OFICINA DE POSTGRADOS

TEMA:

MECANISMOS DE CIBERSEGURIDAD EN DISPOSITIVOS DE TELETRABAJO PARA UNA INSTITUCIÓN FINANCIERA

Proyecto de investigación previo a la obtención del título de Magister en Ciberseguridad

Línea de Investigación:

Protección de datos y Comunicaciones / Seguridad de la Información

Autor:

Ing. Paúl Sebastián Silva Guevara

Director:

Ing. Mg. Galo Mauricio López Sevilla

Ambato – Ecuador

Mayo 2022

PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR SEDE AMBATO

HOJA DE APROBACIÓN

Tema:

MECANISMOS DE CIBERSEGURIDAD EN DISPOSITIVOS DE TELETRABAJO PARA UNA INSTITUCIÓN FINANCIERA

Línea de Investigación:

Protección de datos y Comunicaciones / Seguridad de la Información

Autor:

Ing. Paúl Sebastián Silva Guevara

Galo Mauricio López Sevilla Ing. MSc. f._____
CALIFICADOR

Paul Hernán Zurita Llerena, Ing. MSc. f._____
CALIFICADOR

Liliana del Rocío Mena Hernández, Ing. MSc. f._____
CALIFICADOR

Juan Carlos Acosta Teneda, P. PhD. f._____
DIRECTOR UNIDAD ACADEMICA

Hugo Rogelio Altamirano Villarroel, Dr. f._____
SECRETARIO GENERAL PUCESA

Ambato - Ecuador

Mayo 2022

DECLARACIÓN DE AUTENCIDAD Y RESPONSABILIDAD

Yo: **PAÚL SEBASTIÁN SILVA GUEVARA**, con **CC. 180365004-1**, autor del trabajo de graduación intitulado: **"MECANISMOS DE CIBERSEGURIDAD EN DISPOSITIVOS DE TELETRABAJO PARA UNA INSTITUCIÓN FINANCIERA"**, previa a la obtención del título profesional de **MAGISTER EN CIBERSEGURIDAD**, en la oficina de posgrados.

1. Declaro tener pleno conocimiento de la obligación que tiene la Pontificia Universidad Católica del Ecuador, de conformidad con el artículo 144 de la Ley Orgánica de Educación Superior, de entregar a la SENESCYT en formato digital una copia del referido trabajo de graduación para que sea integrado al Sistema Nacional de Información de la Educación Superior del Ecuador para su difusión pública respetando los derechos de autor.

2. Autorizo a la Pontificia Universidad Católica del Ecuador a difundir a través de sitio web de la Biblioteca de la PUCE Ambato, el referido trabajo de graduación, respetando las políticas de propiedad intelectual de Universidad

Ambato, mayo 2022

PAÚL SEBASTIÁN SILVA GUEVARA

CC. 180365004-1

DEDICATORIA

Dios me ha dado el regalo más hermoso de la tierra, la oportunidad de ser padre, por esa razón, dedico este proyecto al ser que ilumina mi vida cada día, quien con una sonrisa hace que todo sea perfecto, quien con un abrazo y un beso logra darme esa fuerza que necesito para seguir adelante, mi hija, mi princesa hermosa Ana Paula Silva, quien es el motor que me inspira día a día para ser mejor, también a mi esposa por estar incondicionalmente en todo este proceso. Las amo con todo mi corazón, para ustedes y por ustedes, es que vale la pena todo el esfuerzo y sacrificio realizado durante esta maestría y el resto de mi vida.

AGRADECIMIENTO

Primeramente agradezco a Dios por permitirme poder cumplir una meta más en mi vida profesional, a mi familia, mis padres y hermano quien supieron siempre apoyarme, y sobre todo de manera especial a mi esposa y mi hermosa hija, quienes estuvieron siempre a mi lado en cada proceso hasta llegar a culminar este proyecto, también un agradecimiento a la Cooperativa Oscus, quienes supieron brindarme su apoyo, a todos ellos un Dios les pague y muchas gracias por estar a mi lado y confiar siempre en mí, de corazón, muchas gracias.

RESUMEN

La situación de emergencia sanitaria que afronta la sociedad obliga a cambios de paradigma en el ámbito laboral, es así como los ambientes de trabajo se han desplazado hacia los hogares. Esta realidad para las empresas financieras que manejan datos críticos, donde el acceso a los diferentes sistemas de información que permiten el funcionamiento de la organización; representa un ambiente de alta vulnerabilidad, puesto que se han desplazado los equipos de trabajo del ambiente seguro de la organización a los hogares del personal interno. En este ambiente laboral resulta importante buscar mecanismos que mitiguen las vulnerabilidades a las que la información se ve expuesta. El objetivo que plantea la investigación es implementar mecanismos de ciberseguridad en los dispositivos de teletrabajo para asegurar la información de la institución financiera. Para lo cual, se aplicará como metodología de desarrollo el diagnóstico de seguridad mediante la aplicación de una lista de chequeo, un análisis de riesgos aplicándose la norma ISO/IEC 27005:2009 y Magerit v3 para un escaneo de vulnerabilidades sobre los equipos del personal interno en una prueba piloto, buscándose de esta forma dotarles a los equipos de un conjunto de mecanismos que articulados adecuadamente brinden a la organización ambientes de teletrabajo más fiables.

PALABRAS CLAVES: Ciberseguridad, dispositivos, teletrabajo, institución financiera, riesgo, mitigación, mecanismos, vulnerabilidades.

ABSTRACT

The health emergency situation faced by society forces a paradigm change in the workplace, and work environments have shifted to homes. This reality fact for financial companies that handle critical data, where access to the different information systems that allow the operation of the organization; represents a highly vulnerable environment, since the work teams have moved from the safe environment of the organization to the homes of internal staff. In this new work environment, it is important to seek for mechanisms that minimize the vulnerabilities to which the information is exposed. The main purpose of the research is to implement cybersecurity mechanisms in teleworking devices to secure financial institutions' information. For this purpose, a security diagnosis will be applied as a development methodology through the application of a checklist, a risk analysis applying the ISO/IEC 27005:2009 and Magerit v3 standar for a scan of vulnerabilities on the equipment of internal staff in a pilot test, thus seeking to provide the equipment with a set of mechanisms that properly articulated provide the organization with more reliable teleworking environments.

KEYWORDS: Cybersecurity, devices, telework, financial institution, risk, mitigation, mechanisms, vulnerabilities.

ÍNDICE DE CONTENIDO

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

INTRODUCCIÓN

La situación de emergencia sanitaria que afronta la sociedad obliga a cambios de paradigma en el ámbito laboral, es así como los ambientes de trabajo se han desplazado hacia los hogares. Esta realidad para las empresas financieras que manejan datos críticos, donde el acceso a los diferentes sistemas de información que permiten el funcionamiento de la organización; representa un ambiente de alta vulnerabilidad, puesto que se han desplazado los equipos de trabajo del ambiente seguro de la organización a los hogares del personal interno.

En este ambiente laboral resulta importante buscar mecanismos que mitiguen las vulnerabilidades a las que la información se ve expuesta. La idea principal que plantea la investigación es implementar mecanismos de ciberseguridad en los dispositivos de teletrabajo para asegurar la información de la institución financiera.

nivel mundial la forma de ver el teletrabajo es diversa, que tiene como aspecto común ser una forma de empleo que pretende omitir una de las características tradicionales en las relaciones laborales como es la prestación presencial del servicio y conforme a lo consagrado en las legislaciones se supedita a la utilización de las denominadas tecnologías de la comunicación y la información o simplemente a otras estrategias que suplan el desplazamiento del trabajador a lugares específicos de trabajo (Cataño Ramírez & Gómez Rúa, 2014)

En el mundo actual, los riesgos de ser víctimas de un incidente de ciberseguridad se multiplican, y la superficie de exposición al riesgo cada día es mayor, aplicaciones, servicios, activos de tecnologías de información u otros componentes, ordenadores, smartphones, dispositivos del internet de las cosas “IoT” conectados a internet; servicios de cibercrimen, que se ofrecen a cualquiera que esté dispuesto a pagar por ellos; *ransomware “as a service”*, comercializándose los elementos necesarios para ejecutar estas actividades, incluso sin habilidades o conocimientos técnicos por parte del comprador (ESIC & Marketing, 2020).

En el ámbito internacional, la Organización Internacional de Trabajo (OIT), define el teletrabajo como una forma de trabajo en la cual:

a) el mismo se realiza en una ubicación alejada de una oficina central o instalaciones de producción, separándose así al trabajador del contacto personal con colegas de trabajo que estén en esa oficina y,
b) la nueva tecnología hace posible esta separación facilitándose la comunicación.

Por tal motivo, esto implica concebir el teletrabajo como una manera de organizar y realizar el trabajo a distancia con la asistencia de las Tecnologías de la Información y la Comunicación (TIC) en el domicilio del trabajador o en lugares o establecimientos ajenos al empleador, por lo tanto, es posible interpretarse que las dificultades para implementar el teletrabajo estarían cimentadas en la ausencia de la normatividad en material de teletrabajo, pues es de reconocimiento mundial el avance tecnológico, las redes de comunicación y la Internet. En la medida que se amplíen las interpretaciones o improvisaciones de quienes quieran implementarlo existirá mayor desventaja y de manera especial para el futuro teletrabajador. (Cataño Ramírez & Gómez Rúa, 2014).

A nivel de Latinoamérica, se encuentra como definición amplia la propuesta en la que se indica que se entiende el teletrabajo como toda actividad de trabajo que a distancia pueda comercializarse por Internet ya sea para comprar o vender productos o servicios. Para desarrollar esta modalidad de trabajo, en estos países, donde no está claramente legislado como modalidad o alternativa de contratación, lo necesario es que la persona elabore un producto o un servicio y con el uso de un computador y del canal de conexión a Internet se encargue de su publicación en la web para subastarlo y poder así obtener el comprador; este último es quien paga por lo adquirido también conectado por la Internet y el teletrabajador despacha el producto o servicio a vuelta de correo (Cataño Ramírez & Gómez Rúa, 2014).De igual manera las regulaciones del teletrabajo a nivel de Iberoamérica, en su mayoría se encuentran acogidas en normativas generales de cada uno de sus países, sobre

las relaciones laborales y las condiciones de trabajo como se muestra en forma resumida a continuación en la **Tabla 1**.

Tabla 1. Resumen normativas generales

PAIS	REGULACIÓN ESPECÍFICA	REGULACIÓN GENERAL (*)
Argentina	En trámite	Ley Contrato de Trabajo
Bolivia		
Brazil	Ley 13.467/2017	
Chile		Ley 21.220/2020
Colombia	Ley 1.221/2008	
Costa Rica	Decreto 34.704/2008	
Ecuador	Acuerdo Ministerial 190/2016	
El Salvador	Decreto 600/2020	
España	En trámite	Estatuto de los trabajadores
Guatemala	En trámite	
Honduras	Decreto 33/2020	
México	En trámite	
Panamá	Ley 12682019	
Rep. Dominicana		Resolución 007/2020
Portugal		Código de Trabajo 2003
Perú	Ley 30.036/2013	
Uruguay	En trámite	
Venezuela	No	No

Fuente: Organización Iberoamericana de Seguridad Social

En el contexto ecuatoriano, el ambiente de teletrabajo ha significado para las grandes organizaciones financieras un problema por resolver en el área de la ciberseguridad, de igual forma la gran cantidad de personal interno existente en la Cooperativa Oscus que realizan sus labores cotidianas desde sus hogares, se ven expuestos a vulnerabilidades que van desde la configuración de actualizaciones de los sistemas operativos, *spam* de correos, virus informáticos; hasta el filtrado de información sensible de cuentas, tarjetas y credenciales de acceso de cada uno de los usuarios para el ingreso a las distintas plataformas informáticas de la institución. En ciertos casos la institución ha dotado de equipos para la conexión a las plataformas internas, pero en otros casos el personal debe conectarse con sus equipos personales, comprometiendo tanto la seguridad de la infraestructura como de la información.

El Acuerdo 190 de 2016 establece que el teletrabajador gestionará la organización de su tiempo de trabajo. Sin embargo, la jornada de trabajo no podrá exceder los límites establecidos en el Código del Trabajo. La carga laboral y criterio de resultados será equivalente y comparable al de las personas trabajadoras que se desempeñan en las instalaciones del empleador/a. En todo caso, el horario de trabajo podrá ser pactado y modificado por las partes. Los trabajadores que se encuentren bajo la modalidad de teletrabajo tienen la obligación de cuidado y custodia de las herramientas entregadas para el desempeño de sus funciones fuera del lugar del trabajo y la obligación de mantener la confidencialidad de información a las que tuvieran acceso debido a sus actividades (OISS, 2020).

Es por lo cual se plantea la pregunta de ¿cómo se mitigan las vulnerabilidades de ciberseguridad en los dispositivos de teletrabajo de la Cooperativa de Ahorro y Crédito Oscus Ltda.? Para lo cual, se realizará la ejecución de tareas en la cual lo principal es lograr implementar mecanismos de ciberseguridad en dispositivos de teletrabajo para asegurar la información de una institución financiera, procediendo primeramente con la recopilación de información de artículos académicos sobre mecanismos de ciberseguridad existentes relacionados con dispositivos de teletrabajo.

Una vez que se obtenga la información, es necesario diagnosticar los diferentes mecanismos de ciberseguridad encontrados, luego validarlos mediante la ayuda de un plan piloto dentro de los dispositivos de la institución financiera, para finalmente poder realizar una elaboración de una guía que identifique mecanismos de ciberseguridad aplicables en la Cooperativa Oscus para los dispositivos de teletrabajo, mejorándose la seguridad de la información en la institución financiera.

Por consiguiente se procede con la aplicación de metodologías de investigación, las cuales permitirán identificar de mejor manera los estándares de seguridad y los riesgos que conlleva la falta de aplicación de mecanismos de ciberseguridad dentro de las instituciones financieras, como es el caso de las normas ISO/IEC

27005:2009 el cual es un estándar internacional que se ocupa de la gestión de riesgos de seguridad de información y además es aplicable a todo tipo de organizaciones que tengan la intención de gestionar los riesgos que complicarían la seguridad de la información de su organización (SGSI, 2014). De igual manera la aplicación de MAGERIT V3 el cual es una metodología de análisis y gestión de riesgos, que ofrece un método sistemático para analizar los riesgos derivados del uso de tecnologías de la información y comunicaciones, las cuales permiten implementar medidas de control más adecuadas para poder mitigar los riesgos, además analiza el impacto que tendría para la empresa la violación de la seguridad (Gutiérrez Amaya, 2013).

El desarrollo del presente proyecto es justificable, permite a la institución mantener la seguridad de la información, debido a la aplicación de mecanismos de ciberseguridad en los dispositivos que los usuarios internos utilizan para teletrabajo, se prevendrían diferentes tipos de ciber ataques. Es necesaria la aplicación de esto, en la actualidad nadie se encuentra libre de ser atacado y mucho menos entidades financieras, por esta razón se mantendría protocolos de seguridad tanto para los equipos internos como para los que el personal utiliza para realizar sus labores cotidianas, pero desde teletrabajo. Los beneficios que aporta para la institución principalmente es el resguardo de la información, evitar que ciber delincuentes se infiltren y sustraigan el bien más valioso dentro de una entidad financiera que son los datos, mantener equipos seguros, brindar al usuario interno la fiabilidad de que trabajarían desde sus hogares con la tranquilidad de poder ingresar con sus credenciales y cuentas a las diferentes aplicaciones que se manejan diariamente dentro de la institución y obviamente con la confianza de que cuentan con equipos seguros.

Entre las características del teletrabajo se compara el antes y después del mismo, teniendo en cuenta como se muestra en la **Tabla 2**, el tiempo de trabajo, el sitio, las agendas de reuniones, los controles, restricciones y demás características que esto conlleva. Por lo cual al teletrabajo se lo considera a partir de sus características

como una actividad laboral que se lleva a cabo fuera de la institución en la cual se encuentran centralizados todos los procesos, además la utilización de tecnologías para facilitar la comunicación entre las partes sin necesidad de estar en un lugar físico determinado para cumplir sus funciones y finalmente, generar un modelo organizacional diferente al tradicional que replantea las formas de comunicación interna de la organización y en consecuencia genera nuevos mecanismos de control y seguimiento a las tareas (MinTIC, 2008).

Tabla 2. Características del Teletrabajo

ANTES		***AHORA***	
	Horarios fijos de 8 horas continuas		Horarios flexibles de acuerdo con las necesidades del cargo y resultados esperados
	Trabajo únicamente en la oficina asignada por la institución		Trabajo desde cualquier lugar con acceso a internet.
	Uso de computadores pertenecientes a la institución		Dispositivos de oficina o propios, Bring Your Own Device (BYOD)
	Sistemas de monitoreo y control físicos al ingreso.		Control mediante medición de resultados
	Reuniones laborales limitadas a encuentros físicos		Reuniones virtuales con participaciones ilimitadas

Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones

CAPITULO I. ESTADO DEL ARTE Y LA PRÁCTICA

2.2. Mecanismos de Ciberseguridad

Ciberseguridad

Los profesionales de *Information Systems Audit and Control Association* (ISACA), definen la ciberseguridad como “una capa de protección para los archivos de información, que, a partir de ella, se trabaja para evitar todo tipo de amenazas, las cuales ponen en riesgo la información que es procesada, transportada y almacenada en cualquier dispositivo” (Rubio, 2020). Según Viu (2021), la ciberseguridad es la protección de sistemas, datos, software y hardware que están conectados a Internet. Su objetivo es principalmente proteger los datos, muchos de ellos confidenciales, de las empresas evitándose el robo de estos, los ataques cibernéticos y las usurpaciones de identidad.

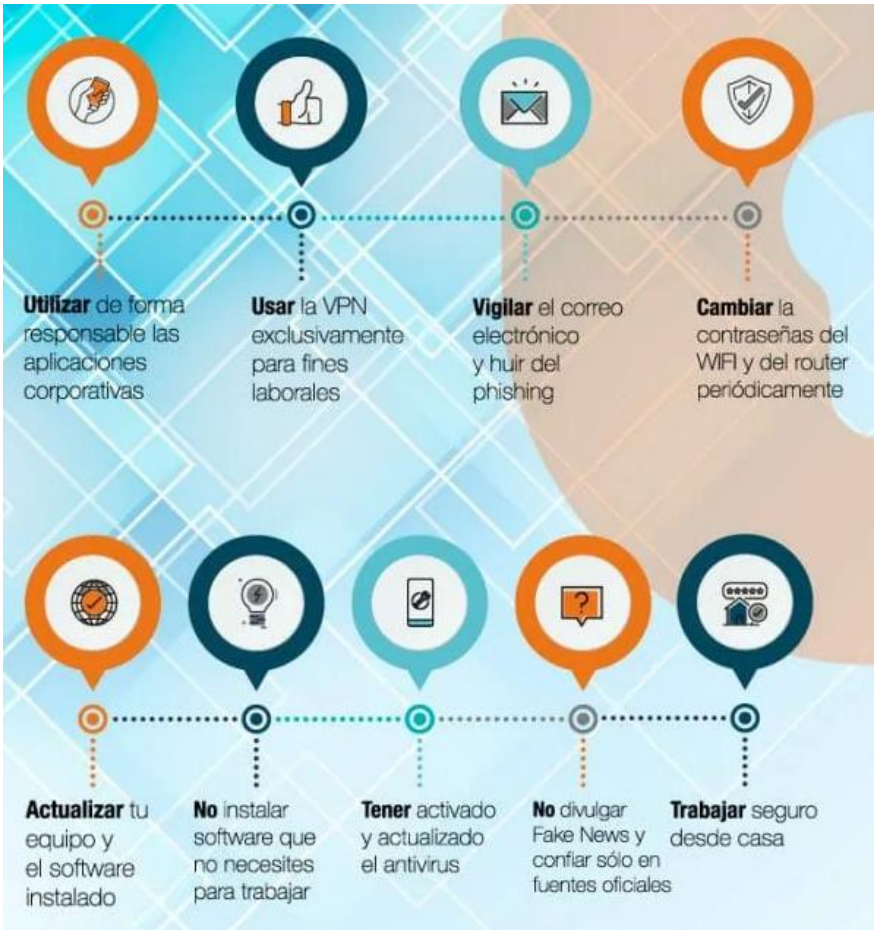
De acuerdo con Kaspersky (2021), la ciberseguridad, es la práctica de defender las computadoras, los servidores, los dispositivos móviles, los sistemas electrónicos, las redes y los datos de ataques maliciosos. También se conoce como seguridad de tecnología de la información o seguridad de la información electrónica. El término se aplica en diferentes contextos, desde los negocios hasta la informática móvil, y puede dividirse en algunas categorías comunes.

Cada vez es más habitual encontrar en medios de comunicación, noticias relacionadas con ciberataques, filtración de datos, escándalos de privacidad, todo tipo de sucesos contra la seguridad. Estos incidentes no se limitan a intentos de ataques contra grandes empresas, instituciones financieras o importantes gobiernos, éstos suelen ser los más protegidos (ElevenPaths, 2021). A la hora de atacar, los cibercriminales no distinguen entre tamaño o sector de empresa, afectándose también al usuario final, muchos de estos se encuentran desprotegidos porque no conocen sobre técnicas, mecanismos o herramientas de protección, siendo un problema tan evidente e importante del que todos son conscientes, la pregunta que surge es ¿existen mecanismos de ciberseguridad que permitan

fortalecer la seguridad en el día a día?; y la respuesta depende de cada uno y del interés que se ponga en protegerse.

Algunos métodos de seguridad que serían utilizados se los muestra en la **Figura 1**, la cual contempla el uso de forma responsable, así como las conexiones de acceso, credenciales y actualizaciones para poder realizar un trabajo seguro.

Figura 1. Medidas de ciberseguridad



Fuente: mtp, Digital Business Assurance, 2020

Actualizaciones

Cada vez que se recibe una notificación para actualizar el sistema, lo primero que se hace es evadirla y eso es uno de los principales errores como usuarios. Mantener los sistemas actualizados es de una importancia vital, en muchas ocasiones estas actualizaciones lo que hacen es corregir fallos de seguridad o vulnerabilidades descubiertas.

Configuración de red Wi-Fi

Resulta un paso sencillo de realizar y que ahorraría más de un disgusto. Cambiar el nombre y contraseña que vienen por defecto, muchas veces estas contraseñas se repiten de una red a otra y sería sencillo acceder a ellas. Además, es importante ocultar el nombre de la red Wi-Fi y desactivar el *Wifi Protected Setup* (WPS) por la seguridad que esto conlleva.

Contraseñas robustas

Fechas importantes, nombre de familiares o mascotas, preferencias o gustos por algo en específico, son algunas de las tácticas más comunes para elegir contraseñas fáciles de recordar, pero también son las más fáciles de identificar. Como se muestra en la **Figura 2**, se utilizaría contraseñas robustas, para lo cual, se cuenta con muchos caracteres, tanto numéricos como alfabéticos, mayúsculas, minúsculas y caracteres especiales, adicional no utilizar la misma contraseña para todas las cuentas, una vez descubierta, es lo primero que intentan en el resto de las cuentas. Y algo primordial es realizar el cambio de contraseñas periódicamente, esto permite que las cuentas se mantengan un poco más seguras de algún ataque o robo de información.

Figura 2. Contraseñas seguras

Fuente: Universidad Veracruzana – Seguridad de la información, 2021

Utilizar gestor de contraseñas

Una práctica muy habitual y peligrosa es reutilizar contraseñas una y otra vez. Lo ideal es contar con una contraseña para cada aplicación, red social o sistema que

se utilice. Es casi imposible recordar todas y cada una de las contraseñas con las que se cuenta, por eso existen gestores de contraseñas como por ejemplo *Keepass, LastPass* o *1Password*. Además, estos gestores tienen versión móvil así que se los llevaría a todas partes.

Conocimiento personal

Esto especialmente con el ámbito técnico, son los que por lo general deben encontrarse al día con la información referente a seguridad. Si se está al tanto de las técnicas y métodos más habituales de estafa, será mucho más difícil ser víctima de estas.

Sentido común

Parece evidente, pero para evitar caer en ciberataques es importante utilizar el sentido común. Normalmente, si algo es demasiado bueno para ser verdad, lo más seguro es que sea una estafa y terminaría mal. Siempre se averiguaría o consultaría a terceros, buscaría información y, si se sospecha que sería algo malicioso, no arriesgarse a ser una víctima más.

Dispositivo móvil

Muchos usuarios piensan que las amenazas sólo afectan a los computadores, pero no es así. En los últimos tiempos se ha podido identificar cómo cada vez surgen más campañas dirigidas especialmente contra dispositivos móviles, según lo indica (ElevenPaths, 2021).

Una recomendación que se incluiría en una buena estrategia de seguridad de la información es la gestión de activos, la seguridad de las operaciones, la gestión de incidentes, recuperación y el control de acceso a sistemas y aplicaciones, las cuales se especifican cada uno a continuación:

Gestión de activos

Uno de los aspectos más complicados, pero que identificarlo suma importancia.

● Es necesario realizar un inventario completo y clasificado de los dispositivos que la institución posee.

● Es recomendable clasificar la información, considerándose los principios de la seguridad de la información; la confidencialidad, la integridad y la disponibilidad de esta.

● Una vez clasificada, analizar y aplicar medidas para su protección.

● Diseñar y mantener manuales de procesos o procedimientos de gestión de configuración que contenga los elementos para proporcionar un servicio y la relación entre ellos.

Seguridad de las operaciones

Son todas las actividades que se encuentran encaminadas a permitir asegurar el correcto funcionamiento de los equipos donde se procesa la información, para lo cual se consideraría lo siguiente:

● Establecer y documentar los procedimientos y responsabilidades que se realizan en la organización.

● Garantizar la instalación de los sistemas y aplicaciones que se realizan conforme a los lineamientos de seguridad de la organización.

● Gestionar y controlar los sistemas de antivirus de la empresa.

● Implantar un sistema de copias de seguridad.

Gestión de los incidentes y recuperación

Es importante tener presente un plan para poder estar preparados ante cualquier eventualidad. Se establecería responsabilidades y procedimientos.

● Definir la gestión de incidencias de seguridad.

● Establecer un plan de recuperación.

Control de acceso a sistemas y aplicaciones

Algo muy importante dentro de una institución es la prevención al acceso no autorizado a los sistemas y aplicaciones, para lo cual es indispensable establecer políticas de control de acceso físico y lógico, teniendo en cuenta lo siguiente:

● Controlar el acceso a las distintas aplicaciones críticas e incluso a las zonas restringidas.

● Administrar los accesos lógicos, la gestión de credenciales, permisos y medidas de autenticación.

● Gestionar usuarios y gestión de sus respectivos roles.

● Controlar que se mantenga una política de asignación de contraseñas seguras.

Cabe recalcar que , cada organismo a nivel de América Latina y El Caribe mantienen políticas o estrategias para normalizar la ciberseguridad en cada uno de sus países como se muestra en la **Tabla 3**, siendo Chile uno de los países con mayor porcentaje de control contándose con un 72%, a diferencia de Ecuador que únicamente tiene un 43% de control en lo referente a las aplicaciones de control en la ciberseguridad a nivel nacional, en donde se contaría con el apoyo de las diferentes instituciones públicas y privadas para mitigar los diferentes tipos de ataques por parte de ciberdelincuentes a los diferentes organismos, empresas o instituciones de diferente índole que se encuentran vulnerables a ser atacados ya sean estos por falta de controles o de personal especializado en el área, teniendo en cuenta también que un organismo invertiría gran cantidad tanto en su infraestructura como en su seguridad y en capacitación a los diferentes usuarios para poder mantenerse más seguros como institución ante ellos y ante el resto de la gente que confía en ellos.

Tabla 3. Organismos encargados de la elaboración de las Políticas y Estrategias de Ciberdefensa en países de América del Sur

ECUADOR 43 %	COLOMBIA 53 %	BRASIL 58 %	CHILE 72 %	ARGENTINA 65 %
No ha desarrollado una ESTRATEGIA NACIONAL DE SEGURIDAD CIBERNÉTICA, Ecuador ha hecho avances en los últimos años para fortalecer su capacidad para abordar las amenazas informáticas	El Consejo Nacional de Política Económica y Social del Gobierno de Colombia estableció LA POLÍTICA NACIONAL DE SEGURIDAD CIBERNÉTICA CONPES 3701 bajo el auspicio del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), el Ministerio de Defensa, el Departamento Nacional de Planeación y otras instituciones nacionales clave	En 2010 el Departamento de Seguridad de la Información y Comunicaciones publicó la Guía de Referencia para la Protección de Infraestructuras Críticas de Información y el Libro Verde de Seguridad Cibernética en Brasil. ESTRATEGIA NACIONAL DE SEGURIDAD DE LAS COMUNICACIONES DE INFORMACIÓN Y SEGURIDAD CIBERNÉTICA DE LA ADMINISTRACIÓN PÚBLICA FEDERAL	El Ministerio del Interior y Seguridad Pública, el Secretario General de la Presidencia y la Subsecretaría de Telecomunicaciones son los principales organismos nacionales que establecen LA POLÍTICA DE SEGURIDAD CIBERNÉTICA A NIVEL GUBERNAMENTAL	Programa Nacional de Infraestructuras Criticas de Información y Ciberseguridad (ICIC) y en coordinación con diversos organismos, instituciones académicas y el sector privado, el Gobierno de Argentina ha desarrollado un proyecto de ESTRATEGIA NACIONAL DE SEGURIDAD CIBERNÉTICA Argentina se distingue por haber formado el primer CSIRT nacional en 1994, que desde 2011 ha funcionado bajo el ICIC. ICIC-CERT
El Centro de Operaciones Tecnológicas Estratégicas y Contrainteligencia de la Secretaría de Inteligencia se encarga de los aspectos técnicos de la seguridad cibernética del país y un CSIRT nacional, el EcuCERT, entró en funcionamiento en noviembre de 2013	Las fuerzas del orden y el Poder Judicial tienen la capacidad de investigar y manejar casos de delincuencia cibernética	Las Fuerzas Armadas brasileñas también discuten las preocupaciones sobre defensa cibernética en su Libro Blanco de Defensa Nacional 2012. Recientemente crearon un Comando de Defensa Cibernética formal y una Escuela Nacional de Defensa Cibernética, además del Centro para la Defensa Cibernética del Ejército (CDCiber)	Las ramas de las Fuerzas Armadas de Chile comparten responsabilidades de defensa cibernética e información pero no tienen una estructura central de mando y control.	2015 la Presidencia de la República de Argentina emitió el Decreto nº 1067/2015 que reestructuró el control gubernamental de la ICN, y estableció una Oficina Nacional bajo la dirección de la Subsecretaría de Protección de Infraestructuras Críticas de Información y Ciberseguridad bajo la Jefatura del Gabinete de Ministros y Secretaría del Gabinete

Fuente: OBSERVATORIO DE LA CIBERSEGURIDAD EN AMÉRICA LATINA Y EL CARIBE 2016

Ciberseguridad en Teletrabajo

La modalidad de teletrabajo en la actualidad se ha convertido en uno de los escenarios principales en las instituciones para poder cumplir con sus actividades, lo cual implica que la comunicación con el entorno de trabajo se realice a través de correos, chats, videoconferencias, redes privadas virtuales (*VPN*) y otros, implicándose el uso de redes externas de Internet para conectarse a la red corporativa, la misma red a la que están conectados varios dispositivos inteligentes, todas estas tecnologías podrían ser la puerta de entrada que utiliza un atacante.

El teletrabajo también implica que algunos usuarios deban hacer uso de su computador personal para desempeñar sus actividades, o dependiendo del caso,

sería que utilicen el computador que les brinda la institución en la cual laboran, pero también para realizar actividades personales que tal vez en la oficina no lo podrían realizar debido a los controles o restricciones que cuentan en las políticas de seguridad de la institución, como realizar compras por internet, utilizar las redes sociales o acceder a servicios personales como el correo electrónico o algo más delicado como el acceso a sus cuentas bancarias, corriendo el riesgo de que sus datos sean violados, y analizándose un paso más adelante el riesgo de que la información de la institución llegaría a ser vulnerada.

Algo que se ha podido observar durante este tiempo es el incremento en lo referente a ataques de ingeniería social, en el cual los ciberdelincuentes distribuyen distintos tipos de información maliciosa, en donde lo que buscan es intentar engañar a los usuarios con información falsa para distribuir publicidad invasiva, mientras que otros más peligrosos intentan distribuir *malware*, suplantándose la identidad de alguna marca, entidad, o en estos últimos meses aprovechar información de la pandemia en la cual el mundo entero se encuentra viviendo.

El teletrabajo abrió un gran reto a las empresas que garantizaría la seguridad de sus datos y sistemas en un contexto remoto, como consecuencia de la pandemia y el aislamiento social, hoy se afirmaría que el teletrabajo es moneda corriente. Esta modalidad se acentuó vertiginosamente en los últimos meses, empujando a las empresas a adaptarse en todos sus aspectos: trabajo a distancia, capacitación de los equipos, infraestructuras para el *home office* y, sobre todo, ciberseguridad. (Lzzia, 2021).

Triada de la Seguridad

Más conocida como la *CIA TRIAD*, la triada de la seguridad informática se compone de tres propiedades principales como se muestra en la **Figura 3**, la confidencialidad, la integridad y la disponibilidad, pilares fundamentales e importantes dentro de la seguridad de la información, una depende de la otra y viceversa, permitiendo el cumplimiento de la institución en brindar el servicio adecuado, seguro, exacto y a tiempo.

Figura 3. *Triada de la Seguridad*

Fuente: Castro, Introducción a la Ciberseguridad, 2021

Confidencialidad

La confidencialidad se refiere a los esfuerzos de una institución por mantener sus datos privados, secretos y seguros, por lo cual se trata de controlar el acceso a los datos para evitar su divulgación no autorizada, esto implica asegurarse que sólo aquellos usuarios autorizados tengan accesos específicos y que quienes no están autorizados, sean impedidos de obtener acceso. Además, dentro de un grupo de usuarios autorizados, existiría limitaciones adicionales y más estrictas en cuanto a la información a la que dichos usuarios autorizados accederían. Para proteger la

confidencialidad incluyen la clasificación y el etiquetado de los datos; controles de acceso y mecanismos de autenticación, así como encriptación de los datos en proceso, en tránsito y en almacenamiento, de igual manera la capacidad de borrado remoto, educación y capacitación adecuadas para todos los usuarios con acceso a los datos. (Walkowski, 2019). De igual manera como manifiesta Rock (2018), los datos estarían solo al alcance de los usuarios autorizados, para lo cual deben establecerse políticas de control de acceso para evitar que la información clasificada caiga en manos equivocadas, ya sea de forma intencional o no, de un usuario sin acceso.

De tal manera la institución establecería diferentes políticas de control y de seguridad para poder mantener la confidencialidad de su información una forma segura, teniendo en cuenta que al realizar el trabajo, los equipos externos tendrían la probabilidad de correr riesgo de algún ciberataque y perder la confidencialidad de los mismos, por tal razón, los accesos, autorizaciones, roles y demás permisos que se les otorga a cada uno de los usuarios de internet serían controlados correctamente por los diferentes departamentos que los otorgan dentro de la institución financiera.

Integridad

Empleándose las palabras de Walkowski (2019), en seguridad informática, la integridad consiste en garantizar que los datos no hayan sido manipulados y, por lo tanto, sean confiables. Garantizar la integridad implica proteger los datos en uso, en tránsito (por ejemplo, al enviar un correo electrónico o al cargar o descargar un archivo) y al almacenarlos, ya sea en aparatos físicos o en la nube. Para proteger la integridad de los datos se incluye la encriptación, funciones *hash*, firmas y certificados digitales, sistemas de detección de intrusos, auditorías periódicas, control de versiones, mecanismos de autenticación, y los controles de acceso.

Desde el punto de vista de Mejía (2018) la integridad se analizaría desde 3 perspectivas:

a. Prevenir que alguien con permisos de modificación cometa algún error y modifique los datos.
b. Prevenir que alguien sin permisos de modificación realice algún cambio.
c. Prevenir que algún programa o aplicativo que interactúa directamente con la información “objetivo” realice algún cambio.

La violación a la integridad no solo sería efectuada por los ciber atacantes, al igual que la confidencialidad se debería a fallas en los mecanismos de seguridad, configuraciones o incluso derivado del error humano.

Al momento de realizar teletrabajo si los equipos no se encuentran parametrizados correctamente para que estos trabajen fuera de la infraestructura de la institución, podría ser vulnerable a perder la integridad de la información que no se identificaría la manera y que cada uno de los colaboradores se encuentra realizando su trabajo en sus hogares, por tal motivo los principales responsables encargados de que la información no sea alterada ni manipulada de una manera errónea son los propios usuarios con sus permisos y accesos.

Disponibilidad

La disponibilidad implica que la información tiene que ser accesible para los usuarios autorizados dentro de un tiempo establecido, dicho de otra manera, la información debe estar siempre disponible para el usuario autorizado (Rock, 2018). De igual manera la disponibilidad significa que las redes, los sistemas y las aplicaciones están en su pleno funcionamiento, garantizándose que los usuarios autorizados tengan acceso oportuno y fiable a los recursos si los necesiten. Entre las medidas para asegurar la disponibilidad están la redundancia en servidores, redes, aplicaciones y servicios, tolerancia a fallos de hardware para servidores y almacenamiento, parches de software y actualizaciones de sistema regulares (Walkowski, 2019).

En la opinión de Mejía (2018), enfatiza que la disponibilidad de la información hace referencia a mantener activo el acceso a la información necesaria a aquellas

personas que tendrían acceso a la misma en el momento que sea necesario. Al igual que las propiedades anteriores, el impacto a la disponibilidad se debería también al error humano. Uno de los mayores inconvenientes al realizar teletrabajo sería la disponibilidad de la información, por varios motivos cómo sería, conexiones, accesos, roles, estos impedirían que la información se encuentre disponible al momento en que se la necesite, es por lo cual se encontrarían bien establecidas todas estas políticas de control para que los usuarios finales que necesitan hacer uso de la información de la institución accedería sin inconvenientes y brindar la atención adecuada a los socios y clientes de la cooperativa.

Estos tres componentes dependen tanto del uno como del otro, si no se tiene confidencialidad por parte de los usuarios o los controles, existe una gran posibilidad de que la integridad de la información llegaría a ser vulnerada, y si la integridad de esta información llega a ser alterada, generaría un gran impacto en la disponibilidad de la misma, la información se vería afectada y no se podría brindar el servicio esperado, y mucho más si se trata de una institución financiera la cual necesita tener la información clara y precisa en todo momento y obviamente confiando de que se encuentra segura.

Seguridad de la información en instituciones financieras

Todos los días, el mundo se vuelve más conectado, lo que significa una mayor vulnerabilidad de los bancos. También significa una mayor demanda de los clientes para garantizar la seguridad de sus activos financieros. Los clientes corren un gran riesgo al seleccionar un banco, y es responsabilidad del sector financiero implementar la mejor tecnología para asegurar los recursos que están a su cuidado (Solis, 2018).

La administración de seguridad de la información se encuentra distribuida principalmente entre las áreas de tecnología y seguridad de la información, cuyas actividades vienen desde:

- la creación y eliminación de usuarios
- la verificación y asignación de perfiles en las diferentes aplicaciones

- el control de la red
- administración de dispositivos de seguridad como firewall
- administración de accesos a las respectivas aplicaciones incluyendo la información interna.

Para el Foro Económico Mundial, la división del trabajo entre humanos, máquinas y algoritmos creará 133 millones de nuevos roles en los próximos años, consolidándose el uso de la tecnología en la optimización del trabajo con fenómenos importantes como la normalización del teletrabajo que obligan a todas las organizaciones a actualizar su infraestructura TI, donde la nube tiene un papel protagónico. El confinamiento provocado por la pandemia del COVID-19 demostró que las empresas que mejor han resistido la crisis han sido las que han podido mantener sus actividades desde un entorno digital sin perder su eficiencia. (González Fajardo, 2021).

Para evitar hackeos informáticos, los empleados bancarios utilizarían siempre los dispositivos que haya facilitado la empresa. También tienen que mantener las políticas de seguridad y emplear el ordenador de la empresa o el móvil de la compañía solo para tareas relacionadas con el trabajo. De hecho, en el caso de que no utilizarían los dispositivos de la empresa, tendrán que informar a sus responsables para adaptar la seguridad de otros dispositivos (González, 2021).

Según lo indicado por Bravo Sandoval (2010), la información es uno de los bienes más importantes que tiene una empresa en especial las Instituciones Financieras, la información incluso es considerada el activo principal y sin la cual la empresa no podría realizar sus operaciones de forma normal, es más importante que la misma edificación o que todos los activos físicos juntos, proteger la información es una tarea que conlleva múltiples escenarios y responsables, los datos correctamente protegidos ayudan a las empresas a levantarse, reconstruirse inclusive si no tuviera un espacio físico luego de un desastre. Pero así también, si la información esta desprotegida contra fugas, sin respaldo; así se disponga de los mejores sistemas de seguridad física, electrónica e infraestructura la empresa no podría ejecutar sus

operaciones e incluso se encontraría en medio de una crisis mayor, su desaparición (Quishpe Reinoso, 2007).

Así también, según Ernst & Young (2012), “La información es poder. Los nuevos paradigmas de enfocar tanto el negocio como la tecnología han provocado el cambio de la protección del perímetro de seguridad hacía el aseguramiento y control a nivel de información y datos”, esto conlleva a reunir los esfuerzos necesarios para proteger la información. Erróneamente se cree que la seguridad de la información simplemente es mantener respaldados los datos, realizándose los procesos de respaldo establecidos y mantener en lugares restringidos, sin tomar en cuenta muchos riesgos existentes y brechas de seguridad que ocasionen perdida de información y que carezcan de controles físicos y lógicos necesarios y adecuados. (Rojas Urgilés & Vela Veintimilla, 2011).

Como manifiesta López Argüello (2013), es por lo que la fuga de información puede ser un problema común para los responsables de seguridad lógica y puede convertirse en un inconveniente muy grave con consecuencias desafortunadas si la información llegara a manos equivocadas. La fuga de información sería tratada como un incidente que sería causado ya sea de forma interna como externa, y a la vez intencional o no. Se mencionaría múltiples causas, por ejemplo: algún funcionario de la empresa que venda información a otra, extravío de documentos en lugares públicos, documentos que se arroja a la basura sin destruir, perdidas de laptops o dispositivos extraíbles que contengan información sensible, fuga por medio de programas de software malicioso o spyware instalados en equipos de cómputo infectados (Bortnik, 2010).

Para lo cual es necesario implementar controles necesarios que vayan de acuerdo con las recomendaciones de los estándares y buenas prácticas internacionales, por lo cual se aborda esta problemática y se analizan controles básicos y controles gestionados por medio de sistemas especializados en prevenir la fuga de información (Quishpe Reinoso, 2007).

CAPITULO II. DISEÑO METODOLÓGICO

2.1. Caracterización de la Cooperativa de Ahorro y Crédito Oscus Ltda.

El primer acto de la Asamblea que descansa en la Cooperativa está fechado el 7 de marzo de 1962 donde se informa que 25 personas están inscritas como miembros de lo que más tarde se convertiría en la Asociación Cooperativa de Crédito del Centro Obrero de Instrucción a los efectos de la aprobación del proyecto Estatuto.

El 23 de junio de 1962: convocado por un comité organizador, encabezado por el Dr. Padre José Arellano, el Sr. Vicente Villarroel, entre otros, en las instalaciones del Centro de Capacitación de Trabajadores, se informa que el 29 de mayo de ese año, mediante acuerdo ministerial 6321, se ha establecido la Cooperativa y se designan los primeros órganos internos: el Consejo de Administración, el Consejo de Supervisión y el Comité de Crédito.

El 23 de junio de 1963 fecha en que se reconoció que la Cooperativa había adquirido su personalidad jurídica ante los Órganos de Gobierno pertinentes, se decidió que las reuniones de la Asamblea se realizarían cada 6 meses y la gestión de la Cooperativa fue delegada a la Junta Directiva. En tales circunstancias y como era normal en ese momento, fue el Consejo de Administración quien tomó las decisiones políticas, administrativas e incluso operativas, respecto al desarrollo de las actividades de la Cooperativa, incluso los primeros gerentes que atendieron a los socios en días designados para este fin, sin recibir una remuneración económica por su gestión.

OSCUS amplía su cobertura a través de su primera oficina, ubicada en el cantón Patate e inaugurada el 13 de diciembre de 1968, que fue el inicio de la expansión de sus servicios en beneficio de sus asociados y la comunidad. Durante la década de 1970, se abrieron nuevas oficinas ubicadas en los cantones de Píllaro, Baños y

Pelileo. La Asociación Cooperativa de Crédito del Centro Obrero de Instrucción mantuvo su razón social hasta 1975, cuando cambió su nombre por el de Obra Social Cultural SOPEÑA 'OSCUS' registrado en la Dirección Nacional de Cooperativas por Acuerdo Ministerial No. 5470 de 19 de septiembre de 1975.

A principios de los años ochenta, OSCUS se aventuró en otra provincia abriendo la oficina de Latacunga en octubre de 1981. El 8 de agosto de 1993, la Superintendencia de Bancos de la República del Ecuador otorgó el certificado de autorización para que pueda operar la Oficina Principal de la Cooperativa de Ahorro y Crédito "OSCUS" LTDA. en la ciudad de Ambato.

Misión

“Somo una Cooperativa sólida que apoya al progreso de nuestros Socios, Clientes y la comunidad, ofreciendo productos financieros y servicios eficientes e innovadores.”

Visión

“Ser una Cooperativa de excelencia que crece con responsabilidad social.”

Política Integrada

“Asumimos el compromiso de ofrecer productos financieros y servicios dirigidos a nuestros Socios y Clientes, así como el cumplimiento de los requisitos aplicables, sustentados en la cultura organizacional, el mejoramiento continuo, la confidencialidad, integridad y disponibilidad de la información; con un equipo humano calificado y permanente innovación organizacional.”

En la actualidad la Cooperativa Oscus cuenta orgullosamente con 16 oficinas distribuidas estratégicamente a nivel nacional, con su oficina matriz en pleno centro de la ciudad de Ambato, en la cual se encuentran los departamentos de Seguridad, TIC, Riesgos, los cuales se encargan de que la seguridad de la información se mantenga segura, confiable y disponible, además, dentro de la provincia de

Tungurahua cuenta con siete sucursales como se muestra en la **Figura 4** distribuidos tres oficinas adicionales en Ambato, una en Pelileo, Patate, Baños y Píllaro.

Figura 4. Enlaces agencias provincia de Tungurahua

Fuente: Enciclopedia del Ecuador – Arreglos personales

Adicional a esto, cuenta con ocho sucursales a nivel nacional como se muestra en la **Figura 5** distribuidos en dos oficinas en Quito, una en Latacunga, Riobamba, Guayaquil, Salcedo, Tena y Puyo.

Figura 5. Enlaces agencias nivel nacional

Fuente: Ecuador noticias – Arreglos personales

A raíz de la emergencia sanitaria que se encuentra en el país a partir de marzo del 2020, la Cooperativa Oscus procedió con el resguardo del mayor bien que la institución tiene el cual son sus usuarios internos, por lo cual, dependiendo del cargo y la labor que desempeñan en la institución se procede a la autorización para la realización de teletrabajo, para lo cual la Cooperativa cuenta con un número limitado de equipos de cómputo portátil, siendo estos configurados para poder hacer uso de los mismos, y para el personal restante se procede con la revisión de los equipos personales propios de cada empleado, identificándose que cuenten con licencias originales, actualizaciones vigentes, antivirus activos y de no ser el caso, la institución provee con una instalación que permita mantener la seguridad tanto de los equipos como de la información.

Metodología de Investigación

La metodología de investigación es una forma estructurada del proceso de investigación que permite la obtención de información requerida para encauzar de manera eficiente la solución al problema (Perez Vera, Ocampo Botello, & Sánchez Pereza, 2015). Es decir, el método es la manera muy organizada y estructurada del trabajo de investigación, o son los procesos que permiten obtener información de manera organizada de los aspectos importantes para ser analizados, revisados y finalmente, procesados a deducir.

2.2.1. Tipo de investigación

El presente proyecto tiene un enfoque de investigación cuantitativo debido a que se intenta centrar fundamentalmente en los aspectos observables de cuantificar los fenómenos que ocurrirían, incluyendo la observación para identificar cuáles serían los factores que puedan involucrarse y adicional, la encuesta que se realizará al personal del área técnica, el cual generará resultados que podrán ser analizados y elaborado pruebas estadísticas de la información obtenida para la toma de decisiones.

2.2.2. Métodos de investigación

Como señala Pulido Polo (2015), es un método complementario que brinda un estudio con mayor fiabilidad, validez y operatividad, que se utiliza en las investigaciones. Por tanto, la investigación tiene un enfoque de carácter descriptivo que ayuda a la comprensión del contexto de ciberseguridad dentro una institución financiera.

El presente proyecto plantea que la investigación realizada para permitir implementar mecanismos de ciberseguridad en los dispositivos de teletrabajo para asegurar la información de la Cooperativa de Ahorro y Crédito Oscus Ltda. para lo cual, se aplicará como metodología de desarrollo el diagnóstico de seguridad mediante la aplicación de una lista de chequeo, un análisis de riesgos aplicandose la norma ISO/IEC 27005:2009 y Magerit v3 para un escaneo de vulnerabilidades sobre los equipos del personal interno en una prueba piloto, buscandose de esta forma dotarles a los equipos de un conjunto de mecanismos que articulados adecuadamente brinden a la organización ambientes de teletrabajo más fiables.

Método teórico:

Análisis-Síntesis

Citando a los autores Rodríguez Jiménez & Pérez Jacinto (2017), se refiere al análisis-síntesis como el proceso lógico que permite descomponer de un todo en partes, y determinar un conjunto de información para el análisis. Este método se lo aplica, es la base para el inicio de una investigación de la realidad, adicionalmente, se requiere la búsqueda, procesamiento y análisis de información de los documentos encontrados, en donde permita relacionar los datos consultados con la realidad que se la palparía dentro de la institución.

Inductivo-deductivo

Desde el punto de vista de Rodríguez Jiménez & Pérez Jacinto (2017), es un conjunto de procedimiento que permite generar conocimientos escenciales de

forma racional y más general de los fenomenos individuales, porque esto ayuda a la organización de los hechos para extraer premisas para un mejor entendimiento y llegar a una conclusión válida. Mediante este método de la inducción y deducción de los hechos a investigar, se encontraría el punto de partida a inferir en la solución concreta del análisis del conocimiento, de forma que los mecanismos de ciberseguridad analizados llegarían a ser ejecutados correctamente permitiendo llegar a resultados óptimos de lo que desde un inicio se tenía planteado.

Método empírico:

Observación

Según Rekalde Rodríguez, Vizcarra Morales, & Macazaga López (2014), la observación es una herramienta de recolección de datos, que se enfoca a obtener información de los comportamientos y acciones del hecho a investigar, pues permite el análisis de las notas indagadas del campo. Por otra parte, la observación es sistemática por el hecho de que toda observación es seleccionada, anotada y codificada para posterior análisis de los sucesos que ocurren de modo natural, esto permite la formulación del problema a investigar y fomentan la obtención de los datos (Pulido Polo, 2015). Por tal motivo referente a la observación, este método permite la obtención de información más abierta desde el punto de vista del investigador que llega a tener contacto directo en el sitio con los involucrados, permitiendo poder determinar el registro de datos observados para su correspondiente análisis.

Encuestas

Citando a Tamayo y Tamayo (2018), la encuesta es aquella que permite dar respuestas a problemas en términos descriptivos como de relación de variables, tras la recogida sistemática de información según un diseño previamente establecido que asegure el rigor de la información obtenida. Es importante señalar que esta técnica se encuentra dirigida al área técnica que comprenden los departamentos de tecnología, seguridad y mesa de servicios de la institución

financiera, son quienes cuentan con un mayor conocimiento sobre el tema. Para lo cual se adjunta el **Anexo 1** con la encuesta que se procede a aplicar a los usuarios involucrados en el área técnica.

2.2.3. Población y Muestra

La Cooperativa de Ahorro y Crédito Oscus Ltda. cuenta con alrededor de 424 usuarios internos distribuidos en las diferentes agencias a nivel nacional, por lo cual, no todos han sido contemplados para la realización de teletrabajo debido a los cargos que mantienen como por ejemplo gerentes, asesores y cajeros quienes obligatoriamente mantendrían contacto directo con los socios y clientes por pertenecer al *front office* de la cooperativa, de igual manera al personal encargado y responsable del negocio, por tal razón se solicita al departamento de Talento Humano de la institución, un listado general del personal que han realizado o se encuentra realizando teletrabajo pertenecientes al área operativa como se muestra en la **Tabla 4**.

Tabla 4. Usuarios del área operativa

USUARIOS OPERATIVOS	
Área	**Cargo**
Contabilidad	Responsable de Contabilidad / Contador 1
Mesa de Servicios	Analista de Mesa de Servicios
Negocios	Coordinadora de Negocios
Operaciones	Responsable de Operaciones / Analista / Asistente de Cartera
Proyectos	PMO
Quejas y reclamos	Asistente de Quejas y reclamos
Seguridad Física	Analista de Seguridad Física
Subgerencia A.F.	Subgerente Adm. Financiera
Tarjetas	Gestor / Analista de Tarjetas / Analista Monitoreo y Antifraude
Tesorería	Tesorero / Analista de Tesorería
TTHH	Responsable TTHH / Analista de Talento Humano
N/A	Gerente Oficina Operativa / Asesor Crédito

Fuente: Departamento de TI – Coop. Oscus

Por lo cual para la obtención de información se realiza una segmentación, considerándose a los usuarios que pertenecen a las diferentes áreas técnicas de la

institución como se muestra en la **Tabla 5** (TI, Seguridad de la Información, Mesa de Servicio).

Tabla 5. Usuarios del área operativa

USUARIOS TÉCNICOS	
Área	**Cargo**
Mesa de Servicios	Analista de Mesa de Servicios
TIC	Responsable de TIC / Adm. Infraestructura / Adm. App y Base de Datos / Analista Programador / Operador de Aplicaciones / Asistente de Hardware y Software
Seguridad de la Información	Responsable de seguridad de la información / Analista de Seguridad / Asistente de Seguridad

Fuente: Departamento de TI – Coop. Oscus

2.3. Metodología de Desarrollo

2.3.1. ISO/IEC 27005:2009

Es un estándar internacional que se ocupa de la gestión de riesgos de seguridad de información. La norma suministra las directrices para la gestión de riesgos de seguridad de la información en una empresa, apoyándose particularmente los requisitos del sistema de gestión de seguridad de la información definidos en ISO 27001. Además, es aplicable a todo tipo de organizaciones que tengan la intención de gestionar los riesgos que complicarían la seguridad de la información de su organización.

No recomienda una metodología concreta, dependerá de una serie de factores, como el alcance real del Sistema de Gestión de Seguridad de la Información (SGSI), o el sector comercial de la propia industria. La norma incorpora algunos elementos iterativos, por ejemplo, si los resultados de la evaluación no son satisfactorios (Espinosa, Martínez, & Amador, 2014). No obstante, como otras normas ISO y sistemas basados en procesos, un método considerado válido y, por lo tanto, recomendable es utilizar como base el modelo PHVA con la finalidad de establecer un proceso de gestión que se enfoque en la mejora continua siguiendo el siguiente esquema:

Planificar

Se establecen los objetivos, procesos y procedimientos para el proceso de gestión de riesgos tecnológico, con el objeto de conseguir unos resultados acordes con las políticas y objetivos globales de la organización.

Hacer

Corresponde a la implementación y operación de los controles, procesos y procedimientos e incluye la operación e implementación de las políticas definidas.

Verificar

Se trata de evaluar y medir el desempeño de los procesos contra la política y los objetivos de seguridad e informar sobre los resultados.

Actuar

Consiste en establecer la política para la gestión de riesgos tecnológicos e implementar los cambios requeridos para la mejora de los procesos (ISOTools, 2015).

2.3.2. MAGERIT V3

Es una metodología de análisis y gestión de riesgos elaborada por el Consejo Superior de Administración Electrónica de España, que ofrece un método sistemático para analizar los riesgos derivados del uso de tecnologías de la información y comunicaciones para de esta forma implementar las medidas de control más adecuadas que permitan tener los riesgos mitigados.

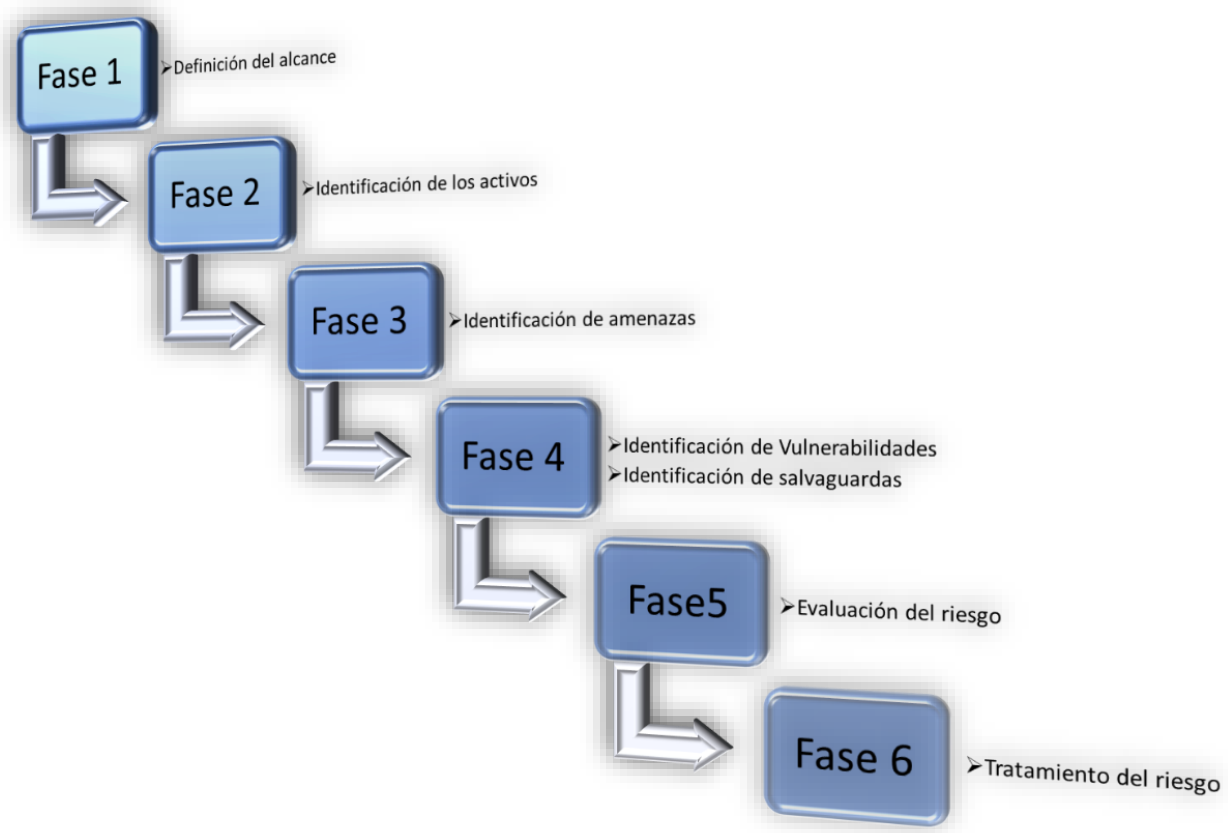
Puntualmente MAGERIT se basa en analizar el impacto que tendría para la empresa la violación de la seguridad, buscandose identificar las amenazas que llegarían a afectar la compañía y las vulnerabilidades que serían utilizadas por estas

amenazas, logrando así tener una identificación clara de las medidas preventivas y correctivas más apropiadas.

Esta metodología es muy útil para aquellas empresas que inicien con la gestión de la seguridad de la información, pues permite enfocar los esfuerzos en los riesgos que resultarían más críticos para una empresa, es decir aquellos relacionados con los sistemas de información. Lo interesante es que al estar alineado con los estándares de ISO es que su implementación se convierte en el punto de partida para una certificación o para mejorar los sistemas de gestión (Gutiérrez Amaya, 2013).

Magerit maneja una forma sencilla para el análisis de riesgos que se encuentran compuestas por seis etapas o fases como se muestra en la **Figura 6** a continuación.

Figura 6. Fase de análisis de riesgos



Fuente: Gestión de riesgo metodologías Octave y Magerit

Fase 1. Definición del alcance

La justificación de un proyecto consiste en una explicación argumentada de las razones que motivan a la realización de este, buscandose responder a la pregunta “¿Por qué?” o “¿Para qué?”, por lo cual es común que se la formule de manera conjunta con los antecedentes del proyecto, (Raffino, 2021).

Dentro de la Cooperativa Oscus, el alcance se encuentra basado específicamente en el personal interno que se encuentra realizando teletrabajo, tanto con los dispositivos que la institución brinda, como con los dispositivos propios que cada uno de ellos cuenta, para poder identificar los diferentes mecanismos de ciberseguridad que llegarían a ser aplicados en los diferentes dispositivos que son utilizados para la realización de teletrabajo por parte del personal interno de la institución.

Fase 2. Identificación de los activos

Los activos son todos los elementos que una organización posee para el tratamiento de la información (hardware, software, recurso humano, entre otros.). Es importante tener en cuenta que los activos se deben agrupar en varios tipos de acuerdo con la función que ejercen en el tratamiento de la información (Tapeiro Tapeiro & Suarez Ramirez, 2017).

La Cooperativa Oscus cuenta con diferentes activos que son importantes para el desarrollo de sus labores diarias, tales como:

- **Hardware (Equipos Informáticos)**

La herramienta principal para el desarrollo de teletrabajos son los equipos de cómputo personales, por lo cual, dentro de los 51 dispositivos utilizados para la realización de teletrabajo, la institución hace la entrega de 15 equipos a diferentes usuarios, no cuentan con tantos equipos para entregar a todo el personal, por lo cual el resto de los equipos es decir los 36 restantes pertenecen a los equipos

personales propios de cada usuario, obviamente cumpliendo ciertos requisitos solicitados por parte de la institución para mantener la seguridad de la misma.

Dentro de los dispositivos del personal que realiza teletrabajo se encuentran equipos con diferentes sistemas operativos la mayoría de ellos pertenecen al fabricante que gran parte de usuarios generalmente utilizan el cuál es el sistema operativo Windows, pero dentro de este existen diversas versiones, antiguas y actuales que los usuarios utilizan, cómo se visualiza en la **Tabla 6**, los dispositivos contendrían unas características mínimas para que estos sistemas operativos trabajen de la mejor manera.

Tabla 6. Características mínimas para Sistemas Operativos Windows

Sistemas Operativos Windows	Windows 7		Windows 8		Windows 8.1		Windows 10	
Versión	***x86***	***x64***	***x86***	***x64***	***x86***	***x64***	***x86***	***x64***
Procesador	1GHz	1GHz	1GHz	1GHz	1GHz	1GHz	1 Ghz - sistema en chip (SoC)	1 Ghz - sistema en chip (SoC)
Disco Duro	16 Gb	20 Gb	16 Gb	20 Gb	16 Gb	20 Gb	16 GB	32 GB
Memoria	1 Gb	2 Gb	1 Gb	2 Gb	1 Gb	2 Gb	1 Gb	2 Gb
Resolución	1024 x 768		1024 x 728 px		1024 x 768		800 x 600	
Tarjeta Gráfica	Directx 9 - WDDM 1.0		Directx 9 - WDDM 1.0		Directx 9 - WDDM 1.0		Directx 9 - WDDM 1.0	

Fuente: Soporte Microsoft

De igual manera hay ciertos usuarios, aunque en poca cantidad, utilizan otro tipo de sistemas operativos entre estos se encuentran los más conocidos como Linux en su distribución más utilizada como es Ubuntu y Mac OS como se muestra en la **Tabla 7**, para los cuales de igual manera se necesitan requerimientos mínimos para que estos sistemas operativos trabajen de forma óptima y los usuarios cumplirían con su trabajo sin tener ningún inconveniente.

Tabla 7. Características mínimas para otros Sistemas Operativos

Sistemas Operativos Adicionales	Ubuntu	Mac OS
Versión	***x64***	***x 10.***
Procesador	Doble nucleo 2 GHz	PowerPC G3
Disco Duro	25 Gb	10 Gb
Memoria	2 Gb	2 Gb
Resolución	1024 x 768	--
Tarjeta Gráfica	Directx 9 - WDDM 1.0	Display XDR

Fuente: Soporte Linux – Soporte Apple Mac OS

Dentro de los dispositivos analizados previamente para la realización de teletrabajo, se especifican los siguientes Sistemas Operativos en la **Tabla 8** que se detalla a continuación.

Tabla 8. Cantidad de usuarios por Sistema Operativo

Sistema Operativo	Usuarios
Windows 7	8
Windows 8	4
Windows 8.1	5
Windows 10	31
Ubuntu	1
Mac OS	2
TOTAL EQUIPOS	**51**

Fuente: Cooperativa Oscus

- **Software**

Dentro de un *hardening* generado para el análisis de software especificado para el registro de dispositivos utilizados para teletrabajo como se demuestra en la **Tabla 9** a continuación, se mantiene un control de los equipos y lo que tendría como característica mínima un sistema operativo de Windows 7 o mayor en el caso de los equipos personales de cada usuario, y Windows 10 para los equipos entregados por la institución, adicional la verificación de que cuenten con un antivirus activo, de no tenerlo, la Cooperativa otorga una licencia de antivirus perteneciente a la

institución. Adicional a esto se realiza una revisión de todo el dispositivo por parte del departamento de seguridad para verificar que los aplicativos que se encuentran instalados en el mismo no lleguen a ser maliciosos, si la aplicación analizada pertenece a un proveedor confiable, si es libre o propietario, y de serlo, si éste cuenta con una licencia respectiva para su operatividad.

Tabla 9. Registro de equipos para teletrabajo

REGISTRO DE EQUIPOS PARA TELETRABAJO			
Usuario:			
Oficina:		**Fecha:**	
Cargo:			
EQUIPO DE COMPUTO			
Marca:		**Modelo:**	
Serie:		**Cod. Act.:**	
CARACTERÍSTICAS	**INFORMACIÓN**	**DATOS**	
Sistema Operativo	Proveedor		
	Versión		
	Ultima Actualización		
	Licencia	Si ☐	No ☐
Antivirus	Proveedor		
	Versión		
	Ultima Actualización		
	Licencia	Si ☐	No ☐
Ofimática	Proveedor		
	Versión		
	Licencia	Si ☐	No ☐
Extra 1	Proveedor		
	Versión		
	Licencia	Si ☐	No ☐
Extra 2	Proveedor		
	Versión		
	Licencia	Si ☐	No ☐
Extra 3	Proveedor		
	Versión		
	Licencia	Si ☐	No ☐

Fuente: Elaboración personal

- **Activos de Información**

Para que los usuarios internos que se encuentran realizando teletrabajo cumplan con su labor correctamente, podría acceder a los diferentes aplicativos con los que la cooperativa cuenta como por ejemplo, el sistema financiero *cluster* con sus diferentes derivaciones, en los cuales los usuarios realizan todo el proceso interno de la cooperativa, adicional a estos, el sistema de tarjetas, sistema de *contact center*, entre otros, y dependiendo del área al que el usuario interno pertenezca tiene el acceso correspondiente a los diferentes aplicativos de la institución. Por motivos de información sensible no se especifican los nombres exactos de las diferentes aplicaciones con las que cuenta la institución como se muestra a continuación en la **Tabla 10**, por lo cual únicamente se los describe de una forma genérica.

Tabla 10. Características mínimas para Sistemas Operativos Windows

SISTEMAS INTERNOS	EXPRESADOS
Sistema Financiero cluster	Sistema 1
Sistema Business	Sistema 2
Sistema Process	Sistema 3
Sistema Tarjetas Débito	Sistema 4
Sistema Tarjetas Crédito	Sistema 5
Sistema Contact Center	Sistema 6
Sistema HelpOs	Sistema 7
Sistema SGC	Sistema 8

Fuente: Cooperativa Oscus

- **Infraestructura**

Para que el personal interno realice teletrabajo en los dispositivos ya sean de la institución o sean propios, una vez que se encuentran revisados por el área de seguridad y que cumplan los requerimientos mínimos se procede con la instalación de diferentes herramientas de conexión para sus equipos que se encuentran externamente hacia la institución, dentro de estas se encuentra las herramientas de VPN (*virtual private network*), y Citrix, las cuales son asignadas a los usuarios dependiendo de las licencias que se les otorgue, por lo general a los gerentes, responsables de procesos y personal técnico se les asigna una licencia de VPN, al

resto de usuarios se les asigna una licencia de Citrix. A continuación, en la **Tabla 11** se realiza una descripción de forma genérica los grupos de usuarios que cuentan con una licencia específica para la conexión a los aplicativos de la institución y que les permiten la realización correcta de sus labores cotidianas.

En el caso de que los usuarios necesiten de soporte remoto por algún inconveniente, los técnicos para poder conectarse a los equipos que se encuentran realizando teletrabajo utilizan diferentes herramientas de software para conexión remota tales como, *Zoom, Team Viewer, Microsoft Teams o AnyDesk* los cuales ayudan a los diferentes técnicos a poder tener acceso a los equipos de los usuarios que se encuentran realizando teletrabajo y poder brindarles un soporte adecuado.

Tabla 11. Grupo de usuarios por herramientas

HERRAMIENTA	GRUPO	USUARIOS
VPN	Gerentes de Oficina	5
	Coordinadores de Negocio	2
	Responsables de Procesos	7
	Tecnología	12
CITRIX	Asistentes	4
	Analistas	15
	Operadores	6
TOTAL USUARIOS		***51***

Fuente: Cooperativa Oscus

- **Personas**

Dentro de todo este proceso de teletrabajo, diferentes áreas con usuarios de diferente nivel jerárquico han tenido que limitarse en la realización de su trabajo presencial y han tenido que empezar con la realización de teletrabajo por diferentes razones, para lo cual, cómo se especificó anteriormente dependiendo de la responsabilidad de cada uno de los trabajadores, se les asigna un diferente tipo de licencia para la conexión remota a sus labores, como se muestra a continuación en la **Tabla 12,** se indica una clasificación de los usuarios que contemplan la población de teletrabajadores y la cantidad de cada uno de ellos contemplándose su nivel jerárquico dentro de la institución.

Tabla 12. Nivel jerárquico de usuarios en teletrabajo

Contabilidad		**Seguridad Fisica**	
Responsable de Contabilidad	1	Analista de Seguridad Fisica	1
Contador 1	2	**Subgerencia A.F.**	
Mesa de Servicios		Subgerente Adm. Financiera	1
Analista de Mesa de Servicios	3	**Tarjetas**	
N/A		Gestor de Tarjetas	2
Gerente Oficina Operativa	5	Analista de Tarjetas	3
Asesor Credito	1	Analista Monitoreo y Antifraude	3
Negocios		**Tesorería**	
Coordinadora de Negocios	2	Tesorero	1
Operaciones		Analista de Tesoreria	2
Responsable de Operaciones	1	**TIC**	
Analista de Operaciones	1	Responsable de TIC	1
Asistente de Cartera	2	Adm. Infraestructura	1
Proyectos		Adm. App y Base de Datos	1
PMO	1	Operador de Aplicaciones	1
Quejas y reclamos		Analista Programador	8
Asistente de Quejas y reclamos	1	Asistente de Hardware y Software	1
Seguridad Integral		**TTHH**	
Responsable de seguridad integral	1	Responsable TTHH	1
Analista de Seguridad	1	Analsita de Talento Humano	1
Asistente de Revisoria	1	***TOTAL USUARIOS***	***51***

Fuente: Departamento de TI – Coop. Oscus

- **Servicios**

La Cooperativa Oscus cuenta con dos proveedores para las conexiones de internet y datos los cuales brindan su servicio 24/7 y los cuales permiten que los usuarios que realizan el trabajo accedan a cada uno de los diferentes aplicativos de la institución. Estas conexiones se encuentran en un estado redundante es decir que si una pierde conexión la otra se encuentra funcionando y por ende la disponibilidad será continua. Adicional a esto la institución cuenta con servicios adicionales dependiendo el área o el departamento que desea hacer uso, como por ejemplo la digitalización de documentos por parte del área de cartera, los cuales accederían de forma remota (escritorio remoto) a sus equipos internos de la cooperativa para poder hacer uso de ella, son servicios que no serían consumidos desde equipos externos, de igual manera por ser información sensible únicamente se brinda un modelo y se lo especifica de forma general en representación de ejemplo.

Fase 3. Identificación de amenazas

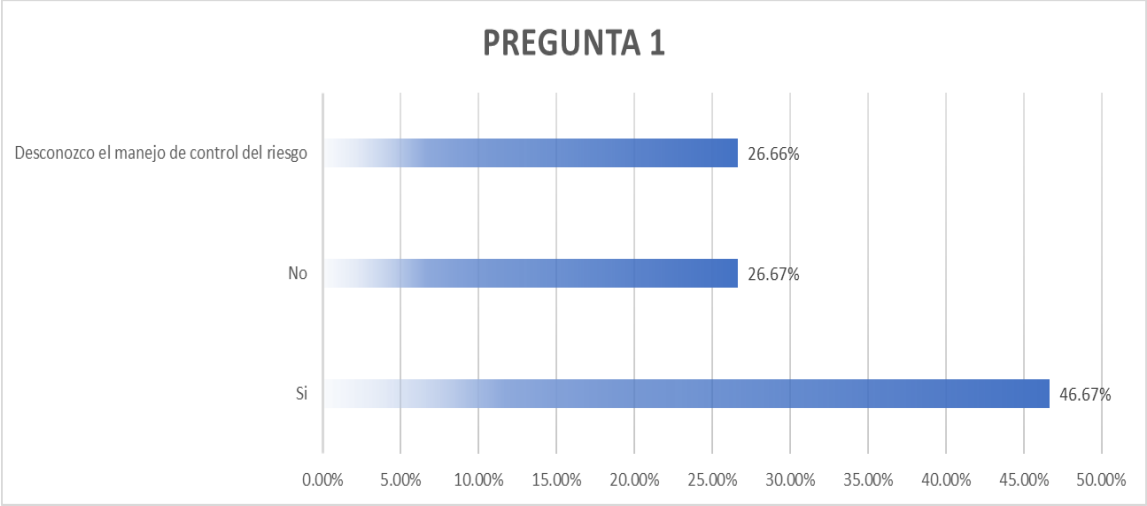
Dicho en palabras de Tapeiro Tapeiro & Suarez Ramirez (2017), las amenazas tienen el potencial de causar daños a los activos tales como información, procesos y sistemas, es decir afecta en gran parte a las instituciones, esto significa que ninguna amenaza se pasa por alto, incluidas las inesperadas. Algunas amenazas afectarían a más de un activo. En tales casos causarían diferentes impactos dependiendo de los activos que se vean afectados.

Una vez aplicada la encuesta se procede con el respectivo análisis de los resultados que cada una de las preguntas arroja, para lo cual mediante la herramienta *QuestionPro,* la misma que permitió la elaboración de la encuesta al personal de la Cooperativa Oscus, y la que permite la generación de resultados para su concerniente análisis, adicionalmente permite la obtención de *dashboards* para un análisis gráfico de los resultados obtenidos. Como se muestra a continuación el análisis de cada una de las preguntas realizadas al personal técnico de la institución.

Concluido el análisis se pudo identificar que el 46.67% de los encuestados creen que la Cooperativa Oscus maneja un control de riesgo adecuado con respecto al personal que realiza teletrabajo, el 26.67% creen que la institución no maneja un control adecuado y el 26.66% desconocen sobre el manejo del control del riesgo dentro de la institución, estos resultados se los muestran en la **Figura 7** a continuación, en donde se realiza el análisis de la primera pregunta de la encuesta que es:

¿Cree usted que la cooperativa Oscus maneja un control de riesgo adecuado con respecto al personal que realiza teletrabajo?

Figura 7. Resultados pregunta 1

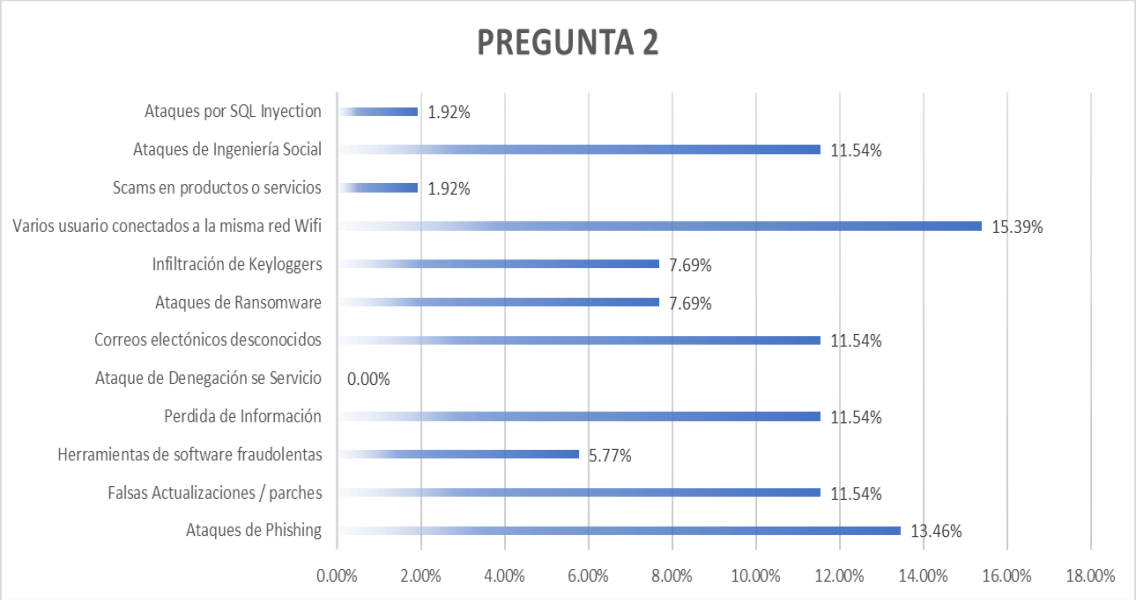


Fuente: elaboración propia

Una vez que se realiza consultas, análisis, y con las encuestas evaluadas, se podría determinar que existe una gran variedad de amenazas que ocurrirían durante la elaboración de teletrabajo, estas amenazas involucra desde ataques de ingeniería social hasta ataques de *phishing* y *ransomware*, los cuales afectan desde el dispositivo del usuario interno que realiza teletrabajo hasta la información o incluso la estructura de la institución financiera, estos ataques costarían información, accesos e incluso pérdidas económicas para la institución que llegue a ser vulnerada y atacada. Estos resultados se los muestran en la **Figura 8** a continuación, en donde se realiza el análisis de la segunda pregunta de la encuesta que es:

De las siguientes opciones ¿Cuál cree usted que es una amenaza al momento de realizar teletrabajo?

Figura 8. Resultados pregunta 2



Fuente: elaboración propia

Como se muestra en la **Tabla 13** a continuación se observa un listado de las principales amenazas que han sido analizadas e identificadas mediante la encuesta y serían las más utilizadas por los atacantes en todo este ámbito de teletrabajo.

Tabla 13. Listado de Amenazas

AMENAZAS
Ataques de Phishing
Falsas Actualizaciones / parches
Herramientas de software fraudolentas
Perdida de Información
Ataque de Denegación se Servicio
Correos electónicos desconocidos
Ataques de Ransomware
Infiltración de Keyloggers
Varios usuario conectados a la misma red Wifi
Scams en productos o servicios
Ataques de Ingeniería Social
Ataques por SQL Inyection

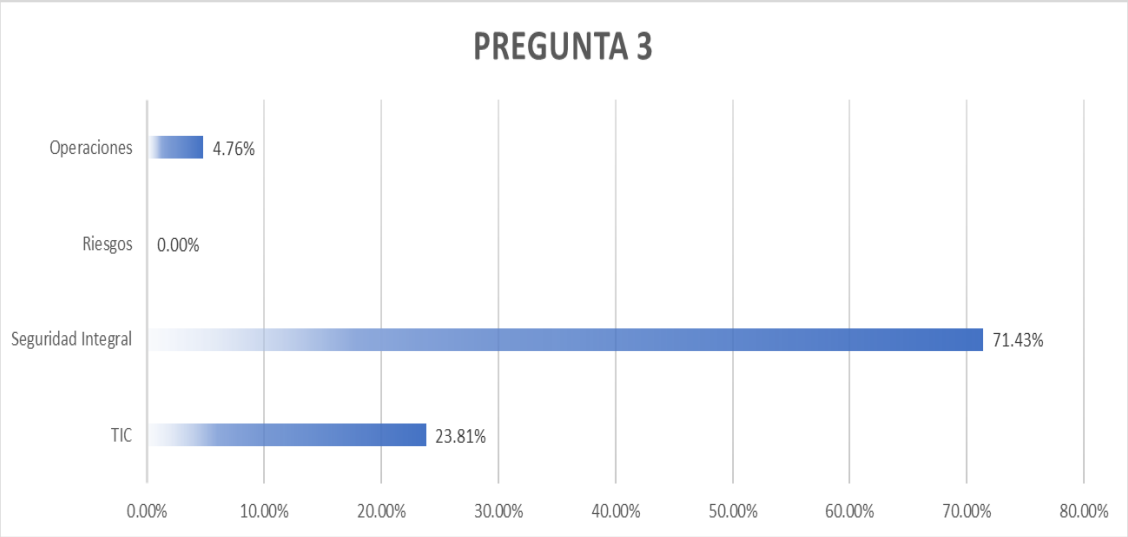
Fuente: elaboración propia

Una vez identificadas las amenazas es idóneo conocer sobre quiénes serían los responsables de brindar una solución en el caso de ocurrir las mismas, para lo cual,

dentro de la encuesta aplicada, el 71.43% de los encuestados indican que Seguridad Integral serían los responsables de dar solución, el 23.81% cree que es el departamento de TIC quienes tendrían que brindar la solución adecuada, y solo el 4.76% de los encuestados indican que sería Operaciones quien de la solución oportuna. Estos resultados se los muestran en la **Figura 9** a continuación, en donde se realiza el análisis de la tercera pregunta de la encuesta que es:

Si la amenaza llegara a ocurrir, ¿Cuál cree usted que sería el departamento que debería dar solución?

Figura 9. Resultados pregunta 3



Fuente: elaboración propia

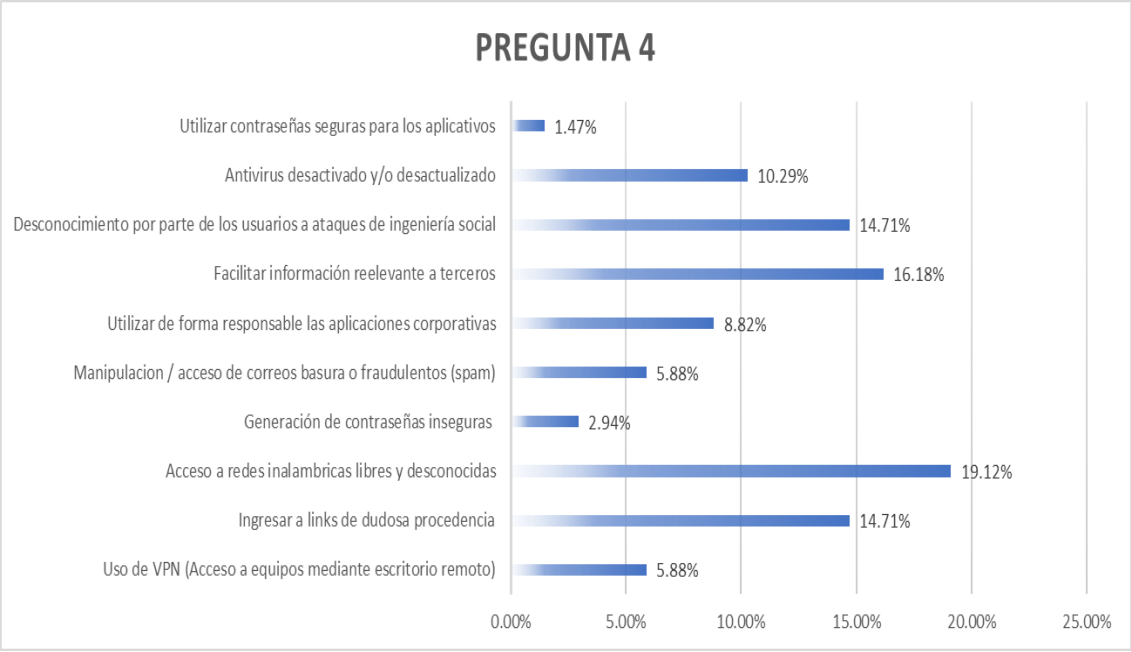
Fase 4. Identificación de Vulnerabilidades / Identificación de salvaguardas

Para iniciar con las vulnerabilidades es importante ya tener identificadas las amenazas y la lista de activos, adicional se identificarían las vulnerabilidades que serían explotadas por las amenazas para causar daños a los activos o la organización, la sola presencia de una vulnerabilidad no causa daño por sí misma, dado que es necesario que haya una amenaza presente para explotarla. Una vulnerabilidad que no tiene una amenaza correspondiente no requeriría de la implementación de un control, pero es recomendable reconocerla y monitorearla para determinar los cambios (Tapeiro Tapeiro & Suarez Ramirez, 2017).

Una vez que se realiza consultas, análisis, y con las encuestas realizadas, se determinaría que existe una gran variedad de vulnerabilidades que estarían presentes durante la elaboración de teletrabajo, estas vulnerabilidades involucra desde antivirus desactivados o desactualizados, hasta el uso de forma irresponsable de las aplicaciones corporativas, los cuales afectan desde el dispositivo del usuario interno que realiza el trabajo, hasta poner en riesgo la infraestructura, la información y varios complementos adicionales de la institución, para lo cual se tendría presente que como institución se estaría un paso adelante para tratar de mitigar las vulnerabilidades y no ser víctimas de ciberataques. Estos resultados se los muestran en la **Figura 10** a continuación, en donde se realiza el análisis de la siguiente pregunta de la encuesta que es:

Al momento de realizar teletrabajo ¿Cuál cree usted que es la o las vulnerabilidades que pueden generar un mayor riesgo tanto para los dispositivos de teletrabajo como para la Institución?

Figura 10. Resultados pregunta 4



Fuente: elaboración propia

Como se muestra en la **Tabla 14** a continuación podemos observar un listado de las principales vulnerabilidades que han sido encontradas e identificadas, además serían las de mayor impacto en todo este tema del teletrabajo.

Tabla 14. Listado de Vulnerabilidades

VULNERABILIDAES
Uso de VPN (Acceso a equipos mediante escritorio remoto)
Ingresar a links de dudosa procedencia
Acceso a redes inalambricas libres y desconocidas
Generación de contraseñas inseguras
Manipulacion / acceso de correos basura o fraudulentos (spam)
Utilizar de forma responsable las aplicaciones corporativas
Facilitar información reelevante a terceros
Desconocimiento por parte de los usuarios a ataques de ingeniería social
Antivirus desactivado y/o desactualizado
Utilizar contraseñas seguras para los aplicativos

Fuente: elaboración propia

Fase5. Evaluación del riesgo

Una vez obtenidos resultados en las fases anteriores, se identificaría que ya se cuenta con una cierta cantidad de información para realizar el proceso de evaluación del riesgo, el cual se encarga de ordenar los riesgos generados y analizados por la prioridad de acuerdo con diferentes criterios de evaluación del riesgo, obviamente basados en un análisis que contemple identificaciones mediante la norma ISO/IEC 27005.

La evaluación de riesgos se representa a partir de los riesgos identificados mediante las amenazas y vulnerabilidades encontradas en las fases anteriores, para las cuales se les asigna un valor según el impacto y la probabilidad de ocurrencia del riesgo, y de esta manera, determinar el riesgo inherente y controlado. Con este análisis, se podrá calcular el estado del riesgo al realizar teletrabajo cumpliendo con los requisitos de los mecanismos necesarios para la realización de este.

La evaluación del riesgo cumpliría con tres fases para poder especificar que la evaluación se cumple correctamente:

Entrada. - lista de los riesgos con los niveles de valores y criterios para la evaluación del riesgo.

Acción. - comparación del nivel del riesgo con los criterios de evaluación.

Salida. - lista de riesgos ordenados por priorización, de acuerdo con los criterios de evaluación del riesgo.

La especificación de estas fases se las describe en la **Figura 11** a continuación.

Figura 11. Evaluación del riesgo

Fuente: Escuela Superior de Redes – Red CEDIA

En esta fase el departamento encargado tomaría decisiones con respecto al nivel del riesgo aceptable, por lo cual también es importante considerar los siguientes términos:

- Se deben mantener activas las propiedades de confidencialidad, integridad y disponibilidad, si alguna de estas no es tan relevante se consideraría con un valor bajo y por tal motivo ser considerada como un riesgo aceptable.
- Entender también la importancia de que, si un proceso o actividad es valorado como de importancia baja, los riesgos asociados a este deben ser también tenidos en cuenta de una manera menor que los riesgos que causarán impactos mayores en procesos importantes (Kowask Bezerra, Alcántara Lima, Motta, & Boca Piccolini, 2014).

Una vez realizados los respectivos análisis, se llega a identificar los diferentes riesgos que se encontrarían asociados directamente con la realización de teletrabajo, cómo se determina en la **Tabla 15** la descripción de cada uno de los riesgos evaluados con un código respectivo, el cual será utilizado posteriormente para futuras evaluaciones y análisis.

Tabla 15. Identificación de Riesgos en Teletrabajo

CODIGO	RIESGO
Risk 001	Alteración o pérdida de información debido a los respectivos accesos a la misma
Risk 002	Falta de controles de seguridad en la ejecución de aplicaciones involucra que los dispositivos ejecuten aplicaciones sin validaciones
Risk 003	Usuarios vulnerables a realización de ingeniería social, involucrando la seguridad de la institución.
Risk 004	Contraseñas débiles que pueden ser identificadas facilmente
Risk 005	Ciberataques que involucra la indisponibilidad de la información y servicios debido a inconvenientes con el proveedor de internet
Risk 006	Falta de control en correos electrónicas, ocasionando ataques de phishing
Risk 007	Las funciones antivirus obsoletas causan inconvenientes en la seguridad de la información e infraestructura de la institución
Risk 008	El impacto de la presencia de malware en los dispositivos utilizados para teletrabajo
Risk 009	La falta de convenios confidenciales, entre la institución y los usuarios internos, lo cual genera que la información confidencial de la institución sea sustraída o alterada.

Fuente: elaboración propia

Según AppSec (2021), en esta etapa se deben tomar en cuenta varios factores como las probabilidades, los impactos y las vulnerabilidades que permitan la

evaluación de las características de cada riesgo, los cuales serían tomados en cuenta para el cálculo del riesgo en las pruebas realizadas, en cada uno de los factores se identifica lo siguiente:

- **Factor Probabilístico**
  - Habilidades Requeridas. – si es indispensable alguna habilidad para poder descubrir alguna posible vulnerabilidad.
  - Motivo. – si la información que se encuentra llega a ser de gran importancia.
  - Oportunidad. – si para acceder a la información sobre alguna vulnerabilidad existente, se requiere de algún tipo de permiso.
  - Tamaño de la Población. – los usuarios que podrían llegar a ser afectados ante una posible amenaza.

- **Factor Vulnerable**
  - Fácil de Descubrir. – es el nivel de dificultad que se llegaría a tener para poder descubrir una vulnerabilidad.
  - Fácil de Explotar. – es el nivel de dificultad que se llegaría a tener para poder explotar una vulnerabilidad.
  - Conciencia. – identificar si la vulnerabilidad encontrada es visual o no.
  - Detección de Intrusos. – si existe la posibilidad de detectar un ataque debido a una vulnerabilidad.

- **Factor Impacto Técnico**
  - Perdida de Confidencialidad. – si el impacto de una posible vulnerabilidad determinará una posible pérdida de la confidencialidad de la información, hacia el usuario.
  - Perdida de Integridad. – si la pérdida o alteración de la información es a causa de una posible vulnerabilidad existente.
  - Perdida de Disponibilidad. – si la información se podrá perder y no tener acceso a la misma ante una posible vulnerabilidad conocida.

Es fundamental tomar en cuenta los factores indicados, permiten determinar el grado de vulnerabilidad, de esto dependerá de que un problema llegue a ser solucionado correctamente, con la finalidad de mantenerse libre o más seguros en el caso de recibir un ciberataque.

En el análisis a los factores de riesgo indicados anteriormente, se considera la estimación del posible riesgo a suscitarse en la realización de teletrabajo, en la cual se evalúa la probabilidad de ocurrencia del riesgo y el impacto de las consecuencias para la respectiva obtención de información para poder establecer el nivel de riesgo respectivo, la respectiva prioridad del riesgo y las estrategias para su tratamiento.

Por lo tanto, para esta fase en la cual se pretende evaluar las medidas correctivas en la realización de teletrabajo se realizaría un cálculo del impacto **Tabla 16** y de la probabilidad **Tabla 17**, los cuales se encuentran relacionados directamente con el riesgo, para lo cual se ha tomado los siguientes criterios.

Tabla 16. Cálculo del Impacto

Impacto		
Rango	**Descripción**	**Cuantitativo**
Bajo	El daño ocasionado por los ciberataques tiene consecuencias relevantes para la institución	1
Medio	El daño ocasionado por los ciberataques tiene consecuencias considerables para la institución	2
Alto	El daño ocasionado por los ciberataques tiene consecuencias graves para la institución	3

Fuente: elaboración propia

Tabla 17. Cálculo de la Probabilidad

Probabilidad		
Rango	**Descripción**	**Cuantitativo**
Ocasional	La institución casi nunca sufre de ciberataques a nivel de dispositivos que realizan teletrabajo	1
Probable	La institución sufre periódicamente de ciberataques a nivel de dispositivos que realizan teletrabajo	2
Frecuente	La institución sufre constantemente de ciberataques a nivel de dispositivos que realizan teletrabajo	3

Fuente: elaboración propia

Para poder identificar el nivel de probabilidad e impacto es necesario determinar niveles de gravedad en cada uno de los riesgos por lo cual se especifica en la **Tabla 18** valores con los cuales se procederá a realizar un análisis para identificar la criticidad de los riesgos detallados anteriormente.

Tabla 18. Nivel de gravedad del riesgo

Nivel de Impacto y Probabilidad	
0 a <3	Bajo
3 a <6	Medio
6 a 9	Alto

Fuente: elaboración propia

Para poder realizar la evaluación del riesgo, se procede a generar una matriz de valoración del riesgo como se muestra en la **Tabla 19** a continuación, en la cual se especifica desde el impacto y probabilidad más baja el cual no causaría efecto, hasta el más alto, el cual conlleva varios análisis para poder solventar y evitar cualquier incidente dentro de la institución.

Tabla 19. Evaluación de riesgo

Evaluación del Riesgo				
PROBABILIDAD	Ocasional	Bajo	Bajo	Moderado
	Probable	Bajo	Moderado	Alto
	Frecuente	Moderado	Alto	Alto
		Bajo	Medio	Alto
		IMPACTO		

Fuente: elaboración propia

Una vez especificada la base de niveles de gravedad y la evaluación del riesgo, se procede a realizar una valoración de cada uno de los riesgos identificados para valorar la criticidad con relación a la probabilidad y el impacto que cada uno de estos llegaría a tener con historial y experiencia generada por parte de

responsables de diferentes áreas de la institución financiera, como se determinan a continuación.

Risk 001 (*Alteración o pérdida de información debido a los respectivos accesos a la misma)* **Tabla 20**. Se detalla un valor alto al riesgo, ya qué debido a que es una institución financiera, la modificación y más aún la pérdida de la información es uno de los activos más importantes para esta institución, siendo una probabilidad media, pero de alto impacto, su riesgo obviamente se convierte en un riesgo alto para la institución.

Tabla 20. Evaluación de riesgo – Risk 001

Evaluación del Riesgo				
PROBABILIDAD	Ocasional (1)			
	Probable (2)			6 - Alto
	Frecuente (3)			
		Bajo (1)	Medio (2)	Alto (3)
		IMPACTO		

Fuente: elaboración propia

Risk 002 *(Falta de controles de seguridad en la ejecución de aplicaciones involucra que los dispositivos ejecuten aplicaciones sin validaciones)* **Tabla 21.** En el caso de la ejecución de aplicaciones que no son autorizadas por la institución, los equipos internos mantienen controles de solicitud de credenciales de administrador para la ejecución de los mismos, pero en el caso de los equipos personales de los usuarios, el control no existe, por lo que hay la probabilidad de que estas aplicaciones vengan de sitios fraudulentos, por lo cual, se la valora con una probabilidad media y un impacto de igual manera medio, existen otros controles de seguridad, por tal razón la valoración del riesgo es moderada.

Tabla 21. Evaluación de riesgo - Risk 002

Evaluación del Riesgo				
PROBABILIDAD	Ocasional (1)			
	Probable (2)		4 - Moderado	
	Frecuente (3)			
		Bajo (1)	Medio (2)	Alto (3)
		IMPACTO		

Fuente: elaboración propia

Risk 003 *(Usuarios vulnerables a realización de ingeniería social, involucrando la seguridad de la institución)* **Tabla 22.** Como es de conocimiento, la ingeniería social llega a ser aplicada a todo tipo de usuario, y éste se vuelve más vulnerable si desconoce del tema, en el caso del teletrabajo los usuarios no mantienen una relación directa con el personal técnico que les guie y serían víctimas más fácilmente, por tal razón se identifica que hay una probabilidad baja de que este ciberataque ocurra, pero en el caso de suceder el impacto sería alto, es por eso que el evento de riesgo en este caso es considerado moderado.

Tabla 22. Evaluación de riesgo - Risk 003

Evaluación del Riesgo				
PROBABILIDAD	Ocasional (1)			3 - Moderado
	Probable (2)			
	Frecuente (3)			
		Bajo (1)	Medio (2)	Alto (3)
		IMPACTO		

Fuente: elaboración propia

Risk 004 *(Contraseñas débiles que pueden ser identificadas fácilmente)* **Tabla 23.** Se identifica que gran parte de los usuarios mantienen contraseñas con fechas o datos continuos lo cual en un ambiente de teletrabajo en donde existe menos control de seguridad que al estar dentro de la institución, y este inconveniente se lo lleva desde tiempo atrás, incluso después de haber recibido charlas e indicado los

riesgos que esto conlleva, por tal razón se conoce que al tener contraseñas débiles el impacto de ser atacados es muy alto, por estos motivos el riesgo en esta evaluación es de grado alto.

Tabla 23. Evaluación de riesgo - Risk 004

Evaluación del Riesgo				
PROBABILIDAD	Ocasional (1)			
	Probable (2)			
	Frecuente (3)		6 - Alto	
		Bajo (1)	Medio (2)	Alto (3)
		IMPACTO		

Fuente: elaboración propia

Risk 005 *(Ciberataques que involucra la indisponibilidad de la información y servicios debido a inconvenientes con el proveedor de internet)* **Tabla 24.** En muchos de los casos la falta de disponibilidad de la información no siempre es falla de la institución, para motivos de comunicación estas dependen de un proveedor de comunicación ya sea de datos o de internet, y en el caso de un ataque a un proveedor, la institución sufriría las consecuencias, por un lado podría perder la comunicación y por otro ser vulnerable a algún ciberataque que venga relacionado con las conexiones hacia un proveedor externo, es por ello que estos casos serían frecuentes porque no se conoce de la seguridad interna del proveedor, por lo cual se convierte en una probabilidad alta y de igual manera en el caso de caer en un ciberataque el impacto sería alto, por esa razón se considera un riesgo alto.

Tabla 24. Evaluación de riesgo - Risk 005

Evaluación del Riesgo				
PROBABILIDAD	Ocasional (1)			
	Probable (2)			6 - Alto
	Frecuente (3)			
		Bajo (1)	Medio (2)	Alto (3)
		IMPACTO		

Fuente: elaboración propia

Risk 006 *(Falta de control en correos electrónicos, ocasionando ataques de phishing)* **Tabla 25.** En muchos de los casos por cuestiones de desconocimiento al abrir un correo electrónico que no se conoce al remitente, por curiosidad se lo abre y en el peor de los casos se accede a una imagen o link que éste contenga el cual estaría realizandose un ciberataque de phishing por medio del correo personal, esto sucede frecuentemente debido a que a los correos los escribirían desde cualquier dirección externa y en el momento de que estos explotan existe un gran impacto de qué, tanto el equipo personal como la infraestructura de la institución llegue a ser vulnerada y atacada, por esta razón el riesgo indicado es valorado como alto.

Tabla 25. Evaluación de riesgo - Risk 006

Evaluación del Riesgo				
PROBABILIDAD	Ocasional (1)			
	Probable (2)			
	Frecuente (3)			9 - Alto
		Bajo (1)	Medio (2)	Alto (3)
		IMPACTO		

Fuente: elaboración propia

Risk 007 *(Las funciones antivirus obsoletas causan inconvenientes en la seguridad de la información e infraestructura de la institución)* **Tabla 26.** Así como los virus y sus derivados se actualizan diariamente, de igual manera la institución hace lo mismo con su seguridad, actualizando sus versiones de antivirus y otros; pero esto no significa que no podrían llegar a ser infectados, por tal razón la protección es siempre continua y el impacto que hasta el momento se ha mantenido ha sido bajo, por ende, la evaluación del riesgo se lo identifica un valor bajo.

Tabla 26. Evaluación de riesgo - Risk 007

Evaluación del Riesgo				
PROBABILIDAD	Ocasional (1)			
	Probable (2)	2 - Bajo		
	Frecuente (3)			
		Bajo (1)	Medio (2)	Alto (3)
		IMPACTO		

Fuente: elaboración propia

Risk 008 *(El impacto de la presencia de malware en los dispositivos utilizados para teletrabajo)* **Tabla 27.** Al igual que los virus, los malware también se modifican y actualizan constantemente la diferencia de éstos es que son más peligrosos que los mismos virus, por ende la institución mantendría sus protocolos de seguridad tanto para los equipos internos y mucho más para los equipos que van a realizar teletrabajo, estos van a estar más vulnerables a cualquiera de estas infecciones que desembocarían en ciberataques, por tal razón hay una probabilidad media de qué los dispositivos que realizan teletrabajo se infecten y el impacto sería alto debido a qué mediante conexiones VPN el equipo podría tener acceso remotamente a la infraestructura de la institución lo que lo convierte en un riesgo alto.

Tabla 27. Evaluación de riesgo - Risk 008

Evaluación del Riesgo				
PROBABILIDAD	Ocasional (1)			
	Probable (2)			6 - Alto
	Frecuente (3)			
		Bajo (1)	Medio (2)	Alto (3)
		IMPACTO		

Fuente: elaboración propia

Risk 009 *(La falta de convenios confidenciales, entre la institución y los usuarios internos, lo cual genera que la información confidencial de la institución sea sustraída o alterada)* **Tabla 28.** El personal que realiza teletrabajo siente que se encuentra laborando dentro de la institución por los accesos que éste tiene pero al igual que en los riesgos anteriores existe una probabilidad media de que la información a la que éstos tienen acceso llegue a ser manipulada, alterada o eliminada por algún ciber atacante, no toman las medidas adecuadas por falta de instrucción sobre el correcto manejo de la confidencialidad de la información al momento de realizar teletrabajo, lo cual indica mantener un impacto alto de la manipulación de la información, conllevándolo hacer un riesgo alto para la institución.

Tabla 28. Evaluación de riesgo - Risk 009

Evaluación del Riesgo				
PROBABILIDAD	Ocasional (1)			
	Probable (2)			6 - Alto
	Frecuente (3)			
		Bajo (1)	Medio (2)	Alto (3)
		IMPACTO		

Fuente: elaboración propia

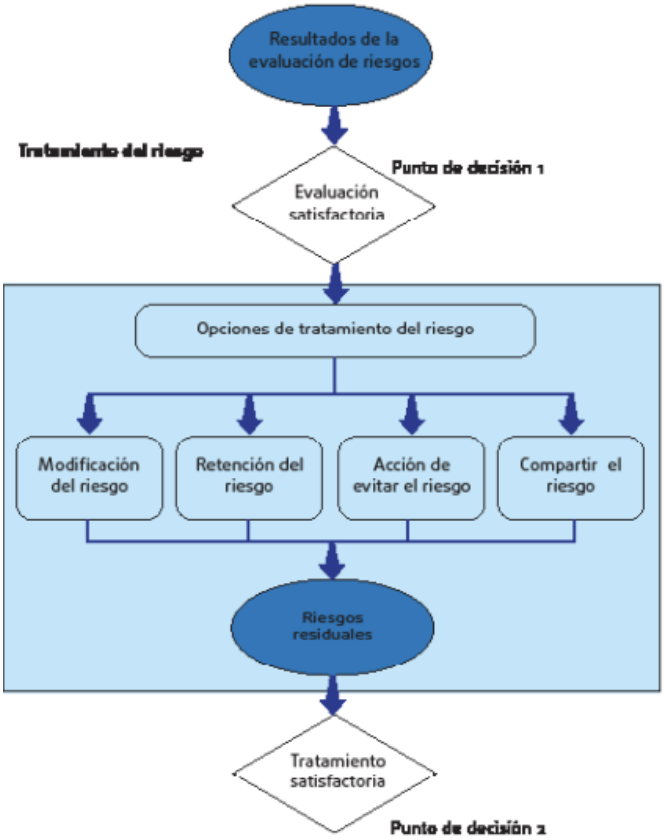
Fase 6. Tratamiento del riesgo

Según lo indicado por Kowask Bezerra, Alcántara Lima, Motta, & Boca Piccolini (2014), el tratamiento del riesgo se utiliza para responder a los riesgos identificados. Hay diferentes opciones para tratar y responder al riesgo. Las elecciones y decisiones tomadas tendrían en cuenta lo siguiente:

- La evaluación del tratamiento del riesgo propuesto ya realizado.
- La viabilidad técnica y financiera, es decir, los costos de implementación del control.
- La eficacia de los controles.
- La eficacia del tratamiento.
- Decisión si los niveles del riesgo residual son tolerables.
- Las características del negocio de la organización (viabilidad económica).

En la **Figura 12** indicada a continuación, se especifican las actividades que se realizan en proceso para el tratamiento del riesgo.

Figura 12. Actividades para tratamiento del riesgo



Fuente: Escuela Superior de Redes – Red CEDIA

Para poder iniciar con el tratamiento del riesgo, primeramente, es necesario tener detectados claramente los activos que la institución posee y que se encuentran involucrados, también las amenazas que se podrían detectar los cuales como su palabra lo indica, serían amenazas con respecto a la realización de teletrabajo por parte del personal interno, y además las vulnerabilidades a las cuales se hallarían involucrados los dispositivos que se encuentran en la realización de teletrabajo, esta información se encuentra indicada en la **Tabla 29** a continuación.

Tabla 29. Actividades para tratamiento del riesgo

ACTIVOS	AMENAZAS	VULNERABILIDADES
Hardware (equipos Informáticos)	Varios usuario conectados a la misma red Wifi	Acceso a redes inalambricas libres y desconocidas
Software	Ataques de Phishing	Facilitar información reelevante a terceros
Activos de información	Falsas Actualizaciones / parches	Ingresar a links de dudosa procedencia
Infraestructura	Perdida de Información	Desconocimiento por parte de los usuarios a ataques de ingeniería social
Personas	Correos electónicos desconocidos	Antivirus desactivado y/o desactualizado
Servicios	Ataques de Ingeniería Social	Utilizar de forma responsable las aplicaciones corporativas
	Ataques de Ransomware	Uso de VPN (Acceso a equipos mediante escritorio remoto)
	Infiltración de Keyloggers	Manipulacion / acceso de correos basura o fraudulentos (spam)
	Herramientas de software fraudolentas	Generación de contraseñas inseguras
		Utilizar contraseñas seguras para los aplicativos

Fuente: elaboración propia

Una vez que se encuentran especificados los riesgos en la fase anterior, se procede con el análisis para poder brindar la respectiva solución y/o su correcto tratamiento para poder evitar o mitigar que estos riesgos sucedan, y en el caso de ocurrir, que no se conviertan en eventos repetitivos dentro de la institución y sobre todo controlar con estos mecanismos que los dispositivos que realizan teletrabajo se vean afectados, para lo cual se realiza una matriz en donde se procede a involucrar los mecanismos de ciberseguridad con cada uno de los riesgos como se muestra en la **Tabla 30,** para verificar cual mecanismo es el óptimo para el control de cada uno de los riesgos identificados.

Tabla 30. Herramientas para tratamiento del riesgo

Mecanismos de ciberseguridad disponibles para la seguridad en una institución financiera asociado al teletrabajo	RIESGOS ENCONTRADOS ENTELETRABAJO								
	Risk 001	Risk 002	Risk 003	Risk 004	Risk 005	Risk 006	Risk 007	Risk 008	Risk 009
Antivirus / antimalware		x				x	x	x	
Firewall / equipo perimetral			x		x	x	x	x	
Control de acceso	x	x		x		x			x
Cifrado de datos	x		x	x			x	x	x
Respaldo Información	x	x	x	x	x		x		x
Redes privadas virtuales	x		x		x				
Filtrado de contenido				x		x		x	x
IPS					x		x		

Fuente: elaboración propia

Al momento de que la institución financiera decide que su personal elabore teletrabajo, se dan cuenta de que van a estar sometidos a un mayor riesgo, entienden que los dispositivos de trabajo no van a poder ser controlados de la misma manera como si los equipos se encontrarán dentro de la institución, por tal motivo se trata de dar la mayor seguridad a los dispositivos que realizarán teletrabajo para poder evitar los diferentes tipos de riesgos que se analizaron anteriormente y mantener a la institución segura de cualquier ciberataque a la que ésta llegue a someterse. Por ende, a continuación, se especifica una guía de buenas prácticas para poder mitigar el riesgo al que se sometería la institución financiera por mantener usuarios internos y dispositivos tanto pertenecientes de la institución como propios a cada uno de los usuarios por el motivo de realizar teletrabajo.

Guía de buenas prácticas para mitigación del riesgo.

Para poder solventar o mitigar cada uno de los riesgos definidos, se aplicarían diferentes tipos de mecanismos de ciberseguridad que permitan ayudar al control adecuado para que la institución financiera no sea víctima de ciberataques, y en el caso de serlo, saber cómo actuar y que mecanismos aplicar para no encontrarse vulnerable ante las amenazas que día a día se presentan y que se estaría preparado para mitigar los ciberataques a los que se podría estar expuesto. Por lo cual se procede a generar una guía de buenas prácticas para la mitigación de los distintos riesgos identificados dentro de la Cooperativa de Ahorro y Crédito Oscus Ltda.

El objetivo de esta guía de buenas prácticas es describir y exponer lo siguiente:

- Apoyar a la institución financiera con recomendaciones para mantener un mejor control de seguridad frente a los dispositivos que realizan teletrabajo.
- Brindar al usuario administrador, una guía para mantener parámetros de seguridad internos dentro de la institución.

- Proponer diferentes tipos de mecanismos de ciberseguridad que se aplicarían dependiendo el tipo de riesgo identificado referente a los dispositivos que realizan teletrabajo.

Los beneficios al momento de aplicar la guía de buenas prácticas para la institución son:

- La institución llegaría a tener un mayor control de los dispositivos que se encuentran realizando teletrabajo.
- Brindar al usuario interno que se encuentra realizando teletrabajo, mayor seguridad sabiendo que la institución cuenta con las medidas adecuadas para no correr el riesgo de ser víctimas de un ciberataque.
- Permitir que la información de la institución cumpla con la triada de seguridad, confidencialidad, integridad y sobre todo disponibilidad de esta.
- Minimizar el riesgo de ser víctimas de un ciberataque ya sea este por el mal uso de los dispositivos o la falta de control en los mismos.

Durante todo un proceso de análisis incluyendo encuestas se pudo determinar diferentes tipos de riesgos a los que los usuarios internos que realizan teletrabajo estarían expuestos y ser vulnerables a un ciberataque, por tal razón para poder generar una guía de buenas prácticas para el control y mitigación de estos riesgos se procede con recomendaciones para la aplicación de diferentes mecanismos de ciberseguridad disponibles para mantener la seguridad tanto en la institución como los dispositivos que realizan teletrabajo.

A continuación, en la **Tabla 31,** se describen los riesgos identificados existentes al momento de realizar teletrabajo los cuales se encuentran especificados por un código que será utilizado durante el proceso de toda esta guía de buenas prácticas,

Tabla 31. Identificación de Riesgos en Teletrabajo

CODIGO	RIESGO
Risk 001	Alteración o pérdida de información debido a los respectivos accesos a la misma
Risk 002	Falta de controles de seguridad en la ejecución de aplicaciones involucra que los dispositivos ejecuten aplicaciones sin validaciones
Risk 003	Usuarios vulnerables a realización de ingeniería social, involucrando la seguridad de la institución.
Risk 004	Contraseñas débiles que pueden ser identificadas facilmente
Risk 005	Ciberataques que involucra la indisponibilidad de la información y servicios debido a inconvenientes con el proveedor de internet
Risk 006	Falta de control en correos electrónicas, ocasionando ataques de phishing
Risk 007	Las funciones antivirus obsoletas causan inconvenientes en la seguridad de la información e infraestructura de la institución
Risk 008	El impacto de la presencia de malware en los dispositivos utilizados para teletrabajo
Risk 009	La falta de convenios confidenciales, entre la institución y los usuarios internos, lo cual genera que la información confidencial de la institución sea sustraída o alterada.

Fuente: elaboración propia

Una vez que los riesgos fueron identificados se procedió con un análisis de diferentes mecanismos de ciberseguridad que podrían ser aplicados para la mitigación de estos, y poder controlar con estos mecanismos que los dispositivos que realizan teletrabajo no se vean afectados, en la **Tabla 30** se realiza una matriz para verificar cual mecanismo es el óptimo para el control de cada uno de los riesgos identificados

Para cada uno de los mecanismos de ciberseguridad especificados anteriormente, se procede a identificar con una simbología gráfica, la cual será utilizada durante toda la guía de buenas prácticas, esta se muestra en la **Tabla 32** a continuación.

Tabla 32. Herramientas para tratamiento del riesgo

Mecanismos de ciberseguridad disponibles para la seguridad en una institución financiera asociado al teletrabajo	*Simbología*
Antivirus / antimalware	
Firewall / equipo perimetral	
Control de acceso	
Cifrado de datos	
Respaldo Información	
Redes privadas virtuales	
Filtrado de contenido	
IPS	

Fuente: elaboración propia

Aplicación de mecanismos de ciberseguridad dependiendo el tipo de riesgo identificado.

Risk 001 (*Alteración o pérdida de información debido a los respectivos accesos a la misma)*

Debido a que este riesgo es considerado como alto se aplicaría varios mecanismos que ayuden a mitigar los ciberataques en los dispositivos que se encuentren realizando teletrabajo, como los equipos pueden encontrarse vulnerables, existe la probabilidad de que estos lleguen a ser víctimas de manipulación de la información debido a accesos no autorizados, por tal razón los mecanismos identificados que ayudarían a que este riesgo disminuya son los siguientes si se identifican en la **Tabla 33**:

- **Control de acceso:** controlando el acceso a la información a los usuarios de acuerdo con sus respectivos roles, se evita de que éstos alteren o eliminen información que no les compete, este control se lo realizaría tanto directamente en los aplicativos de la institución como en los usuarios del directorio activo.

- **Cifrado de datos:** si se trabaja con datos fuera de la institución estos deberían encontrarse cifrados para que un tercero no logre identificar la información correcta, el usuario podría ser víctima de un ciberataque y poner vulnerable la información de la institución.
-
- **Respaldo de información:** en el caso de que se identifique que la información llegó a ser manipulada, alterada incorrectamente o por usuarios sin privilegios, se contaría con respaldos continuos para reemplazar la información incorrecta, esto ayudará que la información este siempre actualizada correctamente.
-
- **VPN:** el uso de redes privadas virtuales, a diferencia de otros mecanismos de conexión remota, es mucho más seguro, su información internamente navega encriptada, llevándolo a un mayor control de la información que se maneja.

Tabla 33. Mecanismos de ciberseguridad – Risk 001

Risk001			
			

Fuente: elaboración propia

Risk 002 ***(Falta de controles de seguridad en la ejecución de aplicaciones involucra que los dispositivos ejecuten aplicaciones sin validaciones)***

Este riesgo es considerado moderado, los dispositivos que se encuentran realizando teletrabajo y pertenecen directamente al usuario interno no tienen un control de protección de ejecución de aplicativos los cuales internamente en la institución son validados por credenciales de administración, como se encuentran en teletrabajo y son dispositivos con una cierta libertad tanto de navegación como de seguridad, por tal razón los mecanismos identificados que ayudarían a que este riesgo disminuya son los siguientes si se identifican en la **Tabla 34**:

- **Antivirus / Antimalware:** como los dispositivos se encuentran en trabajo necesitan un mayor control de seguridad, por ende, el uso adecuado de un antivirus o antimalware que se encuentra actualizado y de ser el caso con licencia original aporta en gran parte a la protección de los dispositivos.
-
- **Control de Acceso:** si el dispositivo llegar a ser comprometido hay que tener en cuenta que la principal vulnerabilidad sería el activo de la información, por tal razón el control de acceso a la información adecuada estaría bien configurado ya sea por parte del departamento de tecnología o de seguridad.
-
- **Respaldo de Información:** en toda institución es necesario tener respaldos de toda la información que se maneja, mucho más si ésta se refiere a una institución financiera que maneja información tanto personal como económica de los socios y clientes, por tal motivo al momento de ser sometido a un ciberataque y haber sido vulnerado mantener respaldos es un arma que permite retomar los servicios.

Tabla 34. Mecanismos de ciberseguridad – Risk 002

Risk 002		
		

Fuente: elaboración propia

Risk 003 *(Usuarios vulnerables a realización de ingeniería social, involucrando la seguridad de la institución*).

Este riesgo es considerado como moderado, se podría dar el caso de que los usuarios internos de la institución que se encuentran realizando teletrabajo sean víctimas de ingeniería social y comprometer ya sea información o credenciales de acceso a los diferentes sistemas de la institución, por tal razón los mecanismos identificados que ayudarían a que este riesgo disminuya son los siguientes si se identifican en la **Tabla 35**:

- **Firewall:** un mecanismo de seguridad para control de este tipo de riesgo sería un *firewall,* los permisos son otorgados a usuarios relacionado a un dispositivo, si un usuario indicado tiene acceso, pero el dispositivo no se encuentra en el listado de permisos otorgados, el acceso es interrumpido, adicional a esto existe un monitoreo constante de accesos no autorizados para tener un adecuado control.
-
- **Cifrado de datos:** esta es la base principal de la seguridad de datos, es decir, que este mecanismo es importante para garantizar que la información de la institución no sea sustraída, leída o utilizada por alguien que no tenga los accesos o permisos suficientes.
-
- **Respaldo de Información:** como en los casos anteriores en el caso de ser vulnerado la mejor opción es mantener un respaldo continuo de la información que se tiene dentro de la institución, la cual permite mantener los servicios activos, y a la institución trabajando normalmente.
-

- **VPN:** se definiría como mecanismo de ciberseguridad para este tipo de riesgo y es que como la información que navega se encontraría en texto plano las conexiones VPN que tienen los usuarios internos hacia la institución al momento de realizar teletrabajo se mantiene encriptada, por lo que ayudaría a la mitigación del riesgo.

Tabla 35. Mecanismos de ciberseguridad – Risk 003

Risk003			
			

Fuente: elaboración propia

Risk 004 *(Contraseñas débiles que pueden ser identificadas fácilmente)*.

La deficiencia en seguridad por parte de los usuarios al momento de generar una nueva contraseña tanto para sus aplicativos como para sus accesos es increíble, muchos de ellos por no olvidarse las contraseñas utilizan la misma para todo o en otros casos utilizan contraseñas tan sencillas que serían vulneradas enseguida, por tal razón los mecanismos identificados que ayudarían a que este riesgo disminuya son los siguientes si se identifican en la **Tabla 36**:

- **Control de acceso:** siendo la fortaleza de las contraseñas uno de los pilares principales en la parte de ciberseguridad, la institución financiera mantendría un mayor control en diferentes aspectos, siendo uno de estos el control de acceso a los usuarios que realizan teletrabajo, existe una vulnerabilidad mayor.
-
- **Cifrado de datos:** si se llegara a dar el caso de ser vulnerado por un atacante y descifrado las credenciales de acceso, la institución mantendría un control de cifrado de datos para que quien acceda desde dispositivos que no se encuentran vinculados a la institución sean detectados.
-
- **Respaldo de Información:** si el atacante logró vulnerar las credenciales del usuario con acceso a los diferentes sistemas mientras se encuentra

realizando teletrabajo, la institución proveería los respaldos oportunos previa identificación de que haya sido ataque quién alteró o elimino la información.

-
- **Filtrado de Contenido:** de igual manera todos estos controles estarían parametrizados de acuerdo con los accesos o roles que tienen cada uno de los usuarios internos al conectarse desde sus casas mientras realizan teletrabajo, y que estos sean validados a mostrar la información necesaria a la que el usuario accedería.

Tabla 36. Mecanismos de ciberseguridad – Risk 004

Risk004			
			

Fuente: elaboración propia

Risk 005 ***(Ciberataques que involucra la indisponibilidad de la información y servicios debido a inconvenientes con el proveedor de internet)***

Cómo se pudo identificar, este es uno de los riesgos más altos, el control no depende únicamente por parte de la institución si no por un tercero qué es el proveedor de internet, para los cuales se establecen controles correspondientes para este tipo de riesgo, por tal razón los mecanismos identificados que ayudarían a la mitigación de este son los siguientes si se identifican en la **Tabla 37**:

- **Firewall:** como toda la parte de navegación viene desde la red, el punto principal es la conexión directa con los proveedores de internet, por tal motivo la institución contaría con un filtro de lo que entra y sale para no ser víctimas de un ciberataque, por esto es necesario la implementación de un firewall perimetral.
-
- **Respaldo de Información:** al momento en que la información navega hacia las diferentes oficinas operativas y a los equipos que realizan teletrabajo, esta información sería vulnerada e interceptada, por tal motivo, al igual que

los riesgos anteriores es recomendable la generación de respaldos constantes de la información que la institución maneja.

-
- **VPN:** al momento de realizar teletrabajo existen varios componentes que se relacionan a la seguridad de esta, por tal razón, una de las principales opciones es la seguridad de la red, esto va relacionado entre el dispositivo que el usuario utiliza para realizar teletrabajo y el proveedor de internet, por esto, la institución ofrece tanto la conexión por una herramienta llamadas Citrix y una red pública virtual para la conexión hacia los aplicativos de la institución.
-
- **IPS:** al momento en que la información navega por la red de la institución, se confiaría en su proveedor de servicios de internet por lo cual la configuración de seguridad es primordial, y adicional tener un contrato que contemple confidencialidad, integridad y disponibilidad de la información.

Tabla 37. Mecanismos de ciberseguridad – Risk 005

Risk005			
			

Fuente: elaboración propia

Risk 006 ***(Falta de control en correos electrónicos, ocasionando ataques de phishing)***

Este riesgo es considerado como alto debido a que en la mayoría de los casos los usuarios que realizan teletrabajo llegarían a ser víctimas de ataques de phishing, es por eso por lo que la prevención principal aparte de los diferentes mecanismos que existen es la concientización hacia los usuarios para que no caigan en este tipo de ciberataques que podrían ocasionar un alto riesgo a la institución, por tal razón los mecanismos identificados que ayudarían a que este riesgo disminuya son los siguientes si se identifican en la **Tabla 38**:

- **Antivirus / Antimalware:** de ser el caso de que el usuario que realiza teletrabajo sufra un ciberataque de phishing, el control por parte de la institución con un antivirus o antimalware podría ayudar en la mitigación de que la persona que realice el ataque llegue a acceder a la información o al control de ciertas aplicaciones que la institución mantiene.
-
- **Firewall:** al momento de que un correo electrónico fraudulento es identificado con los tipos de control de la institución, el control de firewall perimetral permite controlar lo que ingresa a la institución, siendo este el primer filtro de validación para que no exista un ataque mediante phishing.
-
- **Control de acceso:** de confirmar de que se ha realizado un ataque de phishing mediante algún correo electrónico de los usuarios que realizan teletrabajo, el departamento de seguridad tendría un control prioritario para que quien haya podido vulnerar y acceder sin previa autorización, los controles de acceso a la información hacia las aplicaciones internas de la institución sean restringidos y controlados.
-
- **Filtrado de Contenido:** de igual manera dependiendo de los roles que el usuario tenga y los accesos, si es que el ataque es generado, la información se encontraría filtrada para que esta si llega a ser sustraída por el ciber atacante, sea mínima por no decir nula, y su intento de vulneración a los aplicativos del sistema sean opacados.

Tabla 38. Mecanismos de ciberseguridad – Risk 006

Risk006			
			

Fuente: elaboración propia

Risk 007 ***(Las funciones antivirus obsoletas causan inconvenientes en la seguridad de la información e infraestructura de la institución)***

Este riesgo es considerado como bajo debido a la actualización constante y el monitoreo de todos los dispositivos que realizan tanto el trabajo presencial cómo teletrabajo, por tal razón los mecanismos identificados que ayudarían a que este riesgo disminuya son los siguientes si se identifican en la **Tabla 39**:

- **Antivirus / Antimalware:** la institución mantiene actualizados los servidores de antivirus que constantemente se encuentran analizando los dispositivos que realizan teletrabajo, lo que permite mantener una seguridad referente tanto al dispositivo como en los archivos y la información que en este equipo se maneja.
-
- **Firewall:** de igual manera, si hay alguna detección referente a algún inconveniente ocasionado por los diferentes tipos de virus que hayan podido ingresar a la red de la institución, y tal vez lleguen a encontrarse dentro de los dispositivos que realizan teletrabajo, antes de que esto ocurra se procede con un control perimetral para evitar de que llegue a un ciberataque de este tipo, por lo cual se utiliza un firewall para seguridad de acceso.
-
- **Cifrado de datos:** el cifrado de datos más que mecanismo, sería considerado como un control en el caso de que por motivos de fuerza mayor un virus o derivado de este, hayan podido acceder a los dispositivos de la institución, evitar de que este logre obtener información relevante de lo que la institución realiza, en este caso por ser una institución financiera datos de socios clientes y estados económicos.
-
- **Respaldo de Información:** siempre como obligación se recomienda el continuo respaldo de la información para evitar futuros fraudes y que la información que se maneja llegue a perderse, con esta opción se mantendría disponible si se los necesite.
-

- **IPS:** al momento de realizar teletrabajo los usuarios disponen de su propio proveedor de servicio de internet, aparte del dispositivo mantener un cierto control de seguridad, existen proveedores de internet que ofrecen el servicio de protección de seguridad de datos como antivirus con licencia que se encuentran siempre activos durante el tiempo de que se contrate el servicio de internet, es por eso qué es recomendable realizar contratos con proveedores que cuenten con las seguridades adecuadas.

Tabla 39. Mecanismos de ciberseguridad – Risk 007

Risk007				
				

Fuente: elaboración propia

Risk 008 ***(El impacto de la presencia de malware en los dispositivos utilizados para teletrabajo)***

Este tipo de riesgo es considerado como alto, debido al impacto que ocasionaría en institución en el caso de que los dispositivos que son utilizados para realizar teletrabajo lleguen a presentar una infección de malware, se daría el caso de que un ciber atacante logre tener o control del dispositivo y por ende acceso a la información y a los diferentes aplicativos de la institución, por tal razón los mecanismos identificados que ayudarían a que este riesgo disminuya son los siguientes si se identifican en la **Tabla 40**:

- **Antivirus / Antimalware:** al igual que los virus, los malware también se encuentran actualizándose constantemente, por tal razón institución debe mantenerse analizando los dispositivos que realizan teletrabajo, para permitir mantener una seguridad referente tanto al dispositivo como en los archivos y la información que en este equipo se maneja.
-
- **Firewall:** de igual manera, si hay alguna detección referente a algún inconveniente ocasionado por malware que haya podido infectarse en algún dispositivo que realiza teletrabajo, antes de que esto ocurra se procede con

un control perimetral para evitar de que llegue a un ciberataque de este tipo, por lo cual se utiliza un firewall para seguridad de acceso.

-
- **Cifrado de datos:** el cifrado de datos más que mecanismo de seguridad, sería considerado como un control en el caso de que por algún motivo haya podido acceder a los dispositivos de la institución que realiza teletrabajo, y poder evitar de que este se propague y afecte al activo más importante de una institución financiera que son sus socios clientes.
-
- **Filtrado de Contenido:** dependiendo de los roles que el usuario tenga y los accesos a los que ingresaría, si es que la infección de malware llega a ser ejecutada, la información se encontraría filtrada para que el ciber atacante llegue a obtener únicamente una mínima parte de información, por no decir nula, y su intento de vulneración a los aplicativos del sistema sean opacados.

Tabla 40. Mecanismos de ciberseguridad – Risk 008

Risk008			
			

Fuente: elaboración propia

Risk 009 ***(La falta de convenios confidenciales, entre la institución y los usuarios internos, lo cual genera que la información confidencial de la institución sea sustraída o alterada)***

Este tipo de riesgo es considerado como alto debido a que, al momento de realizar teletrabajo, únicamente es evaluado el dispositivo de que cumpla con ciertas características de seguridad y más no un convenio o contrato de confidencialidad entre la institución y el usuario que realiza teletrabajo, por tanto, el usuario podría llegar a realizar actividades fuera del control de la institución, por tal razón los mecanismos identificados que ayudarían a que este riesgo disminuya son los siguientes si se identifican en la **Tabla 41**:

- **Control de Acceso:** el usuario no tendría accesos a más de los establecidos por la institución, esto garantiza de que no realizaría actividades dentro de

los sistemas que no le corresponden a su cargo o a su rol, permitiendo que los accesos sean específicamente los correctos para cada usuario.

-
- **Cifrado de Datos:** el cifrado de datos más que mecanismo, sería considerado como un control, el cual identificando el tipo de usuario que la institución tiene y asignado los roles adecuados, no llegue a ver más allá de lo que realmente tiene establecido y de querer obtener información adicional o entregar lo que se lograría obtener, esta se llegue a cifrar para que no caiga en manos equivocadas.
-
- **Respaldo de Información:** ciertos usuarios dependiendo el cargo que mantienen, disponen con una cuenta *cloud* para el respaldo de su información, por ende, si el usuario en sí elimina sus archivos o registros ya sean voluntariamente o por descuido, el administrador de este vería un histórico de todo lo que el usuario ha mantenido respaldado en su cuenta, ayudándolo a qué si la información es importante se logre mantener respaldada y segura.
-
- **Filtrado de Contenido:** dependiendo de los roles que el usuario tenga y los accesos a los que ingresaría, si el usuario intenta hacer uso indebido de sus accesos o intenta acceder a sitios de las aplicaciones a las cuales no están permitidos, con el filtro del contenido que este tiene, no le permitirá acceder ni a consultas ni vistas que no se encuentran autorizadas por parte del Departamento de seguridad al usuario indicado, y su intento de vulneración a los aplicativos del sistema sean opacados.

Tabla 41. Mecanismos de ciberseguridad – Risk 009

Risk009			
			

Fuente: elaboración propia

Como conclusión, cada uno de los mecanismos de ciberseguridad aplicados a los diferentes riesgos encontrados dentro del teletrabajo en la institución, brinda un apoyo de seguridad, tanto interna, como a los dispositivos externos para realizar sus actividades sin preocupación, pero se tendría en cuenta que nada es 100% seguro y que el primer filtro de seguridad es el usuario, por tanto la mejor inversión que una institución financiera llegara a realizar es la capacitación directa a cada uno de los usuarios para que logren identificar e incluso realizar su apoyo para que la institución no sea víctima de algún ciberataque, y que todos aporten en la mitigación de cualquier riesgo que a esto conlleve.

CAPITULO III. ANÁLISIS DE LOS RESULTADOS DE LA INVESTIGACIÓN

Como se mencionó anteriormente, la institución en el mayor de los casos provee a los usuarios de equipos de cómputo los cuales mantiene las diferentes políticas de seguridad para que estos dispositivos logren ser utilizados dentro de la red interna de la institución, para poder mantener la seguridad tanto de los dispositivos, de los usuarios y sobre todo de la información que en el caso de una institución financiera es lo más importante que ésta posee. Por otra parte los usuarios que no logren recibir un dispositivo para la realización de teletrabajo utilizarían su propio equipo personal, para lo cual pasarían por un análisis por parte del área de seguridad de la información de la institución para poder hacer uso del mismo, este análisis consta de validaciones de licencias, actualizaciones del sistema operativo y otros aplicativos, verificación de antivirus actualizado y funcional correctamente, y en el caso de no tenerlo la institución brinda a los usuarios una licencia de McAfee - *Mvision* para poder proteger sus dispositivos, así estén conectados a la red de sus hogares o sitios de trabajo do nde se encuentran realizando el teletrabajo.

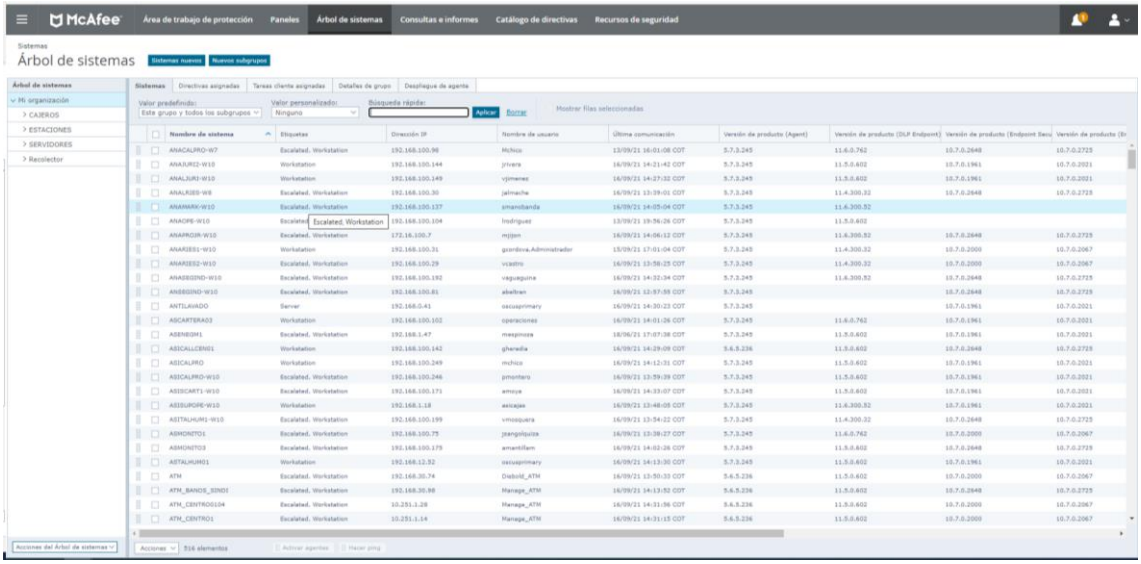
3.1. McAfee EPO (ePolicy Orchestrator)

En este caso se procede con la revisión y el análisis de la herramienta McAfee EPO el cual es el analizador de la parte de seguridad referente a virus, malware, DLP (*Data Loss Prevention*) EPE (*Endpoint Encryption*), WG (Web Gateway) y otros complementos de seguridad referentes a la herramienta de McAfee, el cual no sólo analiza los dispositivos de trabajo, además permite el control y análisis de servidores y cajeros automáticos (ATM) para poder tener una mayor seguridad al momento en que estos diferentes dispositivos lleguen a estar conectados en una red.

Como se muestra en la **Figura 13** a continuación, esta herramienta permite indicar el nombre del equipo, su dirección IP, el nombre del usuario al que pertenece y sobre todo la fecha y hora de la última comunicación que ha tenido con el servidor, lo cual permite analizar y verificar si el dispositivo que se desea investigar se

encuentra o no conectado o relacionado al servidor de la red interna de la institución.

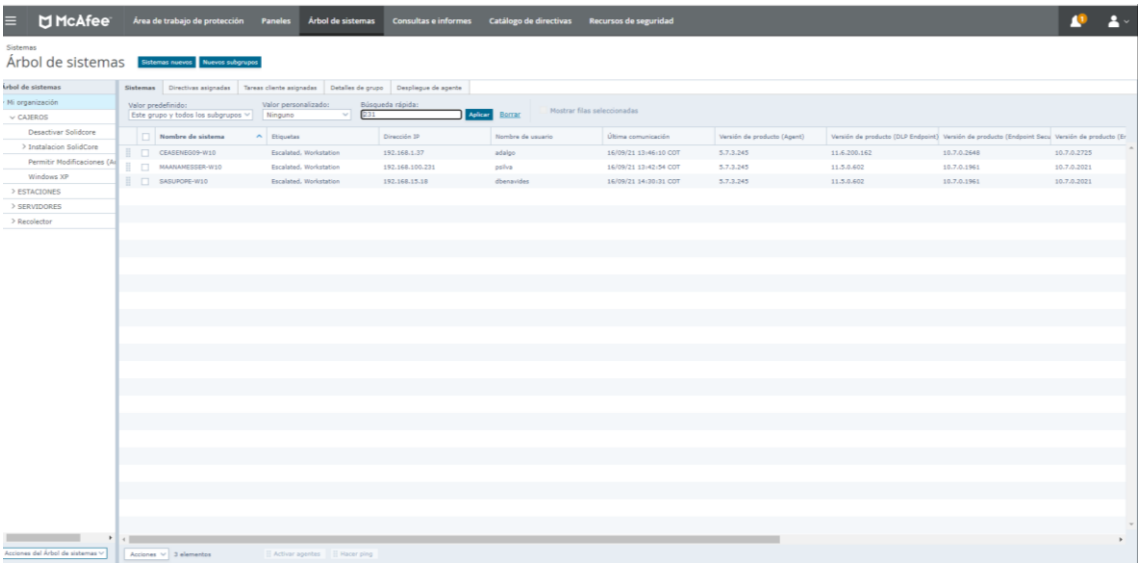
Figura 13. McAfee EPO – Árbol del sistema



Fuente: Coop. Oscus - McAfee ePolicy Orchestrator

Para el análisis concreto de un dispositivo o estación de trabajo se procede a seleccionar un equipo dentro del McAfee EPO, el cual en este caso es el dispositivo con la IP xx.xx.xx.231 como se muestra a continuación en la **Figura 14**, la cual indica los datos pertenecientes a este equipo antes de ser analizado por el personal de seguridad de la institución.

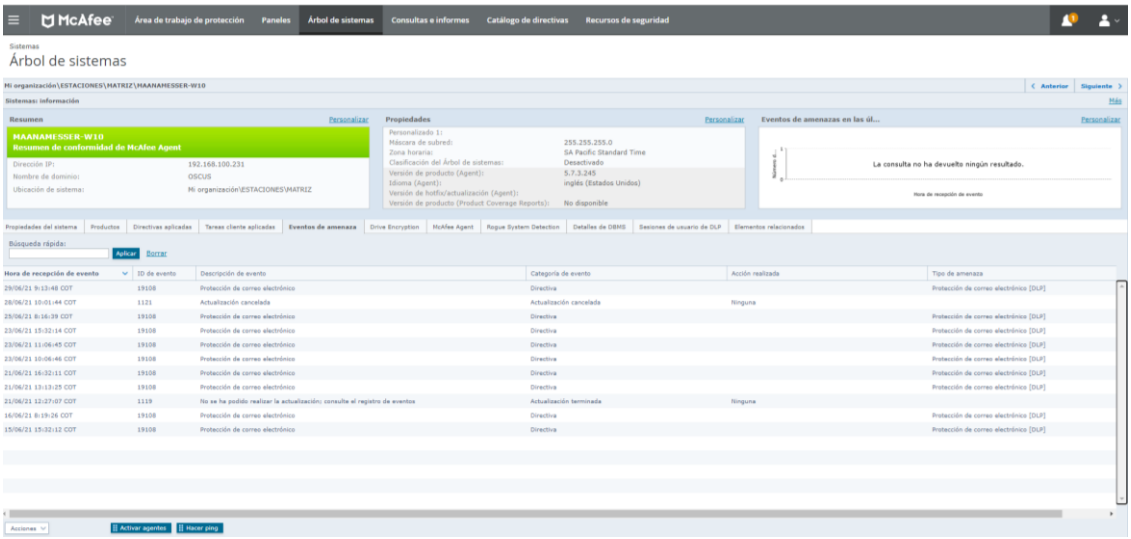
Figura 14. McAfee EPO – Árbol del sistema por IP



Fuente: Coop. Oscus - McAfee ePolicy Orchestrator

La herramienta permite analizar e identificar diferentes eventos de amenazas que serían detectados en el dispositivo analizado, como se muestra a continuación en la **Figura 15**, se detectan varios eventos referentes a correos electrónicos, los cuales son identificados para la protección de estos dentro de una amenaza controlada por DLP (*Data Loss Prevention*).

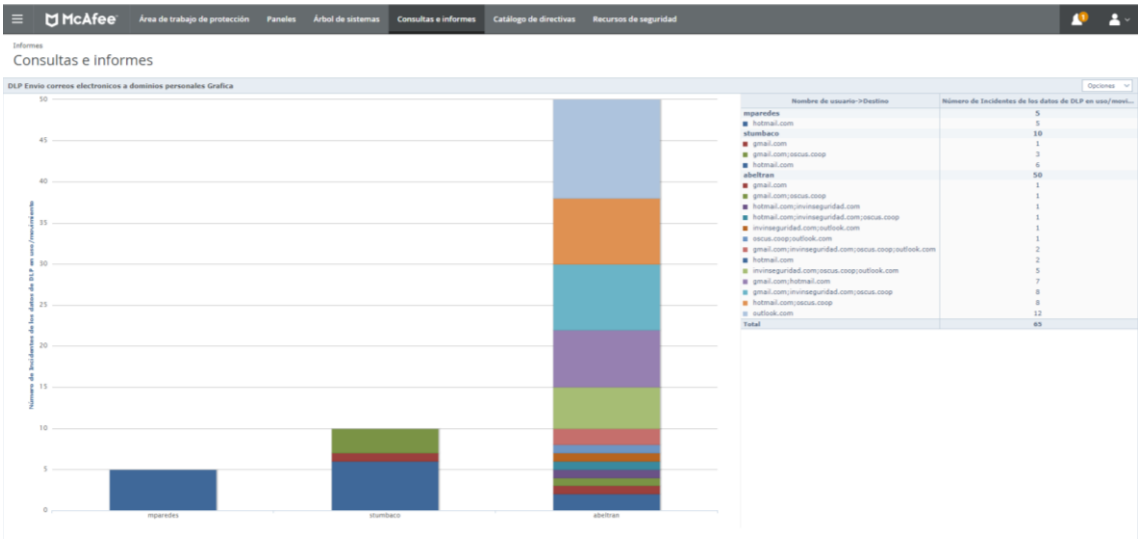
Figura 15. McAfee EPO – Eventos de amenazas



Fuente: Coop. Oscus - McAfee ePolicy Orchestrator

Adicional a lo ya indicado, la herramienta permite en forma general un análisis de los dominios de correo enviados por parte de los usuarios, y la cantidad de correos enviados a los mismos permitiendo generar una consulta o informe por parte de la herramienta con respecto a la cantidad de incidentes de los datos de DLP con relación a los correos. En la **Figura 16**, se logra observar lo indicado en una forma gráfica, también conocidos como *dashboards*, los cuales permiten llegar a ser mucho más entendibles para el usuario que realiza los respectivos monitoreos.

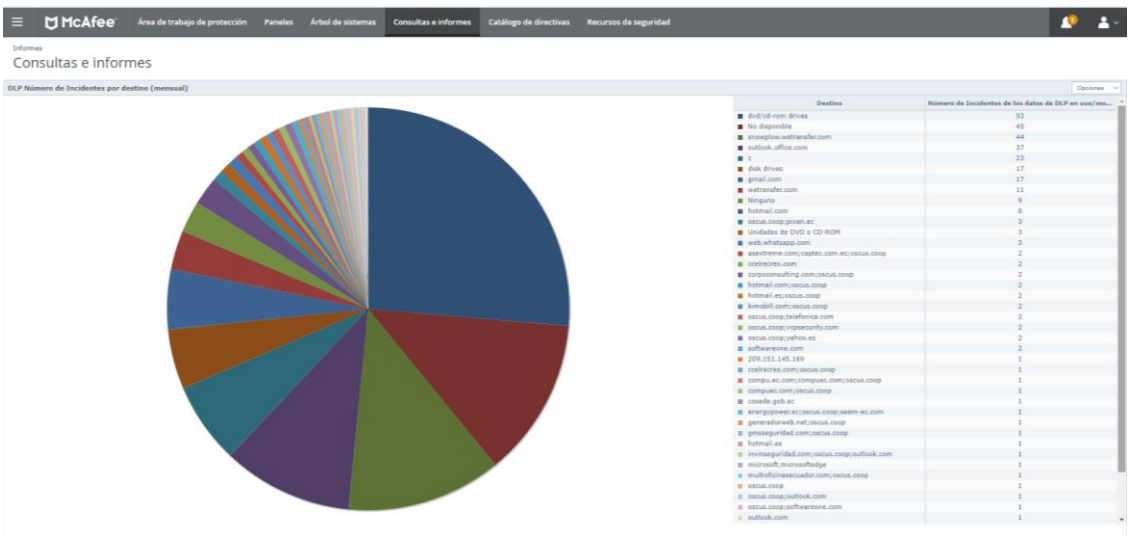
Figura 16. McAfee EPO – Dashboard correos externos



Fuente: Coop. Oscus - McAfee ePolicy Orchestrator

Continuando con el monitoreo del equipo xx.xx.xx.231, la herramienta permite visualizar la cantidad de incidentes generados referente a la navegación a las diferentes páginas direcciones IP a las cuales el equipo analizado accede durante el período de tiempo, permitiendo al personal encargado del monitoreo identificar dentro de todas estas cuál sería probablemente el mayor indicador que podría ocasionar un ciberataque por mal manejo o descuido por parte del usuario que utiliza este dispositivo. Como se muestra en la **Figura 17** a continuación, los índices de navegación controlados por la herramienta.

Figura 17. McAfee EPO – Dashboard navegación



Fuente: Coop. Oscus - McAfee ePolicy Orchestrator

En el caso de una institución financiera se tendría en claro que hay muchos factores que podrían conllevar a ser víctimas de un ataque por parte de ciber delincuentes, los cuales por un mínimo descuido podrían acceder encontrando las vulnerabilidades que se podría estar quedando a la vista, obtener información de la institución y llegar a perjudicar a la institución tanto en su reputación, como en su parte económica, lo cual en el mercado no sería bien visto y tendría grandes pérdidas, sus socios y clientes perderían la confianza y buscarían otra institución.

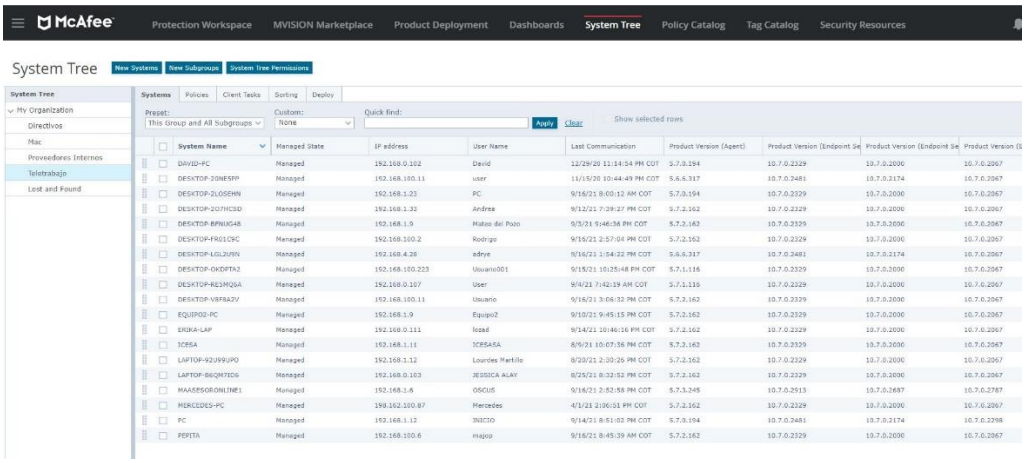
3.2. **McAfee Mvision EPO (ePolicy Orchestrator)**

En este primer caso se procede con la revisión y el análisis de la herramienta McAfee Mvision EPO el cual es el analizador de la parte de seguridad referente a virus, malware, y otros complementos de seguridad referentes a la herramienta de McAfee, pero con la diferencia de que esta herramienta se basa específicamente a los dispositivos de los usuarios que realizan teletrabajo y no cuentan con un control de seguridad, ya sea este antivirus, anti malware o algún otro mecanismo que permita mantener la seguridad y confiabilidad del dispositivo al momento de realizar las actividades encomendadas. Estos dispositivos van a poder ser controlados de igual manera como si estuviesen conectados dentro de la red interna de la institución teniendo en cuenta que no se aplicarían los mismos controles de seguridad que los dispositivos de la institución, por ser dispositivos personales de los usuarios, estos van a necesitar un control diferente, es decir una mayor libertad en ejecución de aplicaciones, navegación a páginas web, uso de aplicaciones financieras, conexión con otros dispositivos y sobre todo conexión a un internet libre en el sitio donde se llegan a conectar.

Como se muestra en la **Figura 18** a continuación, esta herramienta permite mostrar el nombre del equipo, su dirección IP la cual es asignada por su propio ISP (*Internet Service Provider*), el nombre del usuario al que pertenece, como se indicó anteriormente, este no es un usuario de dominio, sino únicamente el usuario creado por la persona que utiliza el dispositivo, además muestra la fecha y hora de la última comunicación que ha tenido con el servidor de la institución, lo cual permite analizar

y verificar si el dispositivo que se desea investigar se encuentra o no conectado o relacionado al servidor de la red de la institución.

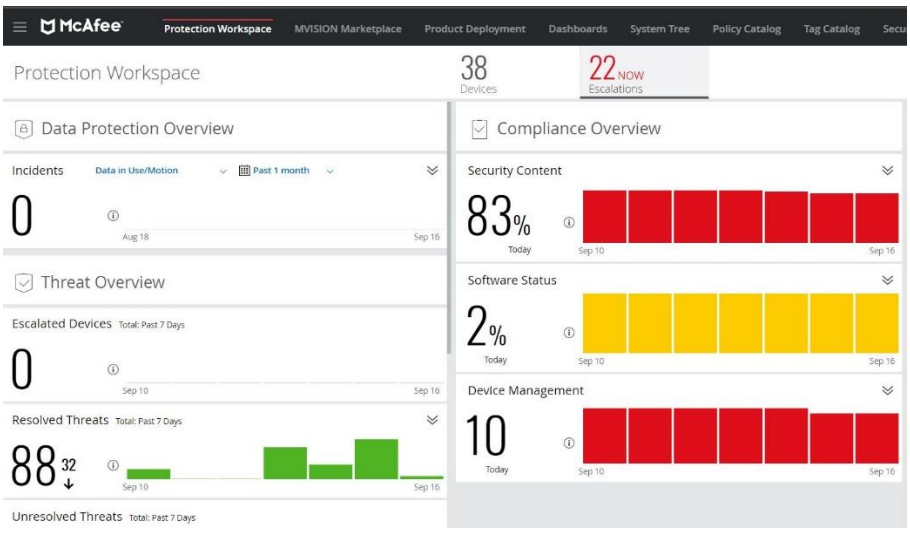
Figura 18. McAfee Mvision EPO – Árbol del sistema



Fuente: Coop. Oscus - McAfee Mvision

Mediante los *dashboard* que la herramienta genera se logra identificar la protección referente al área de trabajo de los dispositivos que se encuentran realizando teletrabajo y cuentan con la herramienta *Mvision* como se muestra a continuación en la **Figura 19**, muestra una descripción general de protección de datos como incidentes, dispositivos escalados, amenazas resueltas, también muestra una descripción general del cumplimiento como el contenido de seguridad, estado de software, administración de dispositivos.

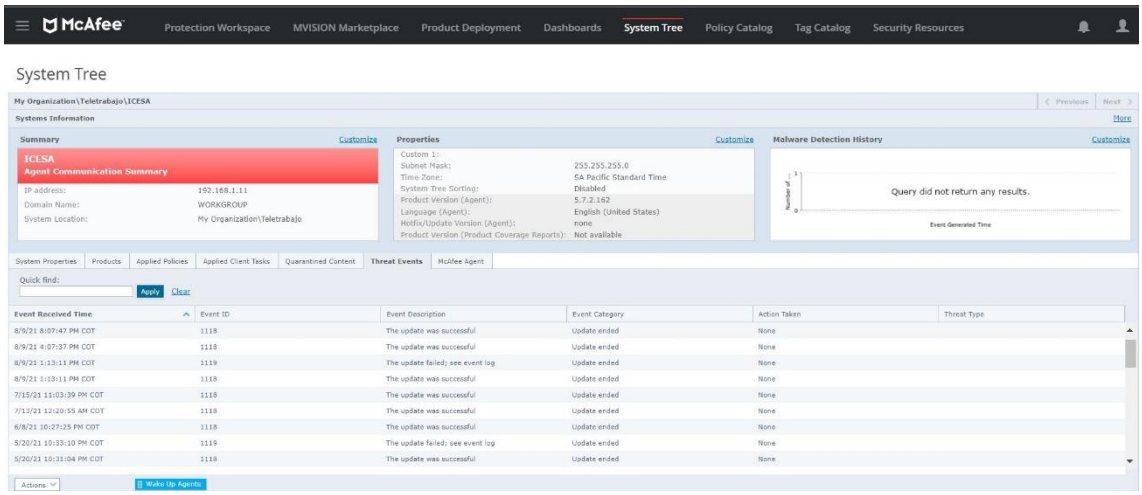
Figura 19. McAfee Mvision EPO – Protección de área de trabajo



Fuente: Coop. Oscus - McAfee Mvision

Y finalmente, la herramienta muestra una forma resumida de un dispositivo en específico indicando ya sean actualizaciones o eventos del producto y de ser el caso si el administrador lo solicitara o lo gestionara, la generación de políticas para los equipos como se muestra a continuación en la **Figura 20**, pero como se mencionó anteriormente estas políticas serían un poco irrelevantes, son dispositivos propios de los usuarios los cuales necesitaría accesos adicionales sin las restricciones que la institución aplicaría a cada uno de ellos.

Figura 20. McAfee Mvision EPO – Eventos recibidos

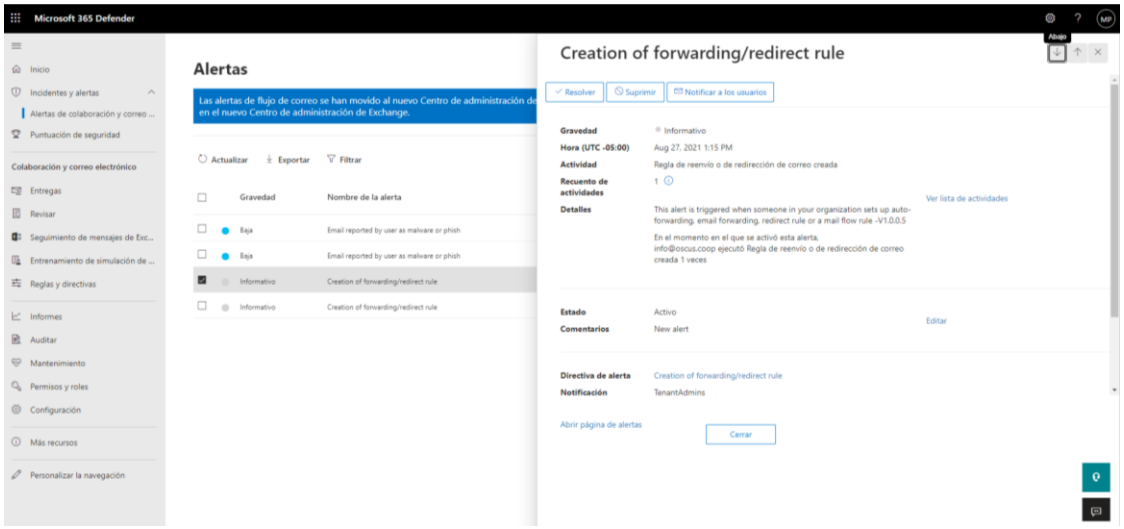


Fuente: Coop. Oscus - McAfee Mvision

3.3. Correo Electrónico

Para la prevención de phishing mediante correos electrónicos la institución cuenta con un control de la herramienta de Microsoft 365 defender, la que permite tener un control de los mismos, como se muestra a continuación en la **Figura 21**, genera alertas en las que se implementaría la creación de reenvíos de correo o reglas de redirección para poder filtrar que los correos que ingresó o salen logren ser re direccionados en el caso de identificar que sean fraudulentos o tengan algún archivo malicioso que llegue a afectar el servicio que la institución ofrece.

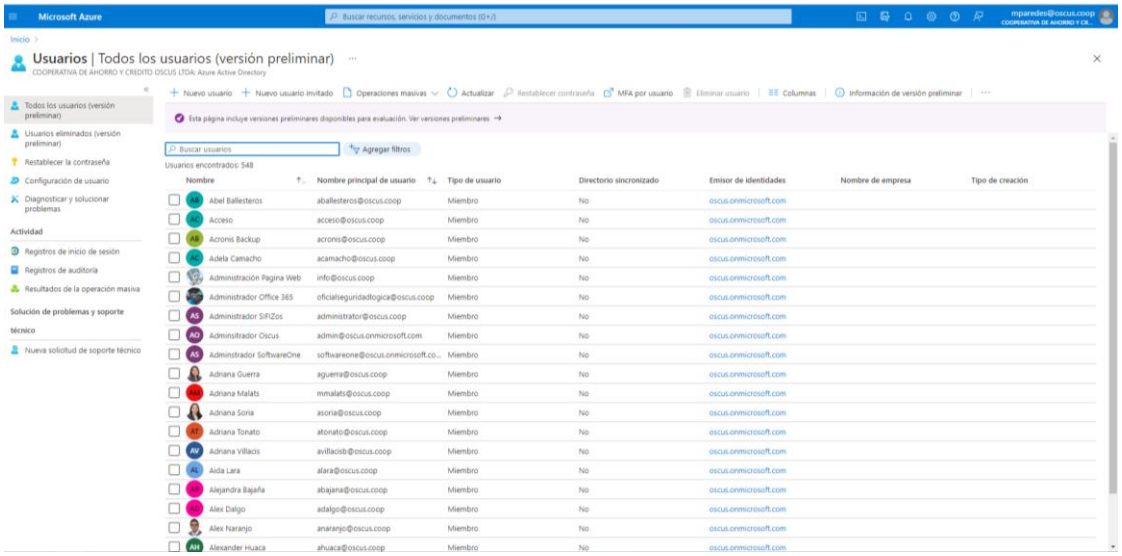
Figura 21. Alertas



Fuente: Coop. Oscus – Microsoft 365 Defender

Esta herramienta tiene una gestión de lista de usuarios como se muestra a continuación **Figura 22**, controla todos los correos corporativos, como de administración de la herramienta, esto para indicar e identificar que todos los usuarios se encuentran monitoreados y logren ser aplicadas las reglas que el administrador realice y gestione.

Figura 22. Listado de usuarios

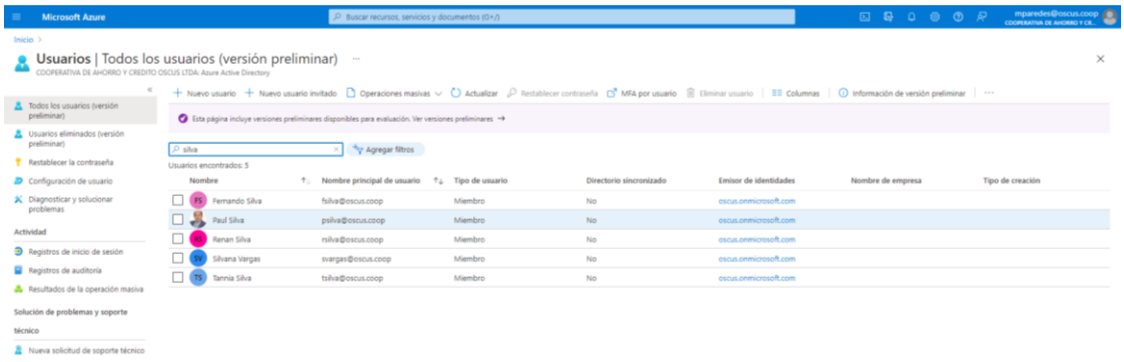


Fuente: Coop. Oscus – Microsoft Office 365 Defender

Para verificación de pruebas de análisis, se lo realiza directamente con el correo *psilva@oscus.coop* perteneciente a Paúl Silva como se muestra a continuación

Figura 23, el cual, para los fines pertinentes del presente proyecto, se procede a identificar ciberataques a los que el correo en mención llegó a ser expuesto.

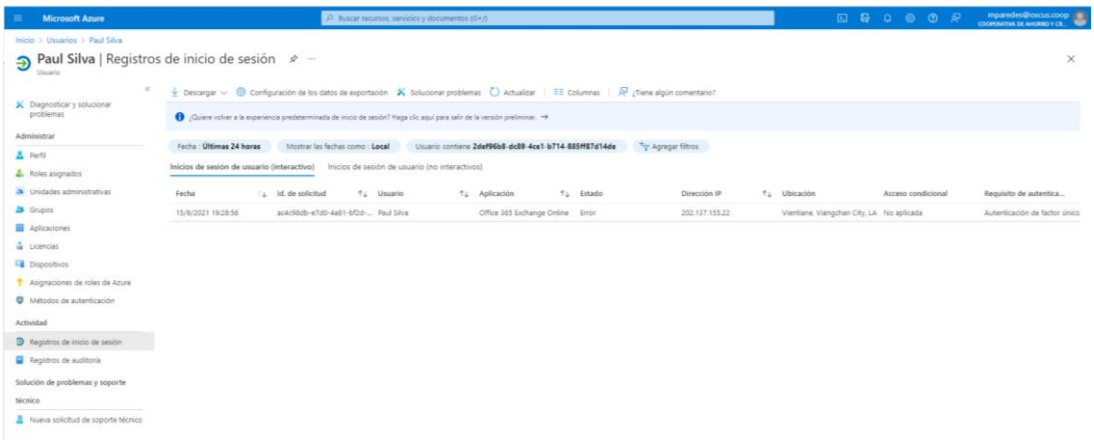
Figura 23. Análisis de usuario



Fuente: Coop. Oscus – Microsoft Azure

Dentro del control de *Microsoft Azure*, se logra analizar las actividades de registro de inicio de sesión de la cuenta indicada anteriormente y como se muestra a continuación en la **Figura 24**, en la fecha 15/09 sufrió un ataque de inicio de sesión, como se observa en la herramienta que permite indicar la ubicación desde donde se intentó el ingreso, la dirección IP, y cuál fue el tipo de ataque que el correo pudo haber sido vulnerado, en este caso el inicio de sesión.

Figura 24. Registro de inicio de sesión

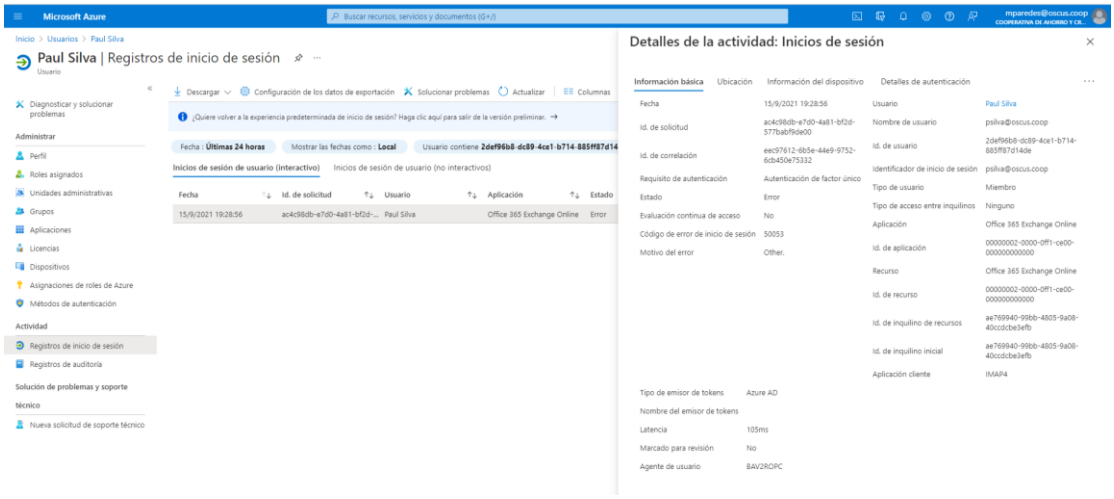


Fuente: Coop. Oscus – Microsoft Azure

En este caso al seleccionar la actividad identificada en la herramienta de *Microsoft Azure*, se logra observar diferentes detalles que fueron generados como por ejemplo los datos específicos del correo la falla que pudo haberse ocasionado en

este caso la autentificación de factor único, así como otros, como se muestra a continuación en la **Figura 25**.

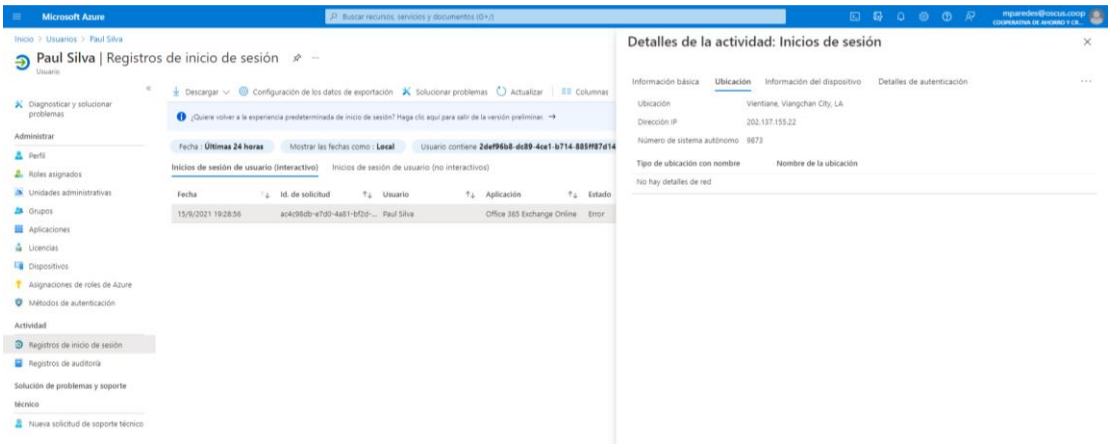
Figura 25. Registro de inicio de sesión – Información básica



Fuente: Coop. Oscus – Microsoft Azure

Una de la información principal que se obtiene es la ubicación del sitio desde donde se trató de vulnerar el correo electrónico, en este caso como se muestra en la **Figura 26**, el ataque fue realizado desde Vientiane, Viangchan City, LA. desde la IP 202.137.155.22, el cual es un indicio para empezar a rastrear a quien haya intentado realizar este ataque.

Figura 26. Registro de inicio de sesión – ubicación

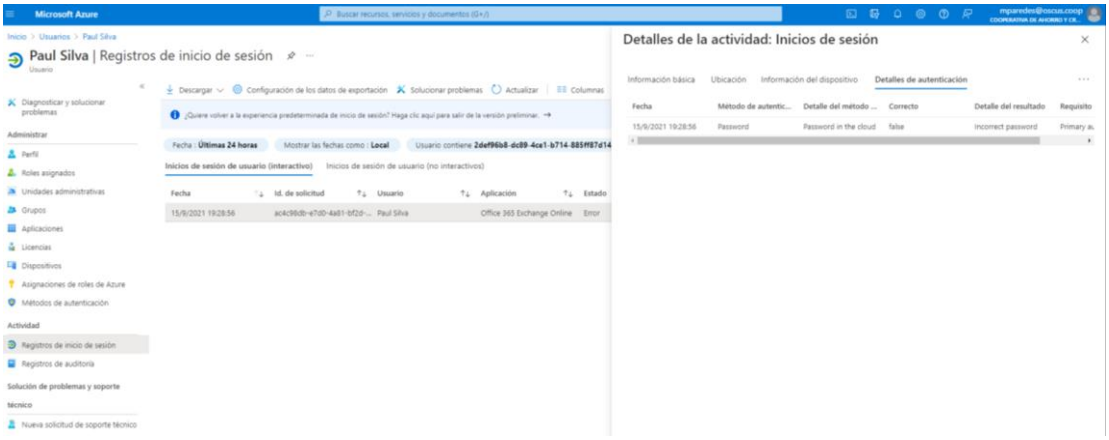


Fuente: Coop. Oscus – Microsoft Azure

Otra información adicional que se identifica son los detalles de autentificación que se pudieron dar al momento de intentar vulnerar este correo electrónico, como se

muestra en la **Figura 27**, como son el método de autenticación por el cual intentaron acceder, en este caso es el método de *Password* como lo indica la herramienta, sí fue exitoso o no dicha validación en este caso el resultado es *false* debido a que la contraseña cumple con todos los requerimientos para la generación de contraseñas, y el detalle del resultado, que por la indicación anterior el resultado es *Incorrect Password*,

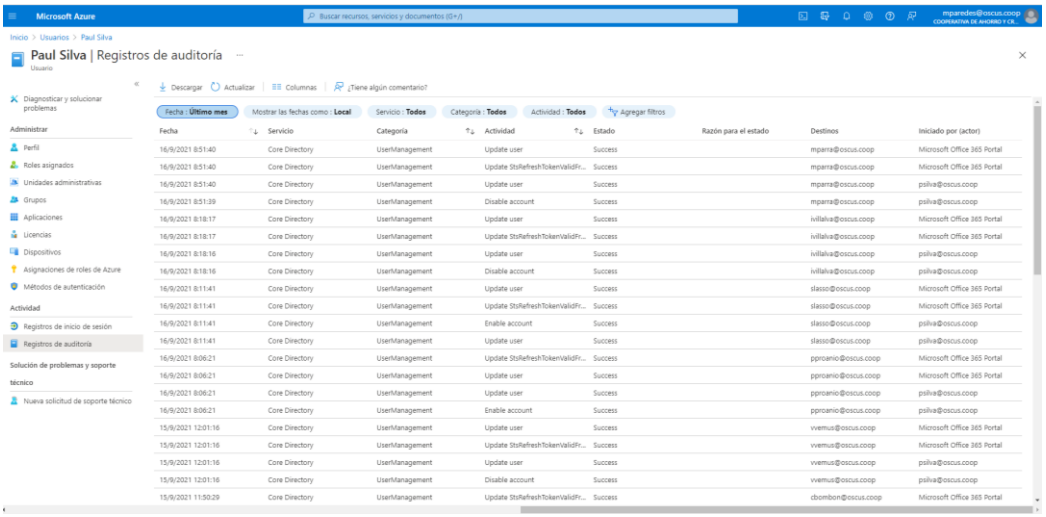
Figura 27. Registro de inicio de sesión - autenticación



Fuente: Coop. Oscus – Microsoft Azure

Un complemento adicional bien útil dentro de esta herramienta de Microsoft Azure son los registros de auditoría, los cuales muestran los servicios que consume la actividad que fue realizada por dicho correo y los destinos, es decir a qué correo fue afectado por parte del correo del usuario antes mencionado, esto ayuda a qué se logre mantener un control tipo logs para análisis en el caso de algún inconveniente con alguna de estas cuentas como se muestra en la **Figura 28** a continuación.

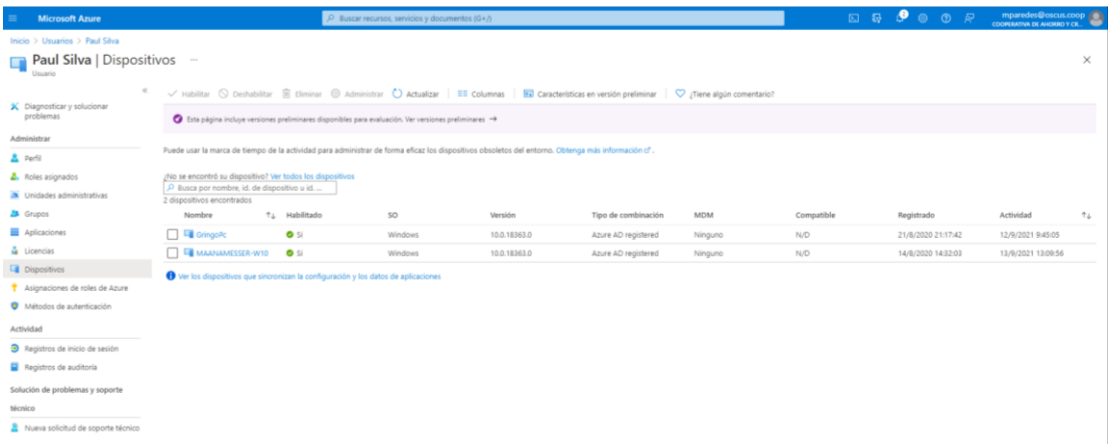
Figura 28. Registro de Auditoría



Fuente: Coop. Oscus – Microsoft Azure

Para un control de acceso el correo electrónico, la herramienta brinda la opción de identificar los dispositivos en el cual el usuario ha iniciado sesión como se muestra a continuación en la **Figura 29**, esto permite al administrador de la herramienta tener un análisis de la fecha y hora, pero sobre todo, el equipo en que se inició sesión, esto con el fin de precautelar la seguridad de cada uno de los correos institucionales, por ende, el usuario interno tendría máximo 3 dispositivos vinculados, estos serían, el equipo que utilizan para el trabajo normal dentro de la institución, el equipo personal en el que se encuentran realizando teletrabajo, por último, y de ser el caso, un dispositivo móvil en el cual se encuentra registrado el correo institucional.

Figura 29. Registro de Dispositivos



Fuente: Coop. Oscus – Microsoft Azure

3.4. Centro de Operaciones de Seguridad (SOC)

El centro de operaciones de seguridad más conocido como SOC, es una plataforma que permite ayudar en la supervisión y la administración de la seguridad de una institución, incluyéndose a estas la seguridad de los sistemas de información a través de diferentes herramientas que realice una correlación de eventos e intervención, ya sea de aplicativos o de la red, más conocido como SIEM (*Security Information Event Management*) la cual es la herramienta principal del SOC y la que permite gestionar todos los eventos de un sistema de información.

La primera etapa para establecer un SOC es definir de forma precisa la estrategia de cómo se van a integrar los objetivos específicos de la institución, para que esta permita supervisar las diferentes vulnerabilidades que se podrían encontrar tanto dentro de la infraestructura de red, como en las diferentes aplicaciones que la institución posee, y permitir ayudarles en la protección de los datos confidenciales de la institución y cumplir con las normativas de seguridad que se establecerían para la misma.

Como se muestra en la **Figura 30** a continuación, la herramienta SOC genera un reporte de incidentes de seguridad, en donde se especifica la fecha y hora en el que el evento ocurrió, en este caso, lo que el SOC reporta es un evento de manipulación de una cuenta de correo electrónico de Office 365, siendo el usuario *psilva@oscus.coop* el que realice la manipulación de la cuenta de correo *slasso@oscus.coop*, en la cual reporta el usuario *psilva* habilitó la cuenta de *slasso*, para esta sustentación el usuario indicaría los motivos porque se realizó la activación de la cuenta antes indicada, caso contrario podrían aplicar sanciones por una manipulación indebida dentro de los aplicativos internos de la institución.

Figura 30. Actividades

gmsoc	CENTRO DE OPERACIONES DE SEGURIDAD (GMS - SOC)			gms seguridad de la información		
	REPORTE DE INCIDENTES DE SEGURIDAD					
Control documental		Riesgo:	Crítico	Rojo		
Fecha:	16/9/2021		Alto	Naranja		
Operador:	HENRY BARROS		Medio	Amarillo		
			Bajo	Verde		
Hora del reporte:	8:38		Informativo	Azul		
Cliente:	OSCUS	Compromiso:	Toda la red	Un grupo de host	Un equipo normal	
Clasificación Activos (SGSI):	CONFIDENCIAL					

INCIDENTES DE SEGURIDAD

ID-Alarma	Nombre de la Alarma	Riesgo	Fecha y Hora	Origen	Destino	Repeticiones
1	Account Manipulation — Habilitación de cuenta Office 365	Medio	16/09/2021 08:11	No aplica	office365[.]com	1

Id-Alarma	Usuario	Cuenta habilitada	Evidencia
1	psilva@oscus.coop	slasso@oscus.coop	https://oscus.alienvault.cloud/#/activity/alarms/f69bdf24-78cb-ba06-cb3d-438689669efd

Nombre Alarma	Descripción
Account Manipulation — Habilitación de cuenta Office 365	Se ha modificado una cuenta de usuario. La cuenta de usuario: psilva@oscus.coop habilito la cuenta de usuario: slasso@oscus.coop.

Nombre Alarma	Recomendación
Account Manipulation — Habilitación de cuenta Office 365	Verificar si la cuenta de usuario: psilva@oscus.coop que realizó el cambio es una cuenta válida y con los privilegios para realizar esa tarea. Verificar que todos los cambios realizados en la cuenta de usuario: slasso@oscus.coop hayan sido cambios establecidos por el administrador.

Fuente: Coop. Oscus – Security Operations Center

Una vez que se detectó los posibles riesgos que pueden ocasionarse al realizar teletrabajo se procedió al análisis de cada uno de ellos y se propuso el uso de mecanismos de ciberseguridad para los dispositivos que realizan teletrabajo, los cuales, al indicarlos a los diferentes departamentos que se encargan de la seguridad de la institución financiera, tanto de Seguridad de la Información, como de Tecnología de la Información para su aplicación, se identificó que en ciertos casos si se mantiene un control referente a los mecanismos indicados anteriormente, y en otros casos faltaba un control para los mismos, por tal motivo al establecer cada una de las acciones con referencia a cada uno de los riesgos como se muestra en la **Tabla 42**, se pudo llegar a concluir que los administradores

mantienen un mejor control, tanto de los dispositivos internos, y de los dispositivos de los usuarios que realizan teletrabajo, como del control interno de la institución.

Tabla 42. Mecanismos de ciberseguridad / Riesgos

Riesgos / *Mecanismos de ciberseguridad disponibles para la seguridad en una institución financiera asociado al teletrabajo*	Cambio o pérdida de información debido a los respectivos accesos a la misma	Falta de controles de seguridad en la ejecución de aplicaciones involucra que los dispositivos ejecuten aplicaciones sin validaciones	Usuarios vulnerables a realización de ingeniería social, involucrando la seguridad de la institución.	Contraseñas debiles que pueden ser identificadas facilmente	Ciberataques que involucra la indisponibilidad de la información y servicios debido a inconvenientes con el proveedor de internet	Falta de control en correos electronicas, ocacionando ataques de phishing	Las funciones antivirus obsoletas causan inconvenientes en la seguridad de la información e infraestructura de la institución	El impacto de la presencia de malware en los dispositivos utilizados para teletrabajo	La falta de convenios confidenciales, entre la institución y los usuarios internos, lo cual genera que la información confidencial de la institución sea sustraida o alterada.
Antivirus / antimalware									
Firewall / equipo perimetral									
Control de acceso									
Cifrado de datos									
Respaldo Información									
Redes privadas virtuales									
Filtrado de contenido									
IPS									

Fuente: elaboración propia

Por lo tanto, con los diferentes mecanismos de ciberseguridad planteados, se afirmaría que la seguridad dentro de la institución referente al uso de dispositivos en teletrabajo generó un cambio positivo para la cooperativa, cumpliendo correctamente con todos los mecanismos, desde:

- La instalación de **antivirus / antimalware** en los dispositivos de los usuarios para la protección de estos.

- El control interno mediante **Firewall / equipo perimetral**, para el control de filtro de conexiones y navegación por parte de cada uno de los usuarios.

- El **Control de acceso** para cada usuario interno que realiza teletrabajo cumpliendo con el control de credenciales para acceder a los diferentes aplicativos.

- El **Cifrado de datos** para mantener una seguridad de que en el peor de los casos la información llegue a ser sustraída por un ciber atacante, esta no llegaría a ser utilizada ni analizada por los mismos.

- El **Respaldo de Información** para que la misma se volviera a obtener y ser utilizada por los usuarios en caso de existir algún inconveniente.

- El uso de **Redes Privadas Virtuales** para mantener conexiones encriptadas al momento de establecer conexión remota desde los sitios de teletrabajo hacia los aplicativos internos de la institución.

- El **Filtrado de contenido** para que los usuarios no logren acceder más allá de lo que se les encuentra permitido en sus roles, y,

- El uso seguro y garantizado de un **IPS** quienes son los que garantizarían que la conexión y navegación por la que los usuarios realizan teletrabajo sea segura y confiable.

De igual manera al comentarles a los diferentes usuarios internos que realizan teletrabajo sobre la implementación de todos estos tipos de mecanismos de ciberseguridad para los dispositivos que se encuentran utilizando para el uso de sus aplicaciones diarias mediante la modalidad de teletrabajo, indican que se encuentran más seguros en el uso de los dispositivos, indicandoles que eso les brinda una mayor confianza y seguridad desde el momento en que se conectan desde sus dispositivos, obviamente teniendo en cuenta que el primer filtro para que todo esto funcione correctamente son ellos, los usuarios, son las piezas fundamentales en identificar e informar cualquier anomalía que se logre detectar en los dispositivos que se encuentran utilizando para teletrabajo.

CONCLUSIONES

- Según lo indicado a lo largo de este proyecto, se llega a la conclusión de que, en la actualidad, debido a la gran cantidad de ataques y estafas cibernéticas que se realizan, las instituciones tenedrían en cuenta que la aplicación de ciberseguridad es una prioridad, sobre todo en este caso que se trata de una institución financiera, la cual aplicaría mecanismos de ciberseguridad para el control de los dispositivos que realizan teletrabajo, existen varios riesgos que serían mitigados con la aplicación de estos mecanismos, como se analizó en la **Tabla 30**, teniendo un impacto positivo como protección tanto a los dispositivos, como al bien más importante que es la información, permitiendo contrarrestar posibles ataques a futuro.

- De acuerdo a la información recopilada de diferentes autores, se concluye que el teletrabajo se ha catalogado como una modalidad indispensable en la labor de las diferentes instituciones, cualquier usuario que tenga los privilegios adecuados podría realizarlo, pero en la mayoría de los casos, las instituciones no cuentan con los respectivos mecanismos de ciberseguridad suficientes para mantener el control y la seguridad dentro de las instituciones debido a su alto costo, y al desconocimiento de los técnicos que los administran, permitiendo a los ciber atacantes estar un paso delante de ellos, y se encuentren listos para explotar cualquier vulnerabilidad que se logre detectar.

- El diagnóstico de la situación actual de los mecanismos de ciberseguridad en los dispositivos de los usuarios de la institución que realizan teletrabajo permitió la adecuada elaboración de una guía de buenas prácticas para la implementación de mecanismos de ciberseguridad en los dispositivos y en la institución para la mitigación de los diferentes riesgos encontrados. Además, como los encuestados pertenecen a las diferentes áreas técnicas, las validaciones tienen un mayor peso, son usuarios que conocen los efectos que podría ocasionar si los riesgos existentes llegan a ser vulnerados.

- Mediante la aplicación de metodologías como los estándares ISO 27005, la cual se basa en la gestión de riesgos de la seguridad de la información con los procesos de planificar, hacer, verificar y el actuar y de Magerit V3 la cual analiza los riesgos derivados del uso de tecnologías de la información, desde la definición del alcance hasta el tratamiento, se valida con los administradores de áreas que la aplicación de los mecanismos de ciberseguridad en los dispositivos de teletrabajo, permiten la generación de mayor control dentro de una prueba piloto aplicada a los usuarios que han realizado teletrabajo en mayor tiempo dentro de la institución.

- Del análisis realizado en la vinculación de los mecanismos de ciberseguridad para la mitigación de los riesgos identificados, su llegaría a concluir que a mayor control, mayor seguridad, al inicio al determinar los riesgos se identifican de diferente magnitud, desde bajos hasta altos, corroborando que al momento de aplicar los distintos mecanismos de ciberseguridad a cada uno de los riesgos, el seguimiento del control es más identificable para los administradores de los departamentos, por tal motivo con la generación de una guía de buenas prácticas para la aplicación de mecanismos de ciberseguridad para los dispositivos que realizan teletrabajo, brinda a la institución un manejo de los controles para ser aplicados en el caso en encontrar vulnerabilidades en la aplicación de teletrabajo.

RECOMENDACIONES

- Como se trata de una institución financiera que mantendrá usuarios realizando teletrabajo, se recomienda diseñar un plan de contingencia en caso de que algún nuevo medio de ataque encuentre alguna vulnerabilidad de seguridad que quebrante los controles y comprometa los sistemas internos de la institución, exponiendo un bien importante como es la información, para lo cual se contaría con copias de respaldo (*backup*) físicamente o en *cloud servers* para tener una base actualizada por si se llega a vulnerar y afectar a la institución.

- Debido a los altos índices de ataques cibernéticos que se detectan y son dados a conocer a nivel mundial, la recomendación principal hacia la institución es mantener capacitados a los técnicos que se encargan de la seguridad interna y externa, al día en la protección de dispositivos e infraestructura, adicional invertir en software y hardware, a mayor vulnerabilidad, mayor protección dentro de la institución y en los dispositivos que se encuentran realizando teletrabajo.

- Así como se obtuvo información relevante de los dispositivos que realizan teletrabajo para la generación de una guía de buenas prácticas para la implementación de mecanismos de ciberseguridad, así mismo se recomienda que se generen revisiones y evaluaciones continuas en dichos dispositivos, estándose siempre en coordinación con los técnicos de la institución para que los controles sean realizados correctamente para futuras actualizaciones de guías que permitan el control constante de la seguridad de la institución.

- De la misma manera que se realizan revisiones y análisis de los dispositivos que realizan teletrabajo, de igual forma se recomienda la realización de pruebas continuas con la aplicación de estándares y metodologías validas que permitan evaluar, controlar y evitar que se vulneren nuevos riesgos que

se llegarían a identificar, debido a los nuevos ciberataques que se desarrollarían.

BIBLIOGRAFÍA

AppSec, O. W. (2021). *Metodología de calificación de riesgos*. Obtenido de https://owasp.org/www-community/OWASP_Risk_Rating_Methodology

Bortnik, S. (2010). *¿Qué es la fuga de información?* Obtenido de https://www .welivesecurity.com/la-es/2010/04/13/que-es-la-fuga-de-informacion/

Bravo Sandoval. (2010). *Importancia de la gestión de servicios de tecnología de información basada en ITIL*. Obtenido de CDIGITAL: http://cdigital.uv. mx/bitstre am/1234567 89/29464/1/

Cataño Ramírez, S. L., & Gómez Rúa, N. E. (2014). El concepto de teletrabajo: aspectos para la seguridad y salud en el empleo. *CES Salud Pública Volumen 5*.

ElevenPaths. (11 de 02 de 2021). *Mecanismos de ciberseguridad para el día a día.* Obtenido de Telefónica:https://empresas.blogthinkbig.com/mecanismos-ciber seguri d ad-dia -a-dia/

Ernst & Young. (2012). *Prevención de Fugas de Información Soluciones DLP – Data Loss Prevention.* Obtenido de http://www.and orratelecom.a d/c/documen t_library/get_file ?uuid=28 bc3e82-0a1f-44f8-a688-1909deb3f363&groupId=10156

ESIC, B., & Marketing, S. (2020). Definicion de la ciberseguridad y su riesgo. *ESIC Business & Marketing School.*

Espinosa, D., Martínez, J., & Amador, S. (2014). Gestión del riesgo en la seguridad de la información con base en la norma ISO/IEC 27005. *Ing. USBMed*.

González Fajardo, D. (21 de 01 de 2021). *La nube marca la diferencia en el teletrabajo de las instituciones financieras*. Obtenido de COBIS, Financial Activity Partners: https://blog.cobiscorp.com/billeteras-digitales-e-wallet-0

González, R. (14 de 01 de 2021). *Teletrabajo (V): ¿cómo se mantendrá en el sector financiero?* Obtenido de Sage Advice, consejos sobre actualidad empresarial: https://www.sage.com/es-es/blog/teletrabajo-v-como-se-mantendra-en-el-sector-financiero/

Gutiérrez Amaya, H. C. (14 de 05 de 2013). *MAGERIT: metodología práctica para gestionar riesgos*. Recuperado el 12 de 06 de 2021, de Welivesecurity by EseT: https://www.welivesecurity.com/la-es/2013/05/14/magerit-metodologia-practica-para-gestionar-riesgos/

ISOTools, E. (05 de 10 de 2015). *Cómo implantar eficazmente la norma ISO 27005.* Recuperado el 03 de 07 de 2021, de PLATAFORMA TECNOLÓGICA PARA LA GESTIÓN DE LA EXCELENCIA: https://www.isotools.org/2015/10/05/como-implantar-eficazmente-la-norma-iso-27005/

Kaspersky, A. (2021). *¿Qué es la ciberseguridad?* Recuperado el 19 de 06 de 2021, de Kaspersky: https://latam.kaspersky.com/resource-center/definitions/what-is-cyber-security

Kowask Bezerra, E., Alcántara Lima, F., Motta, A. C., & Boca Piccolini, J. D. (2014). Gestión del Riesgo de las TI NTC 2705. *Escuela Superior de redes - RED CEDIA*, 220. Obtenido de https://cedia.edu.ec/dmdocuments/publicaciones/Libros/GTI9.pdf

López Argüello, M. E. (2013). *La cultura en seguridad de la información y su relación con la confidencialidad en UNIFINSA de la ciudad de Ambato.* Obtenido de http://repositorio.uta.edu.ec/bitstream/123456789/3661/1/TMGF004-2013.pdf

Lzzia, K. (2021). *Ciberseguridad en el teletrabajo: un desafío 4.0*. Obtenido de CCN, Call Center News: https://www.callcenternews.com.ar/aldea-digital/1702-cbt4

Mejía, R. (15 de 06 de 2018). Tips tecnológicos, de configuración y negocio que complementan tu seguridad. *Blog Smartekh*. Obtenido de https://blog .smartekh.co m/qu e-es-la-triada-de-seguridad-o-cia-triad-y-por-que-deberia-interesarte

MinTIC. (2008). *El teletrabajo*. Recuperado el 23 de 06 de 2021, de Ministerio de Tecnologías de la Información y las Comunicaciones: https://teletraba jo.gov.co/62 2/w3 -article-8228.html

OISS. (07 de 2020). INFORME SOBRE EL. *Organización Iberoamericana de Seguridad Social*. Obtenido de https://oiss.org/wp-content/uploads/2020/07/INFORME-SOBRE-EL-TELETRABAJOTRABAJO-NO-PRESENCIAL.pdf

Perez Vera, Ocampo Botello, & Sánchez Pereza. (2015). Aplicación de la metodología de la investigación para identificar las emociones. *Revista Iberoamericana para la Investigación y* .

Pulido Polo, M. (01 de 09 de 2015). Ceremonial y protocolo: métodos y técnicas de investigación científica. *Opción, 31*(1), 1137 - 1156. Recuperado el 15 de 03 de 2019, de https://www.redalyc.org/pdf/310/31043005061.pdf

Pulido Polo, M. (2015). Ceremonial y protocolo: métodos y técnicas de investigación científica. *Red de Revistas Científicas de América Latina, el Caribe, España y Portugal*. Obtenido de https://www.redalyc.org/pdf/310/31043005061.pdf

Quishpe Reinoso, V. P. (2007). *Definición e implementación de un modelo de respaldos de información en la compañía Transelectric SA.* Obtenido de http://bibdigi tal.epn.edu. ec/bitstream/15000/1475/1/CD-0990.pdf

Raffino, M. E. (14 de 06 de 2021). *Justificación de un proyecto*. Recuperado el 26 de 06 de 2021, de Concepto.de: https://concepto.de/justificacion-de-un-proyecto/

Rekalde Rodríguez, I., Vizcarra Morales, M. T., & Macazaga López, A. M. (2014). La observación como estrategia de investigación para construir contextos de aprendizaje y fomentar procesos participativos. *Educación XX1: Revista de la Facultad de Educación*. Obtenido de http://www.red alyc.org/articul o.oa?id=70629 509009

Rock, D. (12 de 03 de 2018). ¿Qué es la “Tríada CID” o el “Triángulo de la Seguridad”? *INFORMÁTICA, LENGUAJES DE PROGRAMACIÓN, SISTEMAS Y REDES, SQL*. Obtenido de https://donnierock.com/2018/03/12/que-es-la-triada-cid-o-el-triangulo-de-la-seguridad/

Rodríguez Jiménez, A., & Pérez Jacinto, A. O. (01 de 03 de 2017). Métodos científicos de indagación y de construcción del conocimiento. *Revista EAN*. Obtenido de https://doi.org/10.21158/01208160.n82.2017.1647

Rojas Urgilés, J. L., & Vela Veintimilla, J. J. (2011). *Planificación estratégica y plan de seguridad informática de Fabril Fame S. A.* Obtenido de http://reposi torio.espe.edu. ec/bitstream/21000/5167/1/T-ESPE-033137.pdf

Rubio, F. (09 de 05 de 2020). *¿Qué es y para qué sirve la ciberseguridad?* Recuperado el 19 de 06 de 2021, de ExpacioWeb Digital Marketing: https://www.exp acioweb.c om/qu e-es-y-para-que-sirve-la-ciberseguridad/

Solis, J. J. (16 de 07 de 2018). *4 tendencias en seguridad para la tecnología bancaria*. Obtenido de Cobis, Financial Activity Partenrs: https://blog. cobiscorp.co m/tendencia s-seguridad-tecnologia-bancaria-gfmi

Tamayo y Tamayo, M. (2018). *El Proceso de la Investigación Científica.* Mexico: Imusa S. A,. Obtenido de https://es.scribd.com/doc/12235974/Tamayo-y-Tamayo-Mario-El-Proceso-de-la-Investigacion-Cientifica

Tapeiro Tapeiro, H. A., & Suarez Ramirez, H. (2017). Modelo de gestión de riesgos de la seguridad de la información en empresas del sector asegurador utilizando la Norma ISO/IEC 27005. *Universidad Distrital Francisco José de Caldas*, 101. Obtenido de https://repository.udistrital.edu.co/bitstream/handle/11349/8322/TapieroTapieroHa winAndrei2019.pdf?sequence=1&isAllowed=y

Viu. (23 de 03 de 2021). *Por qué es importante la ciberseguridad*. Recuperado el 19 de 06 de 2021, de Universidad Internacional de Valencia: https://www.unive rsidadviu.co m/pe /actualidad/nuestros-expertos/por-que-es-importante-la-ciberseguridad

Walkowski, D. (31 de 07 de 2019). ¿Qué es la tríada de la CIA? *TechTarget, S.A de C.V*. Obtenido de https://searchdatacenter.techtarget.com/es/opinion/Que-es-la-triada-de-la-CIA

ANEXOS

Encuesta dirigida al personal técnico de la cooperativa de Ahorro y Crédito Oscus Ltda.

https://www.questionpro.com/a/SurveyPreview

Pontificia Universidad Católica del Ecuador | Sede Ambato

MECANISMOS DE CIBERSEGURIDAD EN DISPOSITIVOS DE TELETRABAJO PARA UNA INSTITUCIÓN FINANCIERA

OSCUS
Solidez que apoya tu crecimiento

ENCUESTA DIRIGIDA AL PERSONAL TÉCNICO DE LA COOPERATIVA DE AHORRO Y CRÉDITO OSCUS LTDA.

Objetivo: La presente encuesta tiene como objetivo la obtención de información para analizar el impacto de amenazas, riesgos y vulnerabilidades en el ambiente de teletrabajo.

Start

¿Cree usted que la cooperativo Oscus maneja un control de riesgo adecuado con respecto al personal que realiza teletrabajo?

- ○ Si
- ○ No
- ○ Desconozco el manejo de control de riesgo

De las siguientes opciones ¿Cuál cree usted que es una amenaza al momento de realizar teletrabajo?

- ☐ Ataques de *Phishing*
- ☐ Falsas Actualizaciones / parches
- ☐ Herramientas de software fraudulentas
- ☐ Perdida de Información
- ☐ Ataque de Denegación de Servicio
- ☐ Correos electrónicos desconocidos
- ☐ Ataques de *Ransomware*
- ☐ Infiltración de *Keyloggers*
- ☐ Ataques de Ingeniería Social
- ☐ *Scams* en productos o servicios
- ☐ Ataques por *SQL Inyection*
- ☐ Varios usuarios conectados a la misma red WiFi

Si la amenaza llegara a ocurrir, ¿Cuál cree usted que sería el departamento que debería dar solución?

- [ ] Seguridad Integral
- [ ] Tecnología de la Información (TI)
- [ ] Riegos
- [ ] Operaciones

Al momento de realizar teletrabajo ¿Cuál cree usted que es la o las vulnerabilidades que pueden generar un mayor riesgo tanto para los dispositivos de teletrabajo como para la Institución?

- [ ] Uso de VPN (Acceso a equipos mediante escritorio remoto)
- [ ] Ingresar a links de dudosa procedencia
- [ ] Acceso a redes inalámbricas libres y desconocidas
- [ ] -- Content Blocked --
- [ ] Manipulación / acceso de correos basura o fraudulentos (spam)
- [ ] Utilizar de forma irresponsable las aplicaciones corporativas
- [ ] Facilitar información relevante a terceros
- [ ] Utilizar contraseñas seguras para los aplicativos
- [ ] Antivirus desactivado y/o desactualizado
- [ ] Desconocimiento por parte de los usuarios a ataques de ingeniería social

Done