UNIVERSIDAD TECNOLÓGICA ISRAEL

ESCUELA DE POSGRADOS "ESPOG"

MAESTRÍA EN SEGURIDAD INFORMÁTICA

Resolución: **RPC-SO-02-No.053-2021**

PROYECTO DE TITULACIÓN EN OPCIÓN AL GRADO DE MAGÍSTER

Título del proyecto:
INFLUENCIA DE LA GESTIÓN Y COMPORTAMIENTO DE USUARIOS EN EL CONTROL DE LA SEGURIDAD DE LA INFORMACIÓN EN PYMES
Línea de Investigación:
SEGURIDAD INFORMÁTICA
Campo amplio de conocimiento:
TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN
Autor:
Fernando Javier Pérez Vega
Tutor:
Msc. Pablo Recalde

Quito – Ecuador

2023

APROBACIÓN DEL TUTOR

Yo, Pablo Marcel Recalde Varela con C.I: 1711685055 en mi calidad de Tutor del proyecto de investigación titulado: **INFLUENCIA DE LA GESTIÓN Y COMPORTAMIENTO DE USUARIOS EN EL CONTROL DE LA SEGURIDAD DE LA INFORMACIÓN EN PYMES**.

Elaborado por: **Fernando Javier Pérez Vega**, con C.I:1716225436, estudiante de la Maestría: **EN SEGURIDAD INFORMÁTICA**, de la **UNIVERSIDAD TECNOLÓGICA ISRAEL (UISRAEL)**, como parte de los requisitos sustanciales con fines de obtener el Título de Magister, me permito declarar que luego de haber orientado, analizado y revisado el trabajo de titulación, lo apruebo en todas sus partes.

Quito D.M., marzo de 2023

Firmado electrónicamente por:
PABLO MARCEL
RECALDE VARELA

_____

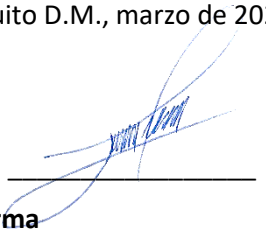
Firma

DECLARACIÓN DE AUTORIZACIÓN POR PARTE DEL ESTUDIANTE

Yo, Fernando Javier Pérez Vega, con C.I: 1716225436, autor del proyecto de titulación denominado: Influencia de la Gestión y Comportamiento de Usuarios en el control de la seguridad de la información en pymes. Previo a la obtención del título de Magister en Seguridad Informática.

1. Declaro tener pleno conocimiento de la obligación que tienen las instituciones de educación superior, de conformidad con el Artículo 144 de la Ley Orgánica de Educación Superior, de entregar el respectivo trabajo de titulación 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. Manifiesto mi voluntad de ceder a la Universidad Tecnológica Israel los derechos patrimoniales consagrados en la Ley de Propiedad Intelectual del Ecuador, artículos 4, 5 y 6, en calidad de autor@ del trabajo de titulación, quedando la Universidad facultada para ejercer plenamente los derechos cedidos anteriormente. En concordancia suscribo este documento en el momento que hago entrega del trabajo final en formato impreso y digital como parte del acervo bibliográfico de la Universidad Tecnológica Israel.
3. Autorizo a la SENESCYT a tener una copia del referido trabajo de titulación, con el propósito de generar un repositorio que democratice la información, respetando las políticas de prosperidad intelectual vigentes.

Quito D.M., marzo de 2023



Firma

ORCID: 0000-0003-0628-107X

Tabla de contenidos

Índice de tablas

Índice de figuras

INFORMACIÓN GENERAL

Contextualización del tema

De acuerdo con el centro National Initiative for Cybersecurity Careers and Studies (NICCS, 2019), de los Estados Unidos, la ciberseguridad se define como «la actividad o proceso, capacidad o estado mediante el cual los sistemas de información, comunicaciones y la información contenida en ellos están protegidos o defendidos contra daños, uso no autorizado o modificación». Los sistemas cibernéticos y de red involucran al menos cuatro componentes: usuarios de sistemas informáticos, analistas de sistemas de seguridad, atacantes cibernéticos y sistemas informáticos. Los atacantes cibernéticos a menudo intentan usar técnicas clave para ayudar a aumentar la seguridad cibernética y mitigar el impacto de la ingeniería social y los métodos de piratería cognitiva.

La mayor parte de la investigación sobre ciberseguridad se ha centrado en mejorar los sistemas de redes informáticas, ya que muchos creen que los avances en tecnología y el desarrollo de software es la principal forma de aumentar la seguridad de la información. Sin embargo, se han realizado menos estudios sobre la mejora de las políticas de gestión de usuarios y la conciencia situacional de los analistas de sistemas.

Según (Rodriguez, 2020), las empresas pequeñas o medianas (PYMES) actualmente representan el sector de más rápido crecimiento y generan una cantidad significativa de empleo. A pesar de esto, las pymes aún enfrentan muchos obstáculos, particularmente en lo que respecta a la tecnología y seguridad informática, convirtiéndolas en blanco fácil para piratas informáticos.

Problema de investigación

Los atacantes cibernéticos también pueden manipular las mentes de los usuarios del sistema informático, en lugar de un sistema informático en sí mismo, por ejemplo, utilizando ingeniería social (engañando a los usuarios del sistema informático para obtener información, como contraseñas) y piratería cognitiva (difusión de información errónea) para entrar en una red o sistema informático, Según (Bowen, et al., 2018), los ataques de ingeniería social representan el 28 % del total de los ataques de ciberseguridad y el 24 % de estos ataques se produjeron debido a la suplantación de identidad. Según Cyber Edge Reports, más del 70 % de los ataques de ingeniería social han tenido éxito en los últimos años. En los informes de 2018 y 2019 de la empresa de telecomunicaciones Telstra, publicados en su sitio (Telstra.com, 2018-2019) los errores humanos son la mayor amenaza en ciberseguridad. Los informes afirman que

los ataques de phishing fueron los ataques más comunes y utilizaron ingeniería social parcial y fraude para estafar a las víctimas para que instalen malware o ingresen a sitios web ilegítimos para adquirir sus credenciales. En este tipo de ataques, las víctimas a menudo reciben correos electrónicos o mensajes de texto que parecen ser, por ejemplo, para una actualización de software, correspondencia legítima de un proveedor externo, información sobre una multa, crisis actual, notificaciones de un banco o un sitio de redes sociales. Según estos informes también se identificaron que entre los errores frecuentes de los usuarios de sistemas informáticos en ciberseguridad están compartir contraseñas y no instalar actualizaciones de software.

Es importante señalar que existen diferencias individuales entre los usuarios de sistemas informáticos en cuanto al cumplimiento de los comportamientos de seguridad. Varios estudios encontraron que las diferencias individuales en la procrastinación, la impulsividad, el pensamiento futuro y los comportamientos de toma de riesgos pueden explicar las diferencias para el cumplimiento de las políticas de ciberseguridad. También hay que destacar que, dados los errores humanos existentes que pueden afectar la seguridad de la red, se discutirá el uso de métodos didácticos para mejorar el cumplimiento de las políticas de seguridad. Dichos métodos didácticos incluyen el uso de nuevas advertencias de seguridad polimórficas, recompensar y penalizar el comportamiento informático bueno y malo, y aumentar el pensamiento sobre las consecuencias futuras de las acciones, esto apoyado en la implementación de normativas de gestión de usuarios.

¿Cómo llevar una adecuada gestión, basada en el comportamiento de los de usuarios, que permita minimizar los riesgos de seguridad informática?

Objetivo general

Analizar la influencia de la gestión y el comportamiento de usuarios en el control de la seguridad de la información en las pymes.

Objetivos específicos

- Ejemplificar los errores de seguridad informática mediante casos de estudio, de los usuarios de sistemas informáticos, para tener un punto de partida del análisis
- Investigar las normas de seguridad de la información, mediante un proceso documental, para guiar la implementación de políticas de gestión de usuarios en pymes.
- Clasificar métodos que podrían usarse, para minimizar los errores humanos que generan inseguridad, según normativas y estudios de seguridad de la información.

Vinculación con la sociedad y beneficiarios directos:

De acuerdo a los ODS cuyas siglas significan: Objetivos de Desarrollo Sostenible de las Naciones Unidas este trabajo se alinea al ODS 9, puesto que, la implementación de las tecnologías explicadas en este proyecto contribuirá a las pymes con innovación en seguridad informática para hacerlas más competitivas y menos vulnerables optimizando sus consumos en tecnología y energía.

CAPÍTULO I: DESCRIPCIÓN DEL PROYECTO

El presente capítulo describe el contexto del proyecto, facilita su entendimiento y referencia los métodos investigativos utilizados.

1.1. Contextualización general del estado del arte

Existen numerosos estudios de ciencias de la computación, sin embargo, los estudios del comportamiento centradas en el error del usuario informático pueden proporcionar técnicas clave para ayudar a aumentar la seguridad cibernética y mitigar el impacto de la ingeniería social y los métodos de piratería cognitiva (la difusión de información falsa) de los atacantes. En consecuencia, en este trabajo, se centra la investigación sobre los rasgos y las diferencias individuales entre los usuarios de sistemas informáticos frente a las políticas de Gestión de Usuarios, que explican las vulnerabilidades a los ataques y a ser propensos, en mayor o menor rango, a ser víctimas de delitos de seguridad cibernética.

Los usuarios de sistemas informáticos poseen diferentes niveles de preparación informática que determinan su capacidad para contrarrestar las amenazas a la seguridad de la informática, ante ello una correcta gestión de usuarios por parte de los administradores de los sistemas es determinante para evitar los más frecuentes errores que generan riesgos para la información de las pymes. Con la ayuda de casos de estudio se va a identificar las brechas más comunes de seguridad y definir métodos para ayudar a los usuarios y administradores de sistemas informáticos a cumplir con las políticas de seguridad y, por lo tanto, aumentar la seguridad de la infraestructura de redes y de los archivos digitales de información.

1.2. Proceso investigativo metodológico

Investigación Bibliográfica

(Cázares, 2010), conceptualizó a la investigación bibliográfica como: la recopilación, consulta y análisis de documentos que se utilizan como fuentes o referencias de un proceso investigativo. Este tipo de investigación permite realizar comparaciones entre distintos estudios y publicaciones de diferentes autores y aportes científicos.

Método inductivo

El enfoque inductivo, llamado otras veces como pensamiento inductivo, inicia con la observación y las conclusiones se plasman en el final del proceso investigativo y se manifiestan como un efecto de la observación. La investigación inductiva según (Bernard, 2011), el método inductivo envuelve la indagación de patrones partiendo de la observación, hasta generar

definiciones o teorías, partiendo de una serie de hipótesis. El investigador tiene la capacidad de alterar el camino del estudio en cualquier momento y no se establecen hipótesis al inicio del estudio.

Vale mencionar sobre la metodología inductiva, que esta no involucra omitir teorías al enunciar hipótesis u objetivos del proceso investigativo, sino más bien busca generar significados partiendo de datos recopilados para establecer una teoría. Según (Saunders, 2012), el pensamiento inductivo parte de aprender de la experiencia. Mediante la observación de patrones, que se asemejen en la experiencia, para formular conclusiones o una teoría.

1.3. Análisis de resultados

La protección de datos confidenciales, la propiedad intelectual y la información personal, es el objetivo principal del control de acceso y del control de usuarios. Como parte del marco de seguridad contemporáneo de confianza cero, es una parte fundamental para garantizar que solo los usuarios autorizados cuenten con accesos a una red. Las organizaciones corren el riesgo de fuga de datos de fuentes internas y externas si no cuentan con procedimientos sólidos para control de acceso.

Controlar el acceso a los datos, aplicaciones y recursos tanto en entornos locales como en la nube es fundamental para las empresas que utilizan arquitecturas de nube híbrida o multi nube. El inicio único de sesión (SSO) y la administración de acceso pueden proteger estos entornos del acceso no administrado y en el caso de empresas que apliquen la política BYOD (Bring Your Own Device) se torna aún más indispensable restringir el acceso a ciertos recursos y aplicaciones.

CAPÍTULO II: PROPUESTA

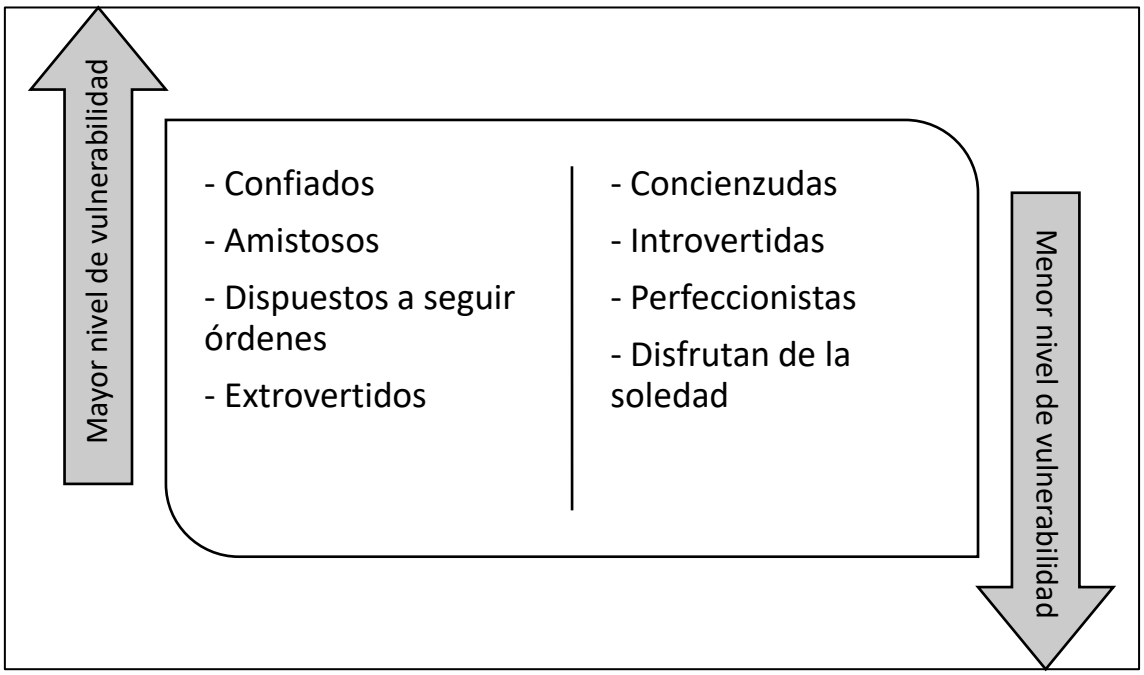
1.1. Fundamentos teóricos aplicados

Cumplir con las políticas de seguridad es un comportamiento clave para proteger la red y los sistemas. Ha habido pocos estudios sobre el nivel acatamiento de las normas de seguridad. La falta de acatamiento de las políticas de ciberseguridad puede socavar significativamente la seguridad de la información (West, 2019). Por ejemplo, varios estudios han demostrado que los usuarios de sistemas informáticos a menudo ignoran las advertencias de seguridad (Gary Brase, 2019)

Para medir los comportamientos de seguridad de tales humanos, (Egelman & Peer, 2020) desarrollaron la escala de Intenciones de Comportamiento de Seguridad. La escala mide las actitudes hacia la elección de contraseñas, la seguridad del dispositivo, la actualización periódica del software y la conciencia general sobre los ataques de seguridad. La encuesta tiene 16 preguntas, tales como: (a) utiliza una contraseña/código de acceso para desbloquear el computadora portátil o tableta, (b) cuando se me solicita una actualización de software, la instala de inmediato, (c) bloquea manualmente su pantalla de la computadora cuando se aleja de ella, y (d) si descubre un problema de seguridad, continúa con lo que estaba haciendo porque asume que alguien más lo arreglará. La escala en sí representa aspectos muy básicos de los métodos de protección y mitigación de la ciberseguridad por parte de los usuarios. Varios estudios han utilizado esta escala para medir los tipos de errores de seguridad cometidos por los usuarios del sistema informático. El incumplimiento de una política de seguridad puede ir más allá de ignorar advertencias, elegir malas contraseñas o no adoptar las medidas de seguridad recomendadas, ya que también depende de la apertura que exista por parte de los administradores de la gestión de los usuarios o de la inexistencia de políticas adecuadas.

Figura 1.

Nivel de vulnerabilidad a ser víctimas de ingeniería social según los rasgos de personalidad



Nota: Creación propia, basado en declaraciones de La Dra. Margaret Cunningham, investigadora del comportamiento humano en Forcepoint X-Labs.

1.2. Descripción de la propuesta

Estudios han demostrado que el factor humano es considerado la mayor vulnerabilidad a la seguridad, lo que sigue también ha sido confirmado por informes recientes. Un informe estimó que el 95 % de los ataques cibernéticos y de red se deben a errores humanos (Nobles, 2018). En este contexto, aunque gran parte de las exploraciones en esta área se concentran en los errores cometidos por los usuarios de sistemas informáticos se puede deducir que los empleados de la empresa son el eslabón más débil para garantizar la seguridad del sistema.

Algunos errores humanos relacionados con la seguridad cibernética y de redes incluyen, entre otros, compartir contraseñas, compartir información en exceso en las redes sociales, acceder a sitios web sospechosos, usar medios externos no autorizados, hacer clic indiscriminadamente en enlaces, reutilizar las mismas contraseñas en varios lugares, abrir un archivo adjunto de una fuente no confiable, enviar información confidencial a través de redes móviles, no proteger físicamente los dispositivos electrónicos personales y no actualizar el software. En este sentido, uno de los principales problemas que subyace en la información y la ciberseguridad es el dilema de aumentar la disponibilidad y la facilidad para acceder a una red o datos, pero al mismo tiempo, mantener la seguridad (Vekseler, et al., 2020). Para aumentar la

seguridad, las organizaciones a menudo establecen políticas basadas en normas, que requieren que los usuarios del sistema informático tengan contraseñas complejas, con periodos de caducidad o con doble factor de acceso, lo para los usuarios es una condición que dificulta la usabilidad, pero que disminuye las probabilidades de vulnerabilidad. Los usuarios de sistemas informáticos, sin embargo, tienden a tomar el camino de menor resistencia, como usar una contraseña débil y usar la misma contraseña para varios sitios si es que no existen políticas y controles establecidos para evitar que esto ocurra. A continuación, analizamos estudios previos sobre tres tipos de errores de seguridad humana: ser víctima de phishing, compartir contraseñas con otros e instalar actualizaciones de software.

Ser víctima del phishing: algunos estudios de phishing han utilizado un experimento de phishing en laboratorio. En otro estudio se demostró que el uso de experimentos de phishing en laboratorio se relaciona con el phishing de la vida real (Hakim, 2020). Un estudio encontró que más del 30% de los empleados del gobierno hacen clic en un enlace sospechoso en este correo electrónico de phishing, y muchos de ellos proporcionaron sus contraseñas (Baillon, 2019). En otro estudio que utilizó un experimento de phishing similar, alrededor del 60% de los estudiantes universitarios hicieron clic en un enlace sospechoso en un correo electrónico de phishing (Diaz, Sherman, & Joshi, 2019). En consecuencia, varios estudios sugieren que los factores humanos, los estudios de comportamiento deben tenerse en cuenta en los estudios de seguridad informática y de redes. En otro estudio, (Bowen, et al., 2018), estudió cómo el personal académico y los alumnos de la Universidad de Columbia responden a los correos electrónicos de phishing y descubrió que las personas tardaron alrededor de 4 rondas en descubrir que estaban recibiendo correos electrónicos de phishing.

Un estudio reciente también encontró que un ataque de phishing exitoso está relacionado con los rasgos de la tríada oscura de los usuarios de computadoras, incluidos el maquiavelismo, el narcisismo y la psicopatía (Curtis, et al., 2021). En este estudio se encontró que puntuaciones altas en narcisismo se relacionan con una mayor tendencia a ser víctima de intentos de phishing.

Además de ser víctimas de ataques de phishing, los usuarios de sistemas informáticos también cometen otros errores de ciberseguridad, como:

Compartir contraseñas: compartir contraseñas con amigos y familiares, e incluso con extraños, es un ejemplo frecuente de errores de seguridad cibernética humana. Según (Whitty, et al., 2020), los adultos mayores que obtienen un puntaje alto en perseverancia y autocontrol tienen más probabilidades de compartir contraseñas. Compartir contraseñas suele ser

problemático, ya que la mayoría de las personas a menudo usan las mismas contraseñas para varios sitios web y, por lo tanto, al compartir una contraseña, otros pueden acceder a su otra información segura. Un problema con el uso de la misma contraseña en muchos sistemas es que los ciberdelincuentes, una vez que encuentran estas contraseñas en un sistema, pueden usarlas en muchos otros sitios web.

Instalación de actualizaciones de software: un error común que subyace a los comportamientos de ciberseguridad es un retraso en la instalación de actualizaciones de software o incluso la no instalación de estas. Usando un estudio experimental de toma de decisiones de comportamiento, (Rajivan, et al., 2020)encontraron que los comportamientos de toma de riesgos pueden explicar en parte los comportamientos de algunas personas con respecto a la instalación de actualizaciones de software, de modo que las personas que corren más riesgos tienden a retrasar la instalación de actualizaciones de software. A diferencia de compartir contraseñas y phishing, el área de instalación de actualizaciones de software no ha recibido mucha atención en el campo.

Las diferencias individuales en los conductuales están relacionadas con los comportamientos de seguridad cibernética. (Dawson & Thomsom, 2018) argumentan que las diferencias individuales en las habilidades cognitivas y los rasgos de personalidad pueden desempeñar un papel clave en el éxito para asegurar los sistemas informáticos y de información. A continuación, se presentan algunos de estos rasgos.

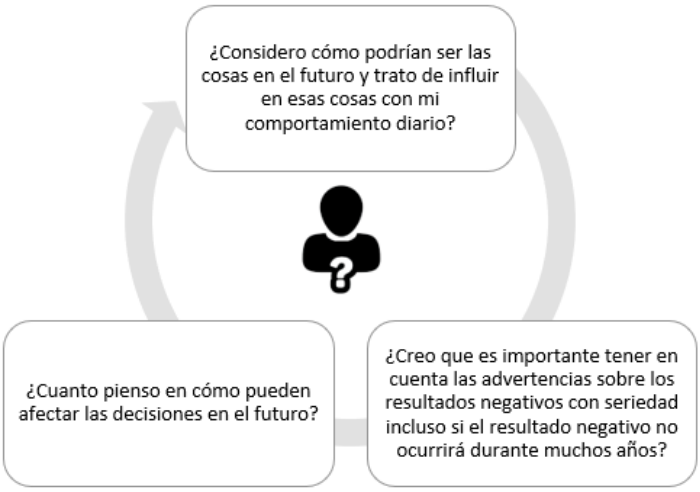
Procrastinación: cumplir con las políticas de seguridad posiblemente esté relacionado con procesos cognitivos, como trabajar duro para lograr ciertas metas. Una escala, conocida como la escala de "necesidad de cognición", mide trabajar duro, disfrutar y participar en actividades que requieren esfuerzo y pensamiento (Lin, et al., 2016). En esta línea, (Egelman & Peer, 2020) encontraron que el desempeño en la Escala de Intenciones de Comportamiento de Seguridad está relacionado con la Necesidad de Cognición (NFC), que se refiere a la inclinación a ejercer esfuerzos cognitivos. Además, utilizando la escala de Estilo General de Toma de Decisiones (GDMS), encontraron que el desempeño en la Escala de Intenciones de Comportamiento de Seguridad está relacionado con la procrastinación, de modo que las personas que procrastinan tenían menos probabilidades de seguir las políticas de seguridad. Esto es plausible ya que la procrastinación se correlaciona negativamente con la participación en actividades.

Impulsividad: el cumplimiento de las políticas de seguridad también puede estar relacionado con las diferencias individuales en los comportamientos impulsivos. (Egelman &

Peer, 2020) encontraron que el desempeño en la Escala de Intenciones de Comportamiento de Seguridad está relacionado con las puntuaciones de la Escala de Impulsividad. Otro estudio encontró que la adicción a Internet y la impulsividad predicen comportamientos cibernéticos riesgosos (Hadlington, 2019). En esta línea, encontraron que las diferencias individuales en el autocontrol y el control cognitivo (una característica clave de los comportamientos impulsivos) están relacionadas con la violación de las políticas de seguridad de la información. (Wiederhold, 2018) también encontró que las personas son víctimas de ataques de ciberseguridad en la búsqueda de una gratificación inmediata. Una característica clave relacionada con la impulsividad es no pensar en las consecuencias futuras de las acciones realizadas (por ejemplo, ahorrar dinero ahora para comprar una casa en el futuro, frente a gastar todo el dinero ahora para disfrutar de la vida).

Pensamiento futuro: Es importante destacar que el cumplimiento de las políticas de seguridad también puede estar relacionado con el pensamiento sobre el futuro, así como el impacto de las acciones presentes en las consecuencias futuras. En otras palabras, las personas que piensan más en el futuro pueden cumplir con las reglas de seguridad para asegurarse de que su sistema informático esté seguro en el futuro. En este contexto, (Egelman & Peer, 2020) encontraron que el desempeño en la Escala de Intenciones de Comportamiento de Seguridad está relacionado con la Consideración de Consecuencias Futuras (CFC). Esta escala incluye ítems que son muy relevantes para los comportamientos de seguridad cibernética, que se resumen en la siguiente gráfica:

Figura 2.
Factores relevantes en el pensamiento futuro



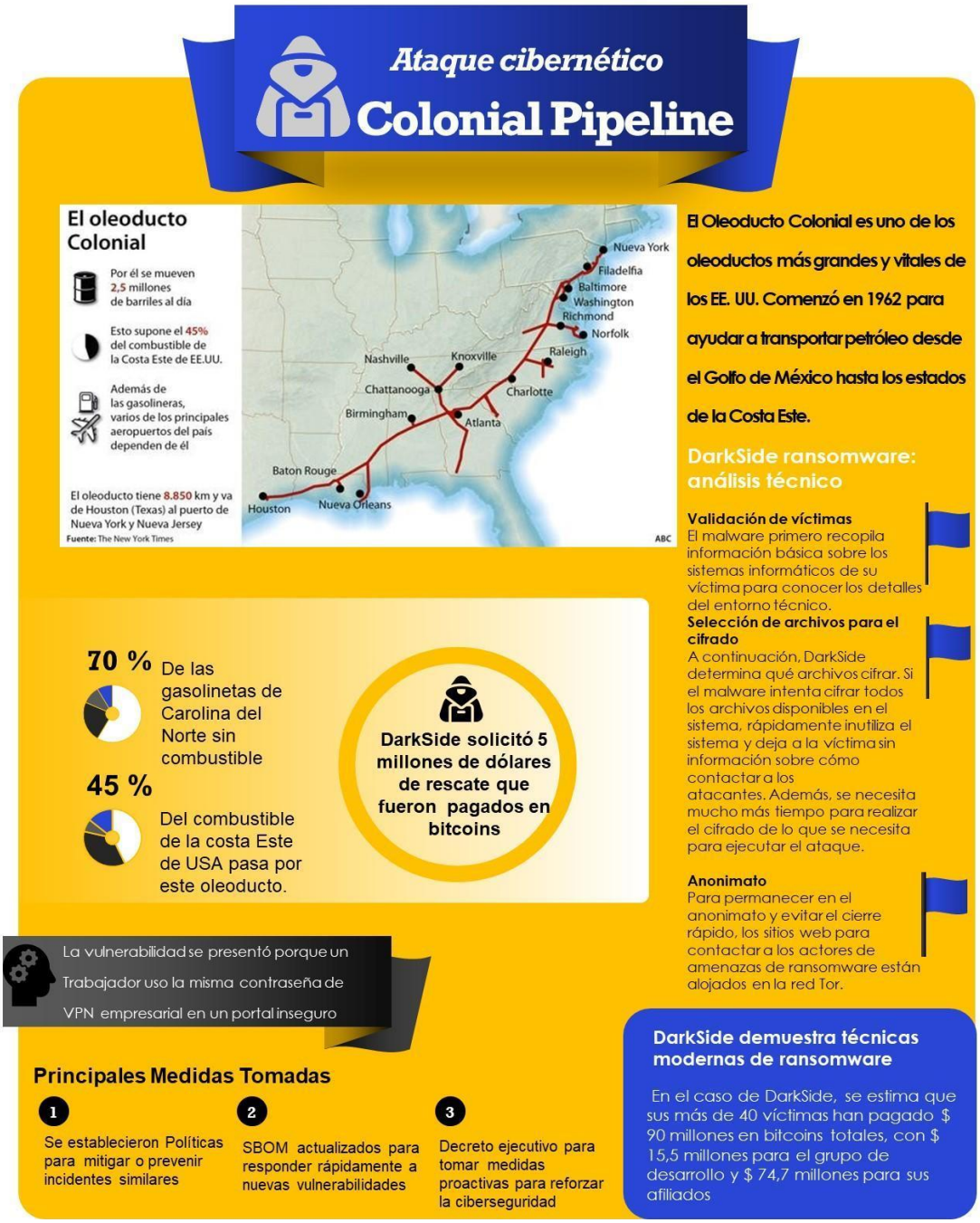
Nota: Creación propia basada en: Consideraciones Futuras (Egelman & Peer, 2020)

Comportamientos de asunción de riesgos: otro rasgo de personalidad relacionado con la ciberseguridad son los comportamientos de asunción de riesgos. Algunos estudios han encontrado que los usuarios de sistemas informáticos que asumen muchos riesgos pueden ser más propensos a ser víctimas de delitos cibernéticos (Henshel, et al., 2019). El riesgo se define como participar en un comportamiento con un resultado incierto, generalmente con el fin de obtener más. Por ejemplo, robar un banco es arriesgado, ya que uno puede ser atrapado. El incumplimiento o ausencia de las políticas de seguridad es riesgoso y el único beneficio que el usuario encuentra, es no hacer ningún trabajo adicional, como la actualización del software, pero el riesgo es ser víctima de delitos cibernéticos y phishing. Otro ejemplo es descubrir que ha habido una violación de datos en la que la información de carácter personal, como nombres de usuario y contraseña, se han visto comprometidas, pero luego no se ha hecho nada para cambiar las contraseñas. El conflicto que tienen los usuarios de sistemas informáticos es realizar trabajo adicional para proteger la red o sus sistemas informáticos lo que asegura, mucho trabajo, pero más seguro o no realizar trabajo adicional en ciberseguridad, lo que representa, menos trabajo, pero menos seguro. Es importante destacar que (Egelman & Peer, 2020) encontraron que el desempeño en la Escala de Intenciones de Comportamiento de Seguridad Informática está relacionado con comportamientos generales de asunción de riesgos en la vida cotidiana. En estudios realizados, mediante el uso de la Escala de Comportamientos de Ciberseguridad Riesgosa, la Escala de Intenciones de Comportamientos de Seguridad (SeBIS) y las Actitudes hacia la ciberseguridad y el ciberdelito en los negocios (ATC-IB), Sobre esto, (Hadlington, 2019) encontró que la multitarea de medios pesados se asocia con comportamientos de seguridad cibernética riesgosos y mayores errores.

El sesgo de optimismo está relacionado con la aceptación de decisiones con riesgo explicito. Generalmente, las personas asumen que les pasará lo mejor, y no creen que estén en riesgo (West, 2019), es decir, los usuarios tienden a ser más optimistas y descartan la probabilidad de que les sucedan eventos negativos. Por ejemplo, las personas generalmente descartan la probabilidad de ser víctimas de phishing, que es una práctica fraudulenta mediante el envío de correos electrónicos, mensajes, llamadas u otros medios, que pretenden ser reales para inducir a las personas a revelar información privada. Esto es relevante para la investigación sobre la ciberseguridad y la seguridad de las redes, ya que los usuarios de sistemas informáticos tienden a descartar el impacto de los ataques cibernéticos o los delitos que les suceden. Por ejemplo, un estudio encontró que las personas son víctimas de ataques de ciberseguridad debido al sesgo de optimismo (Wiederhold, 2018).

Como ejemplo en la gráfica siguiente presentamos el caso del ataque al oleoducto Colonial Pipeline, que causó pérdidas millonarias y que se dio por un error humano en el manejo de contraseñas.

Figura 3.
Ataque cibernético Colonial Pipelin



Nota: Creación propia basado en noticias de The New York Times.

Otro caso ejemplo, esta vez localmente, es el ocurrido con la Corporación Nacional de telecomunicaciones CNT, donde se cree que un empleado abrió un correo que contenía un ransomware.

Figura 4.

Ataque cibernético CNT

Nota: Creación propia basada en video de rueda de prensa de CNT

a. Estructura general

Tabla 1

Implementación de la propuesta basada en ISO 27001:2013, Anexo A9

Control de Acceso	**Requisitos comerciales de control de acceso**	Política de control de acceso
		Acceso a redes y servicios de red
	Gestión de acceso de usuarios	Alta y baja de usuarios
		Aprovisionamiento de acceso de usuario
		Gestión de derechos de acceso privilegiado
		Gestión de la información de autenticación secreta
		Revisión y eliminación de los derechos de acceso
	Responsabilidades del usuario	Uso de información de autenticación secreta
	Control de acceso a sistemas y aplicaciones	Restricción de acceso a la información
		Procedimientos de inicio de sesión seguro
		Sistema de gestión de contraseñas
		Uso de programas de utilidad privilegiados
		Control de acceso al código fuente del programa
Estrategias o Técnicas	**Recompensa**	Recompensas para aumentar el cumplimiento de las políticas de seguridad
	Penalización	Castigo o penalización ejemplificador de conducta
	Simuladores de ataques	Con conocimiento del usuario
		Sin conocimiento del usuario

Nota: Creación propia, basado en ISO 27001 y en estudios (Maqbool, et al., 2020)

b. Explicación del aporte

El proceso de gestión de usuarios está normado por varias entidades como el National Institute of Standards and Technology (NIST) y también por (Organización Internacional de Normalización, 2013) según esta última, el control de acceso del Anexo A.9 asegura que solo los usuarios con autorización tengan acceso a un servicio, mientras que las personas no autorizadas no pueden utilizarlo, de esta forma se pretende limitar los permisos que poseen los usuarios únicamente a lo que requieren para el desempeño laboral, evitando así que se comentan errores humanos involuntarios y cerrando puertas de inseguridad informática.

Por lo tanto, basado en la norma ISO 27001: se proporciona una explicación detallada de cada inciso del Anexo A.9, aplicable a Pymes.

Norma ISO 27001: Anexo A.9

Según la ISO 27001:2013 en su anexo 9, el control de acceso gestiona los controles para que las personas no autorizadas no puedan obtener accesos a la información y a las instalaciones donde se procesa la información, lo que resulta en un mal uso o pérdida de la información. La cláusula de control de acceso aborda estos problemas al permitirle controlar quién tiene acceso a estos activos.

La protección de los activos de información es crítica para todas las organizaciones, y el Anexo A.9 protege contra una variedad de riesgos, incluidos los daños no intencionales o la pérdida de información, el sobrecalentamiento, las amenazas, etc. Esto requiere una política y procesos de control definidos, así como el registro, la eliminación y la verificación de los derechos de acceso de los usuarios, lo que incluye el acceso físico, el acceso a la red, el control de las utilidades privilegiadas y la limitación del acceso al código fuente del programa.

Control de acceso

Un aspecto importante de la seguridad de la información es determinar, quienes son los que pueden acceder a utilizar la información de las instituciones. Para ello las políticas de control de acceso se encargan de garantizan que los responsables sean verificados y que accedan de forma adecuada a los datos de la organización a través de la autenticación y la autorización. Por otra parte, el acceso físico a las instalaciones y centros de datos, también se puede restringir con el uso del control de acceso.

Las contraseñas, los nombres de usuario, los PIN, la biometría y otros tipos de tokens de seguridad se pueden usar para identificar a un usuario en un sistema de control de acceso. Existe también la autenticación multifactor (MFA), que es una característica común de muchos sistemas de control de acceso, que requiere varias formas de identificación para autenticar a un usuario.

En el caso de que se hayan validado las credenciales y la dirección IP de un usuario, se puede otorgar a ese usuario el nivel adecuado de acceso y las acciones permitidas.

El control de acceso se puede dividir en cuatro categorías. Cuando se trata de seguridad y cumplimiento, las organizaciones tienden a adoptar el método que tiene más sentido para sus propias necesidades. Los cuatro tipos de control de acceso son los siguientes:

Tabla 2

Tipos de Control de Acceso

Tipo de control	Descripción
Control de acceso discrecional (DAC)	En DAC, la persona que posee o administra el sistema, los datos o los recursos protegidos decide quién tiene permiso para acceder a ellos.
Control de acceso obligatorio (MAC)	En este modelo no discrecional, a los usuarios se les permite el acceso en función de una autorización de información. Los privilegios de acceso están regulados por una autoridad central según los distintos niveles de seguridad. Por lo general, se utiliza en entornos gubernamentales y militares.
Control de acceso basado en roles (RBAC)	En lugar de otorgar acceso en función de la identificación de un usuario, RBAC ofrece acceso en función de funciones empresariales predefinidas. Los usuarios solo deben tener acceso a la información que sea relevante para sus trabajos en la organización. Los roles, las autorizaciones y los permisos constituyen la base de este enfoque de uso común.
Control de acceso basado en atributos (ABAC)	Con ABAC, tanto las personas como los recursos pueden controlar su acceso de acuerdo con un conjunto dinámico de cualidades y variables ambientales, como qué hora del día es y dónde se encuentran.

Nota: Creación propia, basado en ISO 27001

Anexo A.9.1: Requisitos comerciales de control de acceso

El objetivo de esta cláusula es establecer y poner en marcha procedimientos que restrinjan quién tiene acceso a tanto la información, como a las instalaciones donde se genera o almacena información. Se deben desarrollar políticas de control de acceso para cumplir con esta regulación.

A.9.1.1: Política de control de acceso

Es imprescindible definir, documentar y validar periódicamente la política de control de acceso con los requisitos normativos y de seguridad de la información que la acompañan. Para proteger sus activos, aquellos que son propietarios de la información con valor, deben establecer un control de acceso adecuado, derechos de acceso y restricciones de roles de usuario, con el volumen de información y la rigurosidad de los controles reflejando los riesgos de seguridad de la información que conllevan.

Al considerar los controles de acceso, es importante considerar tanto su razón como su valor. Debe haber una política clara de los requisitos comerciales que deben contener los controles de acceso para proveedores de servicios, usuarios internos y externos.

A.9.1.2 Acceso a redes y servicios de red

La red y los servicios de red que sean necesarios para el empleo del usuario deben estar restringidos a quienes necesiten acceder a ellos.

La política tiene que tratar a los distintos servicios de redes en el ámbito de acceso; procedimientos de autorización para indicar quién (basado en funciones) puede acceder a qué y cuándo; y control de gestión para prevenir o monitorear el acceso en el mundo real.

Anexo A.9.2: Gestión de acceso de usuarios

Esta cláusula busca garantizar que los usuarios autorizados puedan acceder a su sistema y servicios y, al mismo tiempo, impedir el acceso no autorizado.

A.9.2.1 Alta y baja de usuarios

Se debe oficializar el alta y baja de usuario. La capacidad de vincular identificaciones específicas con personas y limitar las identificaciones de acceso compartido debe ser parte de un procedimiento sólido de administración de identificaciones de usuarios, que debe aprobarse y registrarse cuando se haga.

Con el Anexo A.7 Seguridad de los recursos humanos como enlace, es posible un proceso de registro y cancelación sin problemas, al igual que evitar la concesión de identificaciones duplicadas. Para demostrar un fuerte control y reforzar la gestión continua, las identificaciones deben revisarse periódicamente. Junto con esto, se pueden utilizar auditorías de control de acceso y evaluaciones periódicas por parte de los propietarios de activos de información o aplicaciones de procesamiento.

A.9.2.2 Aprovisionamiento de acceso de usuario

Los propietarios de sistemas o servicios de información deben otorgar o revocar el acceso a sus sistemas o servicios de acuerdo con este proceso. Al asegurarse de que el acceso concedido sea importante para la función que se está realizando, y se debe evitar que estos accesos se concedan sin todas las autorizaciones respectivas.

Es crucial que el acceso de los usuarios esté impulsado por el negocio y se adecue a las necesidades de la organización. Sin embargo, esto puede sonar burocrático, pero no tiene por qué serlo, y los procedimientos básicos efectivos con acceso basado en roles pueden abordar esto.

A.9.2.3 Gestión de derechos de acceso privilegiado

El acceso especial a datos y sistemas requiere controles estrictos sobre quién los obtiene y cómo se utilizan debido al poder adicional que otorga a la persona que lo posee. La claridad sistema por sistema sobre los permisos de acceso privilegiado (que se pueden modificar dentro del programa) podría entrar en esta categoría, así como la asignación basada en el uso real en lugar de una política general.

Todos los privilegios otorgados a los usuarios deben documentarse y actualizarse permanentemente los privilegios de los usuarios a los que se otorgan los permisos, para garantizar que puedan desempeñar sus responsabilidades asignadas.

También es una buena idea mantener identidades separadas para los administradores del sistema y los usuarios habituales, especialmente si realizan varios trabajos en el mismo entorno.

A.9.2.4 Gestión de la información de autenticación secreta de los usuarios

El acceso a activos importantes se otorga mediante el uso de información de autenticación secreta. Cuando se trata de información confidencial como contraseñas o claves

de cifrado, debe administrarse a través de un proceso estructurado y mantenerse privado para su usuario.

La identidad del usuario debe verificarse antes de proporcionar cualquier información de autenticación, ya sea esta una clave nueva, un reinicio o una clave temporal. Cuando se configura un nuevo sistema, cualquier información de autenticación secreta predeterminada debe modificarse lo más rápido posible.

A.9.2.5 Revisión de los derechos de acceso de los usuarios

Los propietarios de activos deben realizar auditorías periódicas de los derechos de acceso de los usuarios, tanto para cambios individuales (como incorporación, cambios de funciones y salidas) como para auditorías más amplias de acceso al sistema.

Es esencial que los permisos de acceso privilegiado se evalúen con mayor frecuencia debido a su naturaleza de alto riesgo. Las auditorías internas, como esta, deben efectuarse al menos anualmente, excepto si se producen cambios significativos.

A.9.2.6 Eliminación o ajuste de derechos de acceso

Todos los accesos a la información y a las infraestructuras de procesamiento de la información deben revocarse luego de la terminación del empleo, contrato o acuerdo, como se especifica en el párrafo anterior (o ajustarse al cambiar de función, si es necesario).

Cuando los empleados se van, una política y procedimientos de salida efectivos que se vinculen con A.7 ayudarán a garantizar que se cumpla este objetivo y se pueda verificar con fines de auditoría.

Anexo A.9.3: Responsabilidades del usuario

El propósito aquí es responsabilizar a los usuarios de garantizar que su información de autenticación no se vea comprometida. Esta técnica requiere que el personal siga las instrucciones para usar las credenciales de autenticación secretas.

A.9.3.1 Uso de información de autenticación secreta

La autenticación secreta debe mantenerse privada; las personas no autorizadas no deben tener acceso a él; y, si hay alguna indicación de que puede haber sido comprometida, la información debe cambiarse de inmediato.

Además, debe alentar a los usuarios a elegir contraseñas seguras que cumplan con los requisitos mínimos del Anexo A.9.4 para la longitud y la seguridad de la contraseña.

Anexo A.9.4: Control de acceso a sistemas y aplicaciones

El objetivo de esta subcláusula es contar con sistemas para evitar el acceso no deseado a sus sistemas y aplicaciones de información.

A.9.4.1 Restricción de acceso a la información

El uso de las funcionalidades del sistema de información y aplicaciones debe estar regulado de acuerdo con la política de control de acceso de la empresa. El control de acceso debe aplicarse de conformidad con la política de control de acceso establecida y en función de los requisitos de la aplicación comercial. Para acceder a los estándares de restricción, tenga en cuenta lo siguiente:

- Controlar el acceso a las funcionalidades del sistema de aplicaciones a través de menús.
- Limitar los datos a los que tiene acceso un usuario específico.
- Privilegios de acceso de usuario, como lectura, escritura, eliminación y control de ejecución.
- controlar los derechos de acceso de otras aplicaciones.
- Reducir la cantidad de datos en las salidas.
- Control de acceso físico o lógico para aislar aplicaciones confidenciales, datos de aplicaciones y sistemas del resto de la red.

A.9.4.2 Procedimientos de inicio de sesión seguro

El usuario debe poder autenticar su identidad a través de un procedimiento de inicio de sesión seguro antes de poder acceder a los sistemas y aplicaciones. Se pueden usar autenticación multifactor, biometría, tarjetas inteligentes y otras formas de encriptación en lugar de contraseñas, según el riesgo.

La información de autenticación debe transmitirse y almacenarse en forma cifrada para evitar la intercepción y el uso indebido de la información.

El Centro Nacional de Seguridad Cibernética (NCSC), así como las pautas ISO 27002, son importantes en esta área. Aquí hay algunos consejos más:

- Para evitar la interceptación y el uso indebido, los métodos de inicio de sesión deben construirse de manera que no se pueden violentar fácilmente.
- También debe haber una advertencia de que el acceso está restringido a aquellos que están autorizados.

- Para ofrecer pruebas forenses, tanto los inicios y cierres de sesión exitosos como los fallidos deben registrarse de forma segura, y deben considerarse las notificaciones de intentos fallidos y bloqueos sospechosos.
- Según el sistema, es posible que sea necesario restringir el acceso a horas específicas del día o días, o incluso a ubicaciones específicas.

Cuando se trata de protocolos de inicio y cierre de sesión, las exigencias del negocio y la información en riesgo deben ser las principales consideraciones, hay que mediar entre la funcionalidad y la seguridad, ya que el usuario no puede hacer bien su trabajo si pasa una cantidad de tiempo desproporcionada en procesos de acceso.

A.9.4.3 Sistema de gestión de contraseñas

Esto ayuda a evitar que se utilice el mismo inicio de sesión en varios sitios al proporcionar un método centralizado para la generación y administración de contraseñas.

La implementación de sistemas de generación y gestión de contraseñas debe hacerse con cuidado, como con cualquier otro mecanismo de control, para proporcionar niveles de seguridad aceptables y proporcionados. Las contraseñas deben ser creadas por el usuario siempre que sea posible, pero deben cumplir con un nivel particular de seguridad para que sean lo suficientemente seguras para que el usuario las recuerde sin dificultad.

A.9.4.4 Uso de programas de utilidad privilegiados

Los controles en el sistema y las aplicaciones deben monitorearse cuidadosamente en busca de programas informáticos de utilidad que tengan el potencial de anularlos.

Los atacantes malintencionados pueden aprovechar los potentes programas de utilidades de sistema y red, por lo que solo un pequeño número de usuarios debería tener acceso a ellos.

Los usuarios deben estar limitados en su capacidad para instalar cualquier software en la medida de lo posible, teniendo en cuenta los requisitos de la empresa y la evaluación de riesgos al utilizar dichos programas de utilidad fácilmente disponibles en Internet. Para cumplir con los requisitos del auditor, el uso de programas públicos debe documentarse y monitorearse, revisarse periódicamente.

A.9.4.5 Control de acceso al código fuente del programa

Deben imponerse restricciones al acceso al código fuente del programa. Debe haber fuertes controles sobre quién tiene acceso al código fuente del programa.

Si el código fuente de un programa no está debidamente protegido, un atacante tiene una gran oportunidad de obtener acceso al sistema de manera encubierta. Esto es crítico sobre todo si el código fuente contiene detalles fundamentales para la operación de la empresa.

c. Estrategias para minimizar el error humano

El uso de nuevas advertencias de seguridad polimórficas: según estudios (Anderson, et al., 2019), (West, 2019) , la mayoría de las personas ignoran las advertencias de seguridad en Internet debido a la habituación, es decir, no se presta atención a los objetos que vemos; también se argumentó que la mayoría de los mensajes de advertencia son similares a otros diálogos de mensajes. En consecuencia, los usuarios de sistemas informáticos a menudo los ignoran, ya que es probable que no se muestre una respuesta de asignación atencional novedosa a tales advertencias de seguridad (Moustafa, et al., 2020).

El uso de diferentes advertencias de seguridad polimórficas a lo largo del tiempo ayudará a aumentar la atención a estas advertencias. En esta línea, (Anderson, et al., 2019) encontró que el uso de advertencias polimórficas no condujo a la habituación, es decir, los usuarios del sistema informático aún pueden prestar atención y responder a estas advertencias de seguridad. Responder a actividades nuevas y anómalas son aspectos de la conciencia situacional y clave para detectar intentos de phishing en sistemas cibernéticos o de red. Los ingenieros de software deben desarrollar advertencias de seguridad que capten la atención y no cuadros de diálogo de mensajes estándar, y estos también deben cambiar con el tiempo para aumentar el estado de alerta y la atención en los usuarios del sistema informático. El uso de mensajes de seguridad únicos y novedosos es importante, ya que las investigaciones han informado que estos mensajes pueden aumentar la activación cerebral y los procesos de atención (Moustafa, et al., 2020)

Además, otros estudios han comparado las diferencias en el diseño de las advertencias de seguridad entre los navegadores Firefox, Google e Internet Explorer, (Akhawe & FELT, 2018) encontraron que las advertencias de seguridad del navegador pueden ser mecanismos de seguridad efectivos, aunque hubo una serie de variables importantes que contribuyen a las tasas de clics después de las advertencias, incluido el tipo de advertencia, la cantidad de clics, la apariencia de la advertencia, la fijación de certificados y el tiempo dedicado a las advertencias.

Las personas a menudo están motivadas para realizar ciertas acciones para recibir una recompensa y evitar resultados negativos (Moustafa, et al., 2020). Sin embargo, en el caso de los comportamientos de ciberseguridad, la recompensa es que no pasará nada malo; es decir, el sistema informático del usuario no será atacado si se cumplen las políticas de seguridad.

En otras palabras, cumplir con los comportamientos de ciberseguridad, es un ejemplo de refuerzo negativo, en el que realizar las acciones establecidas en las políticas de seguridad informática, previenen la ocurrencia de un resultado negativo.

En resumen: recompensa y penalización del cumplimiento o no, de las políticas de seguridad informática de los usuarios, calificándolos como bueno o malo, sería aplicable como en la vida cotidiana, que se aprende de los resultados negativos o positivos.

1.3. Validación de la propuesta

Es responsabilidad de los administradores de sistemas, implementar, gestionar y dar seguimiento al acatamiento de las reglas de seguridad de la información aprobadas para cada empresa. Según la investigación realizada la norma ISO 27001:2013 en su anexo A9, cumple con dar los lineamientos para una correcta gestión de accesos a los usuarios de sistemas de información, pero esta gestión no estará completa si no existe el compromiso de la alta Gerencia para utilizar métodos de concienciación, penalización y recompensa a los usuarios de acuerdo con los informes de riesgos detectados para cada usuario. Es aquí donde se conjugan los conceptos de las normas con la realidad de la aplicación y cumplimiento de las políticas por parte de los usuarios de sistemas informáticos y de ello depende la viabilidad de esta propuesta.

Existen hallazgos que certifican que el uso de recompensas puede aumentar el cumplimiento de la política de seguridad que debe estar establecida. Por ejemplo, las empresas deberían imponer multas, un aprendizaje de castigo, a los empleados que no se adhieren a las políticas de seguridad y recompensar a los que sí lo hacen. (Maqbool, et al., 2020)argumentaron que penalizar a las personas debería aumentar los comportamientos de seguridad. Un experimento de phishing realizado por ESET (2021) en el que los voluntarios a sabiendas de que se trataba de un experimento hacen clic en un enlace que luego les pide que proporcionen sus contraseñas, permitió identificar que la experiencia simulada con phishing puede afectar el comportamiento futuro, descubriendo que experimentar phishing simulado, aumenta el porcentaje de desempeño las políticas de seguridad de información, en los usuarios del sistema informático a futuro.

Se ha descubierto también, que proporcionar información sobre la prevalencia del phishing, es decir, los resultados negativos que pueden ocurrir a las personas pueden disminuir

los clics en enlaces sospechosos en los correos electrónicos de phishing (Baillon, 2019). En consecuencia, los usuarios de los sistemas informáticos deben recibir una experiencia simulada de los resultados negativos que pueden ocurrir debido a las acciones de seguridad informática que realizan y que son consideradas inseguras.

Pensar cada vez más en las consecuencias futuras de las acciones, como se mencionó anteriormente, está relacionado con la toma de decisiones, la planificación y puede disminuir los comportamientos impulsivos, lo que está relacionado con los comportamientos de riesgo en la web (Bowen, et al., 2018). En consecuencia, el uso de métodos didácticos para aumentar el pensamiento sobre las consecuencias futuras de las acciones puede ayudar a aumentar la toma de decisiones reflexivas y, por lo tanto, mejorar los comportamientos de seguridad informática.

1.4. Matriz de articulación de la propuesta

Tabla 3.

Matriz de articulación

EJES O PARTES PRINCIPALES	SUSTENTO TEÓRICO	SUSTENTO METODOLÓGICO	ESTRATEGIAS / TÉCNICAS	DESCRIPCIÓN DE RESULTADOS	INSTRUMENTOS APLICADOS
Ingeniería Social y piratería cognitiva, phishing, malware	Riesgos de seguridad informática	Investigación Bibliográfica	Analizar conceptos		NICCS 2019
Niel de vulnerabilidad de los usuarios	Grado en el que un usuario es en mayor o menor medida vulnerable.	Investigación Bibliográfica	Analizar informes	FIGURA 1	Informe Forcepoint X-Labs.
Cumplimiento de Políticas de seguridad	Directrices que garantizan la seguridad de la información	Investigación Bibliográfica	Analizar estudios	FIGURA 2 y 3	Escala de Intenciones de Comportamiento de Seguridad
Control de acceso	Determina quienes son los que pueden acceder a utilizar la información	Investigación Bibliográfica	Analizar normas	TABLA 2	ISO 27001:2013, Anexo A9
Gestión de usuarios	Garantiza que solo los usuarios autorizados puedan acceder a su sistema y servicios	Investigación Bibliográfica	Analizar normas	TABLA 1	ISO 27001:2013, Anexo A9
Estrategias o Técnicas	Advertencias Polimórficas, Penalización y Recompensa, Simuladores de ataques	Investigación Bibliográfica	Analizar estudios	TABLA 1	

Nota: Elaboración propia

CONCLUSIONES

Como se discutió anteriormente, existen diferentes tipos de errores humanos que pueden socavar los sistemas informáticos y de seguridad, incluido el intercambio de contraseñas, el intercambio excesivo de información en las redes sociales, el acceso a sitios web sospechosos, el uso de medios externos no autorizados, el clic indiscriminado en enlaces, la reutilización de las mismas contraseñas en múltiples lugares, usar contraseñas débiles, abrir un archivo adjunto de una fuente no confiable, enviar información confidencial a través de redes móviles, no proteger físicamente los dispositivos electrónicos personales y no actualizar el software. Sin embargo, la mayor parte de la investigación realizada muestra que los errores humanos se han centrado en su mayoría en el acceso a correos electrónicos de phishing y en contraseñas compartidas.

Esta investigación muestra que algunos rasgos de comportamiento, como la impulsividad, la asunción de riesgos y la falta de pensamiento sobre las consecuencias futuras de las acciones, están relacionados con la falta de cumplimiento de las políticas de seguridad informática y que una correcta gestión de usuarios y el establecer en base a normas la política de «confianza cero» limita a los usuarios a cometer menos errores y por consiguiente tener menos brechas en la seguridad informática.

Algunos métodos pueden aumentar los comportamientos a favor de la seguridad, como recompensar y penalizar los comportamientos relacionados con la seguridad, usar nuevas advertencias de seguridad, usar métodos de capacitación para aumentar el pensamiento sobre las consecuencias futuras de las acciones e implementar políticas de seguridad, dichos métodos junto a otros como el entrenamiento de los usuarios, se pueden utilizar para disminuir los riesgos de seguridad informática.

La implementación de las metodologías explicadas en este proyecto contribuirá a las industrias con innovación e infraestructuras más seguras, para hacerlas más competitivas, favoreciendo a los Objetivos de Desarrollo Sostenible definidos por las Naciones Unidas

RECOMENDACIONES

Una investigación futura debe inquirir las diferencias individuales y el entorno laboral, por ejemplo: estado de ánimo, urgencia en el trabajo, trabajo bajo presión o multitarea; que generan otros tipos de errores de seguridad informática.

Otra investigación futura podría centrarse en desarrollar una metodología de pruebas para integrar los rasgos de los usuarios y los procesos cognitivos relacionados con los comportamientos de seguridad informática y de red en un solo marco. Esta metodología de pruebas debe incluir los procesos cognitivos mencionados anteriormente, incluida la impulsividad, la asunción de riesgos y el pensamiento sobre las consecuencias futuras de las acciones.

Por otra parte, si bien existen algunas normas como la ISO 27001, que establecen mecanismos de control de usuarios, también existen herramientas informáticas, como SIEM (Security Information and Event Manager) o UEBA (User and Entity Behavior Analytics) que aplicados a la ciberseguridad pueden usarse para predecir el comportamiento de los atacantes o usuarios del sistema informático, algunos de estos utilizan modelos de redes neuronales para detectar ataques de ingeniería social y también se apoyan en inteligencia artificial, por ello sería de gran utilidad analizar los beneficios de la implementación de estas herramientas en entornos empresariales.

BIBLIOGRAFÍA

Akhawe, D., & FELT, A. (2018). Alicia en el país de las advertencias: un estudio de campo a gran escala sobre la eficacia de las advertencias de seguridad del navegador. *Simposio de Seguridad de USENIX.*

Anderson, et al. (2019). Cómo las advertencias polimórficas reducen la habituación en el cerebro: conocimientos de un estudio de fmri.

Baena, G. (2015). *Metodología de la investigación.* Grupo Editorial Patria.

Baillon, A. (2019). Información, simulación de experiencia, o ambas: un experimento de campo sobre los riesgos de phishing.

Bernard, H. (2011). *Métodos de investigación en antropología: enfoques cualitativos y cuantitativos.*

Bowen, et al. (2018). *Medir el factor humano de la seguridad cibernética.* 2018 IEEE International Conference on Technologies for Homeland Security (HST).

Cázares, L. (2010). *Técnicas actuales de investigación documental.* Universidad de Texas.

Curtis, et al. (2021). La Tríada Oscura y el control de recursos estratégicos en un juego de computadora competitivo.

Dawson, J., & Thomsom, R. (2018). a futura fuerza laboral de ciberseguridad: ir más allá de las habilidades técnicas para un desempeño cibernético exitoso. *Frontiers in psychology*.

Diaz, A., Sherman, A., & Joshi, A. (2019). Phishing en una comunidad académica: un estudio de la susceptibilidad y el comportamiento del usuario. *Taylor & Francis Online*.

Egelman, S., & Peer, E. (2020). Escalando el muro de seguridad desarrollando una escala de intenciones de comportamiento de seguridad. *Security Feedback & Warnings CHI*.

Gary Brase, E. V. (02 de 11 de 2019). Los diferentes modelos mentales influyen en el comportamiento de ciberseguridad.

Hadlington, L. (2019). Factores humanos en ciberseguridad; examinar el vínculo entre la adicción a Internet, la impulsividad, las actitudes hacia la seguridad cibernética y los comportamientos de seguridad cibernética de riesgo.

Hakim, Z. (2020). a prueba de sospecha de correo electrónico de phishing (PEST) es una tarea de laboratorio para evaluar los mecanismos cognitivos de detección de phishing.

Henshel, et al. (2019). La confianza como factor humano en la evaluación holística del riesgo de ciberseguridad. *Procedia Manufacturing*.

Lin, et al. (2016). Ansiedad matemática, necesidad de cognición y estrategias de aprendizaje en cursos de métodos de investigación de comunicación cuantitativa. *Communication Quarterly*.

Maqbool, et al. (2020). Ciberseguridad: efectos de penalizar a los defensores en juegos de ciberseguridad a través de la experimentación y el modelado computacional. *Frontiers in Psychology*.

Moustafa, et al. (2020). Efecto de la mejor autointervención posible sobre la motivación situacional y el compromiso en el contexto académico. *Learning and Motivation*.

NICCS. (2019). *INICIATIVA NACIONAL DE CARRERAS Y ESTUDIOS DE CIBERSEGURIDAD*. Obtenido de https://niccs.cisa.gov/cybersecurity-career-resources.

Nobles, C. (2018). Maltratando los factores humanos en la ciberseguridad en las organizaciones empresariales. *HOLISTICA–Journal of Business and Public Administration*.

Organización Internacional de Normalización. (2013). *ISO 27001*. Obtenido de iso.org: https://www.iso.org/isoiec-27001-information-security.html

Rajivan, et al. (2020). ¿Actualizar ahora o más tarde? Efectos de la experiencia, el costo y la preferencia por el riesgo en las decisiones de actualización. *Journal of Cybersecurity*.

Rodriguez, R. (2020). *Las PYMES en Ecuador. Un análisis necesario.*

Saunders, M. L. (2012). *Métodos de investigación para estudiantes de negocios.* Pearson Education Limited.

Telstra.com. (2018-2019). *Telstra.com*. Obtenido de Telstra.com.

Vekseler, et al. (2020). Simulaciones en ciberseguridad: una revisión del modelado cognitivo de atacantes, defensores y usuarios de la red.

West, R. (2019). *La psicología de la seguridad: por qué los buenos usuarios toman malas decisiones.* Communications of the ACM.

Whitty, et al. (2020). Diferencias individuales en los comportamientos de seguridad cibernética: un examen de quién comparte contraseñas.

Wiederhold, B. (2018). El papel de la psicología en la mejora de la ciberseguridad. *Ciberpsicología. Comportamiento* .

ANEXOS

Anexo 1. Aprobación de la propuesta por un especialista

Quito, 27 de febrero del 2023

Señores:

Universidad Israel

ESCUELA DE POSGRADOS "ESPOG"

Presente. -

Por medio del presente, yo **Carlos Mármol** con C.I.: 1712890043, de profesión Ingeniero en Telecomunicaciones, y Magister en Seguridad de la Información (UAX España), con cargo de **Oficial de Seguridad Informática del grupo empresarial Sudinco**, certifico que: tras haber realizado la lectura de la tesina titulada: **INFLUENCIA DE LA GESTIÓN Y COMPORTAMIENTO DE USUARIOS EN EL CONTROL DE LA SEGURIDAD DE LA INFORMACIÓN EN PYMES,** realizada por: **Fernando Javier Pérez Vega,** puedo dar fe de vialidad de la propuesta presentada y de que es aplicable al entorno empresarial.

Es todo lo que puedo argumentar en honor a la verdad, el interesado puede hacer uso del presente para los fines que considere convenientes.

Atentamente,

Carlos Mármol M.

Telf.: 099 657 6437

C.I.: 1712890043