5	5	
4.- Según su opinión, ¿Los empleados de la institución conocen los riesgos de uso de redes wifi-públicas?	5	5	5	5	
5.- Según su criterio, ¿Los empleados de la institución son capaces de identificar un virus/malware?	5	5	5	5	
6.- ¿En la institución se invierte presupuesto en ciberseguridad?	5	5	5	5	
7.- Según su opinión, ¿Los empleados de la institución tienen la formación que necesitan para prevenir errores de seguridad informática?	5	5	5	5	
8.- Considera usted que, ¿En la institución se cuenta con un plan de prevención de riesgos informáticos?	5	5	5	5	
9.- ¿Cómo se pueden proteger las empresas ante el riesgo de ciberataques?	5	3	4	5	Se sugiere: ¿Considera usted que la empresa garantiza la disponibilidad de sus servicios ante el riesgo de ciberataques?

10.- Según su opinión, ¿Existe el desarrollo de políticas de seguridad dentro de la institución?	5	4	4	5	Se sugiere: Según su opinión, ¿Existe el desarrollo de políticas de seguridad de la información dentro de la institución?
11.- Según su opinión, ¿En la institución existe vulnerabilidad de los navegadores de internet?	5	5	5	5	

UNIVERSIDAD NACIONAL DE CHIMBORAZO



**GUÍA DE IMPLEMENTACIÓN DE POLÍTICAS DE CONTROL PARA
MITIGAR LOS CIBERATAQUES BASADOS EN EL MODELO CARDING.**

Autor:

Paredes Díaz Karen Valeria

Tutor:

Ing. Lorena Paulina Molina Valdiviezo

RIOBAMBA – ECUADOR

2021

Dirigida el personal de la institución:

1.1. SEGURIDAD FÍSICA

1.1.1. Hardware y Software

- a) Los equipos designados por la empresa deben ser empleados solamente para actividades relacionadas con el puesto de trabajo y no para propósitos personales.
- b) Los usuarios de los equipos son responsables de proteger los programas y datos contra daños o pérdidas.
- c) Cualquier falla, anomalía, mal funcionamiento tanto de los equipos o la red debe ser comunicado al supervisor inmediato para evitar daños mayores como indisponibilidad del servicio o pérdida en los datos.
- d) Los equipos de la institución no pueden ser cambiados de lugar sin autorización del supervisor o del personal encargado.
- e) No se puede alterar, modificar o cambiar la configuración del hardware y software de los equipos en ninguna circunstancia.

1.1.2. Áreas de trabajo

- a) Los armarios y cableados donde están ubicados los Switches deben estar protegidos y libres de obstrucciones para poder acceder fácilmente a estos.
- b) La protección de equipos e instalaciones no solo es responsabilidad de la administración, sino también de los usuarios.
- c) Entre las herramientas de trabajo que cuenta la institución se tienen teléfonos, impresoras, telefax, fotocopadoras, escáners, archivos, carpetas y escritorios, los cuales deben de mantenerse resguardados y cualquier eventualidad debe reportarse al supervisor inmediato.

1.2. CONTROL DE ACCESO FÍSICO A OFICINAS Y ZONAS RESTRINGIDAS

1.2.1. INSTALACIONES

- a) El personal puede permanecer en las instalaciones de la empresa dentro del horario de trabajo y en caso de que el personal necesite estar en las instalaciones fuera de su horario de trabajo se debe solicitar una autorización por escrito a su supervisor inmediato.

- b) Solo el personal autorizado del área de tecnología tendrá acceso a los servidores, Switches de comunicación y equipos críticos de la institución.
- c) Ninguna persona que no esté autorizada previamente podrá ingresar al área de sistemas de la institución.
- d) Toda persona que requiera ingresar en un área restringida deberá identificarse para registrarse y se requerirá de la debida autorización para su ingreso.
- e) Toda persona que no pertenezca a la institución y que requiera el ingreso al área de sistemas de la institución deberá anunciarse ante el personal autorizado y este verificara los datos con su supervisor inmediato, para confirmar la solicitud y proporcionar la autorización del ingreso y el mismo debe ser escoltado durante todo el procedimiento hasta que este concluya su tarea y abandone las instalaciones.

1.3. CONTROL DE APLICACIONES EN ESTACIONES DE TRABAJO

- a) Se prohíbe la instalación de aplicaciones o software que no hayan sido autorizados por la institución.
- b) Se prohíbe realizar cualquier copia de datos o el empleo del software para fines personales.
- c) Se prohíbe el uso de dispositivos de almacenamiento en cualquier computadora de la institución y solo el personal técnico autorizado se le permitirá su uso solo para las funciones a las cuales este autorizado.

1.4. CONTROL DE DATOS EN LAS APLICACIONES

- a) La información que se maneja dentro de los sistemas de la institución es válida y están integrados en cada sistema.
- b) Los usuarios poseen controles de acceso para los datos y aplicaciones, es responsabilidad de cada usuario su conservación.

1.5. SEGURIDAD LÓGICA

1.5.1. ASPECTOS GENERALES

- a) Las estaciones de trabajo deben ser bloqueadas por los usuarios al dejarlas desatendidas.
- b) Luego de renuncia o despido, se debe desactivar el usuario antes que abandone el cargo.

- c) Se deben ratificar cada año los privilegios de usuario, adicionalmente el personal autorizado del área de sistemas será en responsable de bloquear, eliminar o suspender cuantas de usuario una vez reciba la autorización correspondiente.

1.5.2. IDENTIFICACIÓN DE USUARIOS

Para crear usuarios dentro del sistema y proporcionar los accesos, así como los permisos a los diferentes módulos se necesitan los siguientes datos:

- a) Datos de usuario: Nombre y apellido, identificación única del usuario, dependencia a la que el usuario pertenece.
- b) Permisología: Se debe proporcionar los permisos necesarios para que cada usuario acceda solo al módulo del sistema que su cargo o función le permite.
- c) Rango de horarios: Los accesos al sistema de usuarios administrativos solo están autorizados en los días hábiles laborales, durante periodos de vacaciones las cuentas de estos usuarios permanecerán bloqueadas, igualmente durante días feriados todas las cuentas estarán desactivadas.

1.6. AUTENTICACIÓN EN LA RED

- a) Ingreso al sistema: todos los usuarios para iniciar la sesión deben acceder a través de las credenciales nombre de usuario, dominio y contraseña.
- b) Cuando el usuario ingresa la contraseña dentro del sistema la misma no debe mostrarse en la pantalla, deben mostrarse asteriscos al digitarse la misma.

1.7. PASSWORD

Para definir el password se deben establecer criterios de seguridad y entre los cuales se tienen los siguientes:

- a) La longitud de la contraseña no debe ser menor a 8 caracteres.
- b) La contraseña debe contener minúsculas, mayúsculas, números y caracteres especiales.
- c) La contraseña no puede ser el nombre del usuario, nombre de la empresa, o frases que puedan ser asociadas con el usuario.
- d) Las contraseñas deben expirar a los 30 días, luego de este lapso el sistema solicitará el cambio de la misma forma automática.

- e) Si olvida la contraseña el usuario debe hacer la solicitud por escrita a su supervisor inmediato y este informará al departamento de sistemas para que el mismo elimine la contraseña y permita que el usuario ingrese al sistema para cambiarla por otra directamente desde su terminal de trabajo.
- f) Se prohíbe compartir la contraseña entre usuarios, personal o extraños, ya que esto puede generar faltas graves en la seguridad de la institución.
- g) No se debe anotar la contraseña y dejarla en un lugar donde pueda ser encontrada por otros.
- h) Las contraseñas que vienen por defecto en equipos nuevos como Firewalls, Switches entre otros, deben ser modificadas antes de ser puestos es servicio.
- i) Los usuarios no deben tratar de violentar los sistemas de seguridad y de acceso, ya que representa una falta a las políticas de seguridad de la institución.
- j) Solo el personal con rango de supervisores y jefes tienen la potestad de solicitar se borre una contraseña.
- k) No se permite compartir las credenciales de acceso entre usuarios del sistema.

1.8. LA INFORMACIÓN

1.8.1. POLITICAS GENERALES

- a) Se prohíbe la divulgación de datos, duplicación de información, modificación, pérdida, destrucción, accesos no autorizados de datos pertenecientes a la institución.

1.9. EL CORREO ELECTRÓNICO

- a) Los correos electrónicos empleados dentro de la institución se deben considerar como documentos formales.
- b) Los correos que ya no sean necesarios deben ser eliminados por medidas de seguridad, con el propósito de evitar que sean leídos por personas no autorizadas reduciendo este tipo de riesgos.
- c) Los correos deben ser solo para el uso de trabajo relacionado con la institución.
- d) No se deben recibir ni enviar correos con archivos adjuntos que contengan extensiones de archivos tales como EXE, COM, BAT, PPS, entre otros.

1.10. SEÑALES POR ATAQUES DE CARDING

Entre los criterios que se pueden establecer para determinar señales se tienen los siguientes:

- b) Si se recibe un correo electrónico de un usuario desconocido al que no se haya contactado antes.
- c) Si se ingresa a un sitio web y se observan detalles extraños en la dirección URL.
- d) Si el sistema del ordenador está más pesado y puede que ocasionalmente efectúe movimientos inusuales, es señal de que algún malware se ha instalado en dicho sistema y está captando información sensible y es necesario informar de forma inmediata al supervisor.

1.11. COMO PROTEGERSE DEL CARDING

Recomendaciones puntuales a empleados de la institución:

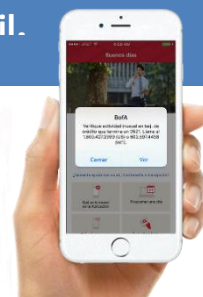
- Desarrolle y mantenga redes y sistemas seguros:
 - 1. Instalar y mantener una configuración de firewall para proteger los datos del titular de la tarjeta.
 - 2. No utilizar contraseñas de sistemas y otros parámetros de seguridad provistos por los proveedores.
- Proteger los datos del titular de la tarjeta:
 - 1. Proteja los datos del titular de la tarjeta que fueron almacenados.
 - 2. Cifrar la transmisión de los datos del titular de la tarjeta en las redes públicas abiertas.
- Mantener un programa de administración de vulnerabilidad:
 - 1. Utilizar y actualizar con regularidad los programas o software antivirus.
 - 2. Desarrolle y mantenga sistemas y aplicaciones seguras.
- Implementar medidas sólidas de control de acceso:
 - 1. Restringir el acceso a los datos del titular de la tarjeta según las necesidades que tenga la empresa.
 - 2. Identifique y autentique el acceso a los componentes del sistema.
 - 3. Restringir el acceso físico a los datos del titular de la tarjeta
- Supervisar y evaluar las redes con regularidad:
 - 1. Rastree y supervise todos los accesos a los recursos de red y a los datos de los titulares de las tarjetas.
 - 2. Pruebe con regularidad los sistemas y procesos de seguridad.

3. Mantenga una política que aborde la seguridad de la información para todo el personal de información.

Guía contra el Carding para clientes de instituciones bancarias

El Carding es una forma de estafa online que consiste en acceder ilegalmente al número de una tarjeta bancaria y a través de un software generar de manera aleatoria la fecha de expiración y el código de seguridad (CVV), con la información que se proporciona en esta guía se pretende disminuir este tipo de fraudes, a continuación, se recomienda:

Activar alertas de movimientos de tarjetas a su teléfono móvil.



No perder de vista las tarjetas al utilizarlas.



No permitir que las personas que hacen el cobro digiten el código PIN, siempre debe hacerlo el titular de la tarjeta.




Evitar las redes o computadoras públicas para hacer compras en línea o utilizar la banca por internet.



NOTA ADICIONAL: Navegación en línea

Los navegadores se comunican con los sitios web con un protocolo llamado HTTP que significa Protocolo de Transferencia de Hipertexto. HTTPS es la versión segura de HTTP. Los sitios web que usan HTTPS encriptan toda la comunicación entre el navegador y el sitio.



 <https://www.website.com>

Los sitios seguros tienen un indicador, como un candado, en la barra de direcciones para mostrar que el sitio es seguro. Siempre se debe asegurar la seguridad al iniciar sesión o transferir información confidencial.



 <http://www.website.com>

seguros y nunca deben usarse cuando se trata con datos personales. Si simplemente se está leyendo un artículo o revisando el clima, el HTTP es aceptable.

En caso de detectar algún importe no reconocido, reportar inmediatamente con la institución bancaria que emitió la tarjeta para realizar el proceso de anulación y cancelación de la tarjeta.



No compartir datos personales bancarios por teléfono al ejecutar compras.



No envíe los datos de cuentas a través de correos electrónicos.



Haga las compras en portales web dedicados a las ventas en línea que posean una trayectoria siendo estas conocidas y prestigiosas.



Siempre realice sus compras empleando plataformas de pago seguras y solo visite establecimientos con prestigio.

Cubrir siempre en todo lugar el teclado cuando se deba digitar claves confidenciales.



- Emplear cajeros automáticos que se encuentren en lugares bien iluminados.
- Proteger la pantalla y el teclado para que nadie pueda ver el PIN o la transacción que se esté realizando.
- Una vez realizada la operación guardar el dinero, la tarjeta y el recibo inmediatamente.
- En caso de observar una persona sospechosa, se aconseja cancelar la transacción y abandonar inmediatamente el cajero automático
- Al momento de utilizar un cajero automático cerrado en el que se requiera el uso de la tarjeta para ingresar, hay que evitar que personas extrañas ingresen detrás.
- Controlar constantemente sus operaciones solicitando a la entidad bancaria la activación de las notificaciones automáticas de operaciones y saldos disponibles en cuentas.
- Ante cualquier situación, acudir ante la agencia bancaria o autoridades policiales.



Instala un antimalware y antispyware de confianza en el ordenador, con el fin de evitar la implantación de cualquier programa o aplicación usada para espiar la actividad en la red y captar información sensible.

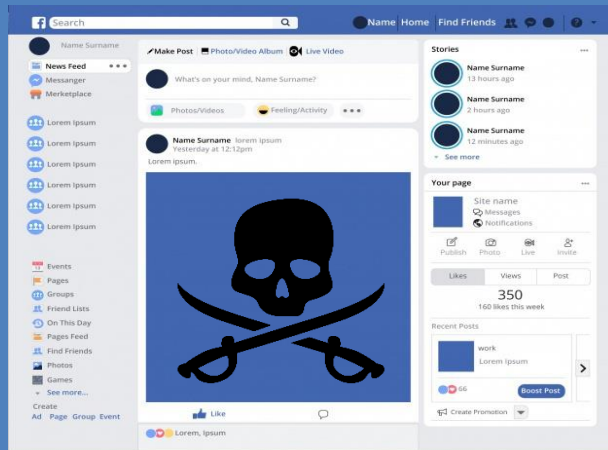
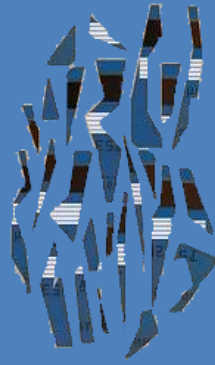
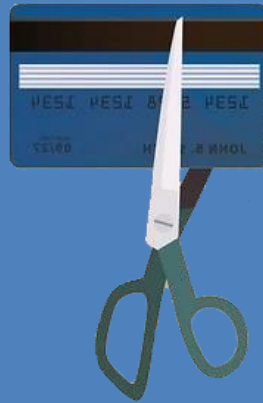


Mantenga actualizados los programas (incluyendo los de seguridad) para así prevenir vulnerabilidades y que estos instalen nuevos malwares que controlarán y robarán datos personales.



Cuando solicite una tarjeta de crédito y se reciba en el domicilio, se debe comprobar que el sobre se encuentre completamente cerrado y no presente indicios de haber sido revisado. De lo contrario, lo mejor será comunicarlo a la entidad bancaria y devolver esa tarjeta.

Si, por cualquier razón, se va a dejar de utilizar la tarjeta de crédito, se recomienda cortarla en varios pedazos hasta destruir el chip y la banda magnética en su totalidad. Hecho esto, se desecha esos pedazos en diferentes contenedores de basura.



Evita utilizar sitios webs ilegales, foros malintencionados o páginas de Facebook sospechosas, ya que, estos son los principales focos de los carders para elegir sus víctimas.

Siempre escriba la dirección del banco, por ejemplo www.nombre.com directamente en el navegador.



Medidas de seguridad en oficinas y entidades bancarias.

- Identifique plenamente los funcionarios del banco.
- Entregue sus instrumentos solamente en la ventanilla.
- Cualquier anomalía que observe dentro de la entidad, comuníquela de forma inmediata a un funcionario de la entidad identificado con su credencial.



En caso de descubrir que algún estafador digital ha descifrado las credenciales de la tarjeta de crédito y está haciendo Carding con la misma, lo más recomendable será notificar a la entidad bancaria a la cual pertenece la misma y de inmediato, cancelar la tarjeta, ya que, solo de esta forma, se podrá evitar una mayor estafa.

