Investigaciones Latinoamericanas en Ingeniería y Arquitectura

El *phishing* como amenaza en la ciberseguridad corporativa de grandes empresas

https://doi.org/10.51378/ilia.vi1.8496

A. L. Álvarez [1], J. A. Cruz [1], S. B. Cruz [1], J. de C. Gallardo [1], I. M. López [1], R. E. García [1]
1Departamento de Mecánica Estructural, Universidad Centroamericana José Simeón Cañas, UCA, El Salvador
E-mail: 00011621@uca.edu.sv

Resumen — **La ciberseguridad es un aspecto crítico en la era digital, y uno de los desafíos más recurrentes que enfrentan las empresas, en especial las grandes, son los ataques cibernéticos que buscan robar información valiosa. Estos ataques no solo representan una amenaza para la integridad de los datos, sino que también pueden causar daños económicos significativos y erosionar la confianza de los clientes. En esta investigación, el objetivo primordial es arrojar luz sobre una forma especialmente insidiosa de ciberataques dirigidos a las empresas, un eslabón aparentemente débil pero crítico en la cadena de seguridad cibernética. Comprender este fenómeno es esencial para prevenir estos ataques, ya que las empresas deben reconocer que a través de su personal pueden perder información crucial. Esta conciencia es fundamental para implementar medidas efectivas y proteger los activos digitales de la empresa.**

Palabras Clave – **ciberseguridad, daño económico, información valiosa**

Abstract — **Cybersecurity is a critical aspect in the digital age, and one of the most recurrent challenges facing companies, especially large ones, is cyberattacks aimed at stealing valuable information. These attacks not only pose a threat to data integrity but can also cause significant economic damage and erode customer trust. In this research, the primary objective is to shed light on a particularly insidious form of cyberattacks targeting companies, an ostensibly weak yet critical link in the cybersecurity chain. Understanding this phenomenon is essential for preventing these attacks, as companies must recognize that through their personnel, they can lose critical information. This awareness is crucial for implementing effective measures to safeguard the company's digital assets.**

Keywords — **cybersecurity, economic damage, valuable information**

I. INTRODUCCIÓN

Más del 90 % de todos los ataques y filtraciones de datos exitosos empiezan con una estafa de *phishing* [1], pero para comprender mejor ¿Qué es el *phishing*? El *phishing* es un método para engañar y hacer que comparta contraseñas, números de tarjeta de crédito, y otra información confidencial haciéndose pasar por una institución de confianza en un mensaje de correo electrónico o llamada telefónica [2], esto puede ser de una manera tan sencilla como descargar y abrir un documento o dar clic al enlace que ha sido enviado.

Desde el año 2020 los casos de *phishing* han incrementado potencialmente siendo esto una preocupación para los expertos, teniendo en cuenta que no todos los ataques terminan siendo exitosos y aquellos que si lo tienen, dejan resultados devastadores. “Las principales consecuencias, por orden de probabilidad son: pérdida de datos, ponen en compromiso cuentas y credenciales de acceso, Infecciones de *ramsonware* y/o *malware* y pérdidas financieras y fraudes por transacciones bancarias.” [3].

En los últimos 6 años los casos de *phishing* han incrementado de forma vertiginosa dentro de las grandes empresas volviéndose más agresivo y presentándose de nuevas maneras, ya que ahora cualquier persona que forma parte de la empresa puede ser si bien objetivo de este tipo de estafa pero no víctima, ya que a través de la concientización y actividades de formación en ciberseguridad se puede tener como resultado una disminución muy considerable en cuanto la susceptibilidad del *phishing* por lo tanto es de vital importancia que este las empresas tengan un plan de contingencia ante este tipo de estafa.

II. METODOLOGÍA

A. Objetivos

El objetivo principal de esta investigación es comprender una forma común de ataques cibernéticos dirigidos a individuos con el fin de obtener información de las empresas donde trabajan. La comprensión de este tema es fundamental para prevenir estos ciberataques y proteger la información sensible de las organizaciones y las personas afectadas.

Esto principalmente enfocado hacia las empresas grandes ya que, en estas empresas, estos ataques causan grandes daños, pérdidas económicas e incluso pierden la fidelidad de los clientes y se debe evitar esto. Las empresas deben reconocer que por medio del eslabón más débil (el personal de una empresa) pueden perder información importante y actuar de acuerdo a esto.

B. *Preguntas de investigación*

Estas preguntas de investigación se basan en el interés por conocer sobre el *phishing*, cómo esto afecta a las grandes empresas en la actualidad y por consecuente cómo evitarlo.

- ¿Por qué la ciberseguridad desempeña un rol importante dentro del correcto funcionamiento de la empresa?
- ¿De qué manera amenaza el *phishing* a la ciberseguridad corporativa de las grandes empresas?
- ¿Qué pueden hacer las grandes empresas para contrarrestar los ataques a la ciberseguridad ocasionados por el *phishing*?
- ¿Por qué el *phishing* es algo tan recurrente en las grandes empresas?

C. *Justificación*

El internet está al alcance de cualquier persona, esto incluye a los incontables ciberdelincuentes que se encuentran navegando por la red. Es por eso que hoy en día los ataques cibernéticos son muy frecuentes, la mayoría de las empresas no están conscientes de lo grave que puede llegar a ser este tipo de delito informático.

En este artículo se pretende conceptualizar y analizar uno en específico: el *phishing*. El *phishing* está haciendo estragos en las empresas de todo el mundo. El llamado BEC (Business Email Compromise por sus siglas en inglés) afectó a más del 90 % de las organizaciones de todo el globo durante el año pasado, según un informe de Proofpoint [4]. Se investigará sobre las formas más comunes de ataque y se darán a conocer las diferentes formas en la que este se difunde, las medidas para evitarlo y que una empresa no se vea afectada por este tipo de robo de identidad y no sufra las consecuencias que puede llegar a traer el no estar informado.

El resultado que se espera obtener en esta investigación es que el *phishing* sea reconocido y diferenciado, que las empresas o usuarios aprendan a detectar los sitios webs que son peligrosos y los podrían llevar a ser estafados, hacer un llamado a los lectores para proteger su empresa con ciberseguridad, de esta manera se evitará compartir datos, credenciales o toda información importante y confidencial de la empresa.

D. *Alcance*

Lograr obtener una definición clara y concisa del *phishing* definiendo los términos necesarios para poder comprender a su totalidad el tema, como a su vez hacer mención de las distintas formas de ataques que se pueden presentar y qué hacer en caso de ser víctima de este tipo de estafa. También estudiar los casos que han tenido mayor consecuencia en las grandes empresas como la historia y su evolución a través de los últimos años ya que el *phishing* ahora no está enfocado únicamente en los directores o usuarios que están en un alto cargo, actualmente cualquier persona que forma parte de la empresa puede ser víctima de dicho tipo de estafa.

¿Por qué el *phishing* es algo tan recurrente en las grandes empresas?, plantear lo anterior tomando en cuenta la vulnerabilidad, ciberseguridad y errores humanos que se presentan como a su vez abordar posibles soluciones y acciones concretas que se puede tomar para protegerse y erradicar dicha problemática. Lo anterior tomando en cuenta la problemática que el grupo ha planteado haciendo comparación mediante gráficos en donde se puede apreciar de manera cuantitativa cómo los casos de *phishing* se han hecho más recurrentes en los últimos años, haciendo hincapié en la pérdida de datos e información valiosa, y significando a su vez pérdida de incluso millones de dólares como disminución en la productividad.[23]

El aumento del *phishing* durante la pandemia por COVID-19 y la vulnerabilidad que tuvieron las empresas durante dicho periodo, haciendo análisis en la importancia de que el *phishing* sea un tema de alta importancia debido a las consecuencias que este podría tener, sugiriendo posibles acciones concretas a tomar en cuenta para poder proteger desde las credenciales de la persona hasta los datos de la empresa.[22]

III. MARCO TEÓRICO

Se puede comenzar con la definición de *phishing*, que según IBM (International Business Machines) es una forma de ataque electrónico, por medio de correo electrónico, mensajes de texto, llamadas o sitios web fraudulentos que está diseñado para que las personas descarguen *malware* o compartan información confidencial.[5] El *malware* es un programa maligno que se escribe para dañar o destruir sistemas informáticos o para ingresar sin autorización a algún sistema de interés. [5]

A. *Tipos de pishing*

Existen distintos tipos de *phishing* entre los cuales están los siguientes:

- Según el modus operandi

Whaling: el *whaling* o suplantación de identidad proviene de personas haciéndose pasar por una empresa, comúnmente por un jefe, por alguien de autoridad o ejecutivo importante de una institución importante, con fin de perseguir a alguna persona en específico de forma de robarle dinero, se hace creando un mensaje una historia muy realista que la víctima pueda creer.[6]

Spear phishing: es donde una persona, un hacker o estafador va en busca de una persona en particular, este envía un correo electrónico haciéndose pasar por alguna empresa. Se le envía un correo electrónico con el nombre, la posición, la institución, el número de teléfono de la empresa y demás datos de importancia dentro de una empresa de forma de hacerle creer que conoce a la víctima y así robarle

información confidencial para luego venderla en el mercado negro.[6]

Pharming: en el *pharming* el principal objetivo del hacker es apropiarse la identidad de alguien haciéndole entrar a un sitio web fraudulento por medio de algún correo electrónico o mensaje de texto, de forma de que el sitio web fraudulento es un sitio web del hacker preparado específicamente para que el usuario piense que está navegando en el sitio que desea, cuando en realidad está conectado al sitio web del hacker y así este último puede obtener la información suficiente para hacerse pasar por la víctima.[6]

Smishing [6]: es el *phishing* por SMS, que surge combinación de las palabras SMS y *phishing*. En el *smishing* se utilizan técnicas de ingeniería social por medio de mensaje de texto. El o los estafadores tratan de hacerle creer a la víctima que son de confianza como un contacto de un banco, para que le brinde los datos de su cuenta de bancaria por ejemplo para robarle la cuenta, a veces incluso le envían la autenticación en dos pasos para obtener acceso a la cuenta de banco de la víctima y robarle dinero. Este posee una variación que es el *wishing* que es el *smishing* por WhatsApp. [6]

- Según el servicio que ataquen

A bancos y cajas, por redes sociales, páginas web, soporte técnico, almacenamiento en la nube, servicios de mensajería, falsas ofertas, etc. [7]Algunas técnicas habituales de *phishing* son:

- Comunicación engañosa: estos saben cómo manipular a sus víctimas con mensajes engañosos.
- Sensación de necesidad: los usuarios se convierten en víctimas de *phishing* porque al recibir un mensaje con algún enlace de interés, sienten la necesidad de lo que el enlace contiene, por ejemplo si se recibe un enlace para armar un curriculum vitae y este es engañoso se puede estar entregando información personal a un cibercriminal.
- Falsa confianza: los cibercriminales engañan a su víctima creando un ambiente de falsa confianza para que estos les den información personal, así como incluso una tarjeta de crédito, por ejemplo
- Manipulación emocional: los cibercriminales usan técnicas de manipulación emocional para convencer a su objetivo.[8]

Dentro de una empresa, la ciberseguridad puede tener el mejor nivel de seguridad, mantenerse actualizando constantemente pero siempre el eslabón más débil va a ser el usuario final [8].

Según el informe "El factor humano 2022", en Estados Unidos las tentativas de *phishing* aumentaron más del doble en el último año [8].

Una de las principales empresas afectadas por *phishing* ha sido Microsoft, ya que alrededor de 1 de 4 correos de *phishing* enviados estaban asociados a la empresa Microsoft con el objetivo de robar credenciales, para así poder obtener información de utilidad. En empresas como esta lo que suele suceder es que un cibercriminal envía un link por correo electrónico o mensaje de texto a algún trabajador de esta empresa con el fin de que el trabajador abra el enlace y así, permitir al cibercriminal obtener información del dispositivo del trabajador, contraseñas, información confidencial que podría tener éste en el dispositivo y otros.

Además de esto suele suceder ataques a personas no específicas de una organización, a estas se las denominan como VAP (*Very Attacked People* por sus siglas en inglés). que son personas que ya han sido atacadas previamente y se les hace más sencillo a los cibercriminal atacarlos a ellos para obtener información. El 36 % de VAP son personas que se pueden encontrar en línea por medio de páginas web corporativas, redes sociales o publicaciones. Si se habla de empleados VIP que sean VAP el 23 % de la información de contacto se puede encontrar en internet.

Los cibercriminales suelen copiar la rutina de un empleado de la empresa para no ser detectados fácilmente al enviar los correos electrónicos en los mismos horarios donde se suelen recibir los correos electrónicos dentro de la empresa [9].

Sin embargo el *phishing* puede ser detectado y a pesar de ser el objetivo se puede evitar ser una víctima más en esta gran cadena. En caso de correos electrónicos:

Remitente. Los correos de tipo *phishing* en ocasiones contienen remitentes que no coinciden con la organización a la que supuestamente representan, este es el primer indicador que ha de comprobarse. Por ejemplo, un correo que supuestamente procede de una entidad bancaria tendría un remitente cuyo dominio coincidiría con la entidad a la que representa, si dicho dominio no coincide es un síntoma de fraude.

B. Fraude del CEO (spear phishing)

El *spear phishing* también muy conocido como fraude al CEO (chief executive officer) o BEC por sus siglas en inglés Business Email Compromise. Es un método empleado por ciberdelincuentes con el fin de realizar robos a los fondos de las compañías.

Esto a través de la suplantación de la identidad, haciéndose pasar por una persona que posee un cargo como alto directivo, el cual está dirigido a una víctima en específico que ya ha sido investigada anteriormente por múltiples medios (podrían ser redes sociales o las misma página web corporativa) de manera que este sea lo más realista posible para aumentar las posibilidades de que la persona caiga en la estafa.

Por lo tanto, en el *spear phishing* se tienen dos objetivos, una persona que tiene un cargo como alto directivo en la empresa y por otro lado otro un empleado con capacidad y acceso para realizar una transferencia bancaria el cual suele ser de un monto significativo ya que se da la excusa de ser una operación de cierre.

El medio por el cual se realiza normalmente es por correo electrónico y usando la misma táctica que el *phishing,* con la

ausencia de la persona que tiene cargo de alto mando con el fin de que se verifique la información, a través de este medio de comunicación se pide que confidencialidad y sea respondido urgentemente. De esta manera el empleado no comenta a otros compañeros y el fraude se puede realizar con concisión. Este tipo de *phishing* tiene como objetivos a las empresas de medianas y grandes.

Según el artículo *A review of phishing attacks and countermeasures for internet of things-based smart business applications in industry 4.0* [10], una de las recomendaciones que más se enfoca en las empresas es que el usuario debe mantenerse informado sobre las técnicas de *phishing*, ya que las diversas formas y maneras de estafar van evolucionando a lo largo del tiempo.[10]

C. Técnicas de concientización

Una manera muy viable para que los empleados se mantengan informados es dar capacitaciones sobre el tema, que implementen el conocimiento de ciberseguridad a estos mencionados anteriormente. Las actividades que pueden realizarse en las capacitaciones podrían ser: simulaciones de *phishing*, charlas que contengan información del tema, explorar las vías en las que puede propagarse. También se tiene la opción de hacerlo mediante actividades creativas como los juegos lúdicos, para que todos los empleados puedan convivir mientras aprenden jugando, esta técnica tiene el nombre de gamificación, básicamente consiste en convertir esta formación en un juego.

La necesidad de llevar a cabo la petición de manera urgente. La ingeniería social es el componente esencial en los correos electrónicos de tipo *phishing*. Los ciberdelincuentes suelen alertar a las víctimas sobre situaciones negativas a las que tendrán que hacer frente a no ser que sigan las instrucciones que facilitan, las cuales suelen ser acceder a una página web fraudulenta e introducir la información que solicitan, visualizar un archivo (malicioso), etc. Algunos de los ganchos más utilizados son la cancelación del servicio o cuenta, multas, sanciones por no acceder en tiempo y forma, etc. Son muchas las artimañas utilizadas cuyo fin es forzar al usuario a realizar una determinada acción a través de una coacción.

Durante la pandemia por el COVID-19 los ciberdelincuentes se adaptaron para utilizar señuelos basados en esta temática y cualquier aspecto que pudiera englobarse, como los ERTE, ayudas gubernamentales, remedios milagrosos, posibles sanciones, e incluso multas de tráfico cuando comenzaba la movilidad entre comunidades. Todos ellos fueron recopilados por INCIBE bajo la etiqueta #CiberCOVID19.

Ingresar a sitios web aleatorios y sin antes comprobar sus procedencias, ponen en riesgo la seguridad de la empresa.[11]

Enlaces falseados. Los enlaces ofuscados son una parte fundamental de este tipo de fraude. En la mayoría de las ocasiones es la vía esencial que utilizan los ciberdelincuentes para robar información confidencial.

Los enlaces suelen aparentar que corresponden a la web legítima o sencillamente contienen un texto haciendo referencia a que sea seleccionado o clicado. Para comprobar a donde apunta realmente el enlace, se puede situar el ratón encima y comprobar el cuadro de diálogo que figura en la parte inferior de la pantalla con la verdadera dirección. También se pueden utilizar herramientas online [11].

Se ha de tener especial cuidado al acceder a enlaces en correos electrónicos, siendo preferible acceder introduciendo la dirección web directamente en el navegador o utilizando la aplicación oficial de la entidad. Las entidades legítimas, como las financieras, nunca solicitarán a los clientes credenciales de acceso en comunicaciones por correo electrónico.

Comunicaciones impersonales. Las comunicaciones de entidades legítimas suelen referirse a su destinatario utilizando nombre y apellidos, por el contrario los ciberdelincuentes no suelen conocer esos datos personales por lo que las comunicaciones son impersonales. Recibir un mensaje procedente de una supuesta organización de la que se es cliente y que no contenga datos personales, como nombre y apellidos, es un síntoma de fraude.

Errores ortográficos y gramaticales. Una auténtica comunicación de cualquier entidad no contendrá errores ortográficos o gramaticales, ya que la comunicación con sus clientes es un aspecto muy cuidado.

Firmas y estética del correo. La estética y la firma del correo electrónico es otro factor a considerar. Cuando se está familiarizado con los correos de una determinada organización y una comunicación no sigue ese patrón, es un síntoma de fraude. [12]

Pero hay acciones concretas que se pueden realizar si se ha caído en este tipo de estafa. Lo primero es cambiar las credenciales de acceso más importantes, posteriormente analizar el ordenador o móvil con un programa antimalware por si queda algún rastro de *ransomware*.

Otras formas de protegerse del *phishing* son:

- Sospechar de los correos electrónicos que hagan llamado a dar clic inmediatamente hacia otras páginas sin mayor información adicional.
- Revisar al recibir correos electrónicos que sean páginas que ya le hayan enviado algún otro correo electrónico al cliente para así evitar la suplantación de identidad haciéndose pasar por alguna empresa.
- Ortografía y gramática: revisar ortografía y gramática del correo electrónico para así verificar que si esta fuera una empresa o entidad real no enviarán correos electrónicos con mala ortografía y gramática.
- Saludos genéricos: revisar que saluden por el nombre completo o alguna forma que no sea genérica por ejemplo evitar los correos electrónicos que empiezan con un “Estimado señor” o “Estimada señora”.
- Dominios de correos electrónicos: revisar que los dominios de correo electrónico sean de acuerdo a la institución de la que se recibe el correo.

- Vínculo sospechoso o datos adjuntos inesperados: si sospecha de un vínculo sospechoso o dato adjunto no los abra. [13]
-

D. *Evolución de ransomware*

El *ransomware* Maze, que entró en actividad a finales del año 2019, es el primer tipo de malware que ha operado de forma tal que la organización, detrás del mismo, no solo extorsiona a sus víctimas para devolver la operación a la normalidad, sino también para no divulgar la información secuestrada.

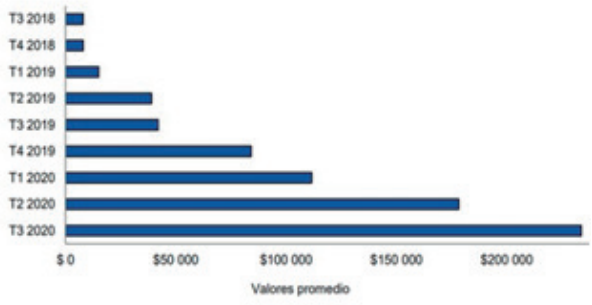

Fig. 1. Rescate promedio por trimestre [14]

IV. RESULTADOS

A. *Principales causas de incidentes de ciberseguridad*

Las principales causas de incidentes de ciberseguridad principio de funcionamiento de los ataques de ingeniería social es manipular psicológicamente a los usuarios, haciendo que revelen información confidencial para tomar medidas beneficiosas para los atacante, el *ransomware* infecta una máquina, encripta sus datos y muestra un aviso que le pide a la víctima que pague un rescate para desbloquear sus datos, la amenaza interna es un acto malicioso dirigido a una organización, ejecutado por el personal de la organización u otras personas a las que la organización ha otorgado deliberadamente acceso a sus sistemas y por último el ataque a la red tiene como objetivo obtener acceso no autorizado a la red de una empresa, para robar datos o realizar otras actividades maliciosas.

B. *Análisis de las causas de los incidentes*

Los incidentes de ciberseguridad, los tres principales vectores pertenecen a *phishing* con "31 % de casos, 30 % escaneo y explotación de vulnerabilidades, y 29 % robo de credenciales de acceso (Symantec, 2019). Es decir que el 60 % corresponden a debilidades que tienen origen en la preparación de las personas para el uso de la tecnología, ya sea por falta de reconocimiento de un email engañosos o por el uso de contraseñas débiles o iguales en múltiples sitios." [15]

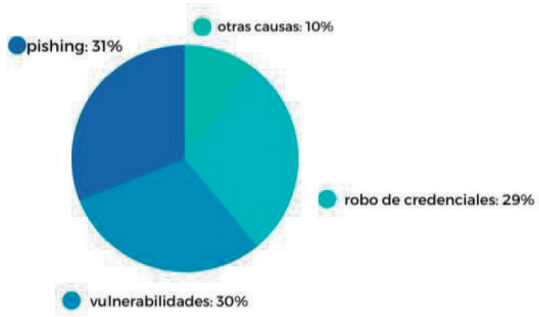

Fig. 2. Causa de los incidentes
Fuente: elaboración propia basada en datos de Internet Security Threat Report 2019 – Symantec

Según los estudios a lo largo de los años, podemos observar que en el año 2020, fecha de punto álgido de de la pandemia por COVID-19 donde las empresas de América latina se dieron más afectadas

> Casi nueve de cada diez encuestados afirman que trabajar desde casa ha afectado negativamente la eficacia de las medidas de prevención de fraude de su empresa, la mitigación del riesgo de incumplimiento o la ciberseguridad. El trabajo remoto ha reducido la capacidad de las empresas para monitorear el comportamiento, lo que aumenta el riesgo de fraude [11].

También se crearon importantes debilidades de ciberseguridad, gracias a un acceso más abierto a los sistemas.

El aumento del trabajo híbrido y un auge generalizado de los ciberdelitos como resultado de la pandemia significan que la mayoría necesitará mejorar sus procesos operativos, incluso después de COVID-19.

> Según fuentes externas, que cuentan con un registro desde 2010 en adelante, demuestran que a lo largo de los años ha ido creciendo de los años analizados, nivelando que en 2020 se generaron grandes cantidades de *phishing* altamente vinculables al aprovechamiento del COVID-19 para atacar a diferentes organizaciones e individuos que se debían mantener actualizados constantemente en materia de higiene y control por diferentes fuentes. [17]

Según fuentes externas se sabe que "31 % de las empresas encuestadas en Latinoamérica han percibido un aumento en los ataques cibernéticos a partir de la pandemia, siendo la industria bancaria la más afectada con un 52 % de incremento percibido". [22]

Un 24 de las empresas aumentaron su presupuesto en ciberseguridad y 26 % en protección de datos a raíz de la pandemia, y sólo 17 % de las organizaciones cuentan con un seguro de riesgo cibernético. Sólo en el 27 % de las empresas que implementaron trabajo remoto, la fuerza laboral trabaja exclusivamente con dispositivos de la organización. [22]

El estudio se obtuvo de los resultados de una encuesta hecha a más de 600 empresas de la región, de más de 18 países en más de 20 sectores. Las empresas encuestadas están distribuidas por toda la región, 31 % en Brasil, 17 % en Colombia, 11 % en México, 8 % en Perú, 4 % en Argentina y 29 % en otros países, en sectores industriales como: alimentos y bebidas, aviación, bienes raíces, comunicaciones, construcción, educación, energía e hidrocarburos, entidades públicas y ONG, hotelería y restaurantes, financiero, manufactura, minería, química, retail y transporte, entre otros. [22]

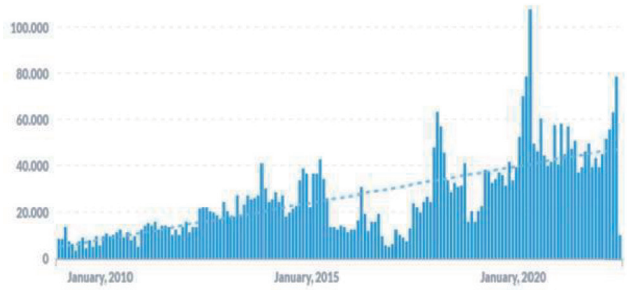

Fig. 3. Distribución de volumen de *phishing* histórico [18]

Además, es posible identificar que con el paso de los años se ha comenzado a utilizar sitios web que además cuentan con certificados de seguridad que permiten generar una imagen visual de mayor credibilidad ante los usuarios ya que se evitan los mensajes de sitio riesgos que generan automáticamente los navegadores web para sitios HTTP. [18]

Para protocolo HTTP se puede ver una constante disminución en su uso desde 2018 a la fecha, mientras paralelamente protocolo HTTPS gana terreno en las campañas de *phishing*.

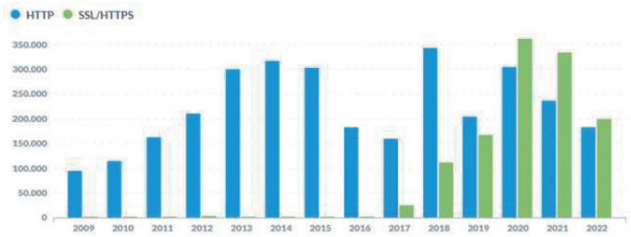

Fig. 4. Distribución historia de sitios HTTP v/s HTTPS [18]

C. Afectaciones del COVID-19 en el phishing

Antes de la pandemia del COVID-19 el *phishing* se solía llevar a cabo a empresas pequeñas y ahora tiende a ser a grandes empresas, incluso a multinacionales, administraciones estatales e infraestructuras esenciales.

Todo esto se debe a que ahora las empresas con el home office se han llevado a cabo nuevas formas de trabajo que involucran mucho más las TIC y por lo tanto se ha vuelto más fácil para los ciberdelincuentes atacar a empresas grandes y también se han aprovechado del aumento en la vulnerabilidad en materia de seguridad de las empresas para robar datos, información confidencial, contraseñas y obtener beneficio de esto.[19]

Según uno de los socios de INTERPOL del sector privado detectó 907000 correos basura, 737 incidentes de tipo malware, y 48000 URL maliciosas, todos ellos relacionados con la pandemia por COVID-19.

Entre los principales ciberataques durante la pandemia se pueden resaltar los siguientes:

- Las estafas por internet y el *phishing*
- *Malware* disruptivos
- *Malware* destinados a la obtención de datos
- Dominios malignos
- Desinformación [19]

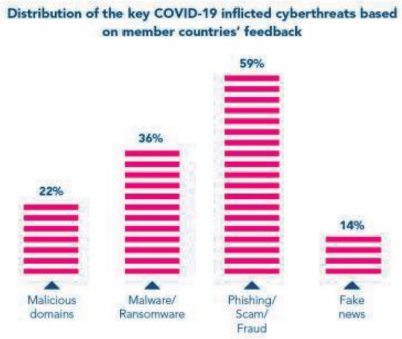

Fig. 5. Distribución de las principales ciberamenazas infligidas por COVID-19 según los comentarios de los países miembros (INTERPOL) [19]

Gracias al COVID-19 el uso del internet se intensificó y por ende también se hace más fácil los ciberataques y gracias a lo inesperado de la pandemia y lo abrupto del cambio de la presencialidad a la virtualidad se generaron huecos en la ciberseguridad, huecos que fueron de provecho para los ciberdelincuentes.

D. Cómo se han visto afectados los negocios o empresas con el phishing

A lo largo de los últimos años se han aumentado los casos de ciberataques por *phishing*. Las empresas han perdido miles de millones gracias a esto. Un estudio de Cisco reveló que el 22 % de las organizaciones que sufrieron un ataque perdieron clientes inmediatamente, en esto se pudo observar la gran importancia que tiene para el cliente el hecho de que sus datos estén seguros [20]

Es muy esencial formar a los empleados sobre el ataque principal con *ransomware* que realiza aproximadamente el 80 % de los casos mediante correos basura o spam. también estos pueden contener un enlace que conduce a una página web infectada, o bien llevan adjunto un archivo con virus. Es muy recomendable formar a los empleados en estos ataques que se pueden dar. Algunos fabricantes de soluciones de seguridad

y de sistemas operativos ofrecen cursos de concienciación sobre seguridad

Si una empresa está bien preparada, por lo general, los datos perdidos se pueden recuperar. Empresas que se han visto afectadas relatan que todas las medidas requieren mucho tiempo y recursos y, en algunos casos, incluso hay que reintroducir datos de usuarios determinados. Lamentablemente, los responsables informáticos de las empresas tienden a restablecer los datos demasiado rápido y sencillamente borran los sistemas afectados.

E. El coste medio de los ataques de phishing para las empresas se ha casi cuadruplicado desde 2015

El *phishing* sigue siendo rentable para los cibercriminales y, consecuentemente, un lastre económico para las empresas que lo sufren.

> En los últimos seis años su coste se ha cuadruplicado. Así lo revela un informe realizado por Proofpoint y el Instituto Ponemon. Según este, grandes empresas norteamericanas pierden de media unos 14,8 millones de dólares al año, o unos 1.500 dólares por empleado, debido a estos ataques. Esto supone un fuerte aumento respecto a los 3,8 millones de dólares registrados en 2015. [21]

Según este estudio, en el que han participado casi 600 profesionales de seguridad y de TI, los ataques Business Email Compromise (BEC) y de *ransomware* son las amenazas más costosas para las empresas. Eso sí, el impacto en dichas organizaciones va mucho más allá de los fondos transferidos a los atacantes.

V. CONCLUSIONES

Tras el análisis, podemos deducir que la problemática del *phishing* viene creciendo y cada día más que pasa, los ataques son más avanzados. Por eso, es necesario que las empresas comiencen a implementar infraestructura y herramientas seguras para contrarrestar ciberataques. Más que todo las empresas que se benefician del comercio electrónico, se les recomienda inculcar conductas sanas o charlas para evitar que sus clientes caigan en trampas.

Las entidades son las responsables de desplegar de distintas maneras y estratégicamente acciones para prevenir la sustracción de datos personales de cualquier índole, ya sea económico, fiscal, etc. Esto hace que como consecuencia no puede exigir que el usuario adopte mecanismos de autoprotección, sino que las entidades tienen que estar preparadas para los nuevos mecanismos de *phishing*.

Es necesario saber que la ciberseguridad desempeña un rol muy importante dentro de las empresas. Básicamente, si hay un mal uso en los sistemas de información privados y recursos internos puede tener consecuencias devastadoras en todas las áreas de la organización, causando problemas productivos y financieros. Por lo tanto, la seguridad de la red de la empresa debe estar enfocada a la prevención de amenazas y riesgos del sistema de información interno. Actualmente, para tener una adecuada seguridad de la información en la empresa, en primer lugar, se necesitan expertos en tecnología informática que sean capaces de predecir las amenazas y riesgos antes mencionados.

Como sabemos el *phishing* es una amenaza para las empresas en la que una de las más habituales es cuando las personas reciben un email procedente de un supuesto ente gubernamental o financiero, solicitando información confidencial adjuntando enlaces fraudulentos, la víctima al abrir este enlace o al brindar la información que se le solicita está causando un daño a su propia persona y a la empresa, generando problemas de confianza entre el cliente y la empresa respectiva, por lo tanto es de gran importancia que todas las personas estén enterados de esta forma de ciberataque.

El *phishing* forma parte de una problemática más grande llamada ingeniería social. Esta se basa en persuadir a las personas a través de las emociones para conseguir sus datos personales.

Por esta razón, no se debe confiar en correos que solicitan información confidencial o personal. Se tendrá que tener presente que ninguna institución financiera o gubernamental pedirá verificar datos por email sin la autorización de la persona.

Otras maneras para contrarrestar los ataques a la ciberseguridad ocasionados por el *phishing* incluyen implementar un sistema de autenticación de múltiples factores en la empresa, a finde de garantizar que las personas que acceden a los sistemas o software sean quienes dicen ser y están autorizadas. También supervisar acciones inusuales por parte de usuarios autorizados y personas no autorizadas que acceden a la información, es necesario enseñar sobre la cultura en seguridad cibernética y convertirla en una prioridad para que todos en la organización sepan cuándo podrían verse atrapados en un delito cibernéticos y llevar a cabo el descubrimiento de datos para comprender dónde reside toda la información confidencial de la organización y utilizarlo para implementar soluciones como el cifrado para proteger a la empresa o al cliente.

Para poder combatirlo se necesita una colaboración global de todos los países, esto a raíz que en cada país el método es diferente y estos pueden ayudarse entre sí para poder combatirlos con una eficacia mayor. La información de gran valor y que sea necesaria debe ser compartida por cada país, así poder tener unos resultados que sean positivos para combatir el *phishing*.

Los cibercriminales o hackers que realizan este delito son personas muy preparadas, llamadas criminales informáticos, ellos poseen gran conocimiento; esto hace que en la mayoría de casos puedan borrar o no dejar rastro del delito.

El *phishing*, con los años se ha vuelto una de las formas más comunes de sacar información confidencial a las empresas grandes ya que es una forma donde se ataca al eslabón más débil que es el factor humano y es una forma

donde la víctima puede caer muy fácilmente en este ciberataque si no se informa sobre esto y se trabaja en la ciberseguridad no solo de la empresa en sí, sino también de cada uno de los trabajadores de una empresa, ya que estos pueden tener información confidencial en sus dispositivos y no estar protegidos debidamente.

REFERENCIAS

[1] Panorama de phishing primer semestre 2022. https://portal.cci-entel.cl/Threat_Intelligence/Boletines/1324/ (consultado el 17 de noviembre de 2022).

[2] R. M. Díaz, "Estado de la ciberseguridad en la logística de América Latina y el Caribe", p. 68.

[3] Gil Vega, "Defienda su empresa de los ataques de phishing." Apr. 21, 2022. [Online]. Available: https://www.veeam.com/blog/es-lat/phishing-attacks.html.

[4] Malwarebytes Ltd., "Suplantación de identidad (phishing)." [Online]. Available: https://es.malwarebytes.com/phishing/.

[5] Moises Molero, "¿Cómo afecta un ataque de phishing a una empresa y cómo prevenirlo?" Mar. 01, 2021.

[6] ¿Qué es el phishing? | IBM. Retrieved Nov 16, 2022, from https://www.ibm.com/es-es/topics/phishing.

[7] Malware | IBM. International Bussines Machines. RetrievedNov 16, 2022, from https://www.ibm.com/es-es/topics/malware.

[8] Universidad Austral de Chile. Tipos de Phishing. https://www.uach.cl/direccion-de-tecnologias-de-información/seguridad/tipos-de-phishing.

[9] Benavides Eduardo, Fuertes Walter, & Sanchez Sandra. (2020). Caracterización de los ataques de phishing y técnicas para mitigarlos. Ataques: una revision sistemática de la literatura. (). https://revistas.uteq.edu.ec/index.php/cyt/article/download/357/4/07.

[10] Filtran los emails de 68 millones de usuarios de Dropbox. (2016, -09-01). El Mundo https://www.elmundo.es/tecnologia/2016/09/01/57c84a37e2704e2a0e8b4590.html.

[11] El factor humano 2022 - Informe de amenazas | Proofpoint ES. (2019). Proofpoint. Retrieved Nov 18, 2022, from https://www.proofpoint.com/es/resources/threat-reports/human-factor.

[12] Gobierno de España, Vicepresidencia tercera del gobierno, Ministerio de asuntos económicos y transformación digital, and Instituto nacional de ciberseguridad, Ciberamenazas contra entornos empresariales. [Online]. Available: https://www.incibe.es/sites/default/files/contenidos/guias/doc/ciberamenazas_contra_entornos_empresariales.pdf#page=73&zoom=100,0,0.

[13] "Take the Advice of Ransomware Actors: Prevent Escalation and Lateral Movement", Coveware: Ransomware Recovery First Responders. https://www.coveware.com/blog/2021/6/24/what-we-can-learn- from-ransomware-actor-security-reports (consultado el 18 de noviembre de 2022).

[14] R. M. Díaz, "Estado de la ciberseguridad en la logística de América Latina y el Caribe", p. 68.

[15] Carcavilla y M. L. Puey, "Reflexiones didácticas sobre algunos razonamientos lógicos con la primera ley de Newton y su relación con las ideas previas de los alumnos", Rev. Bras. Ensino Física, vol. 41, número. 3, p. e20180277, 2019, doi:10.1590/1806-9126-rbef-2018-0277.

[16] "Panorama de phishing primer semestre 2022". https://portal.cclentel.cl/Threat_Intelligence/Boletines/1324/ (consultado el 17 de noviembre de 2022).

[17] Informe de Proofpoint "Human Factor 2019": Principales tendencias entre los cibercriminales: más del 99 % de los ataques está a un golpe de clic del usuario | Proofpoint ES. (2019). Proofpoint. Retrieved Nov 18, 2022, from https://www.proofpoint.com/es/newsroom/press-releases/informe-de-proofpoint-human-factor-2019-principales-tendencias-entre-los.

[18] Un informe de INTERPOL muestra un aumento alarmante de los ciberataques durante la epidemia de COVID-19. Retrieved Nov 18, 2022, from https://www.interpol.int/es/Noticias-y-acontecimientos/Noticias/2020/Un-informe-de-INTERPOL- muestra-un-aumento-alarmante-de-los-ciberataques-durante-la- epidemia-de-COVID-19.

[19] La guía definitiva sobre el phishing. MetaCompliance. Retrieved Nov 19, 2022, from https://www.metacompliance.com/es/lp/ultimate-guide-phishing.

[20] A. Sadiq et al, "A review of phishing attacks and countermeasures for internet of things-based smart business applications in industry 4.0," Human Behavior and Emerging Technologies, vol. 3,2021. .https://www.researchgate.net/publication/355489866_A_review_of_phishing_attacks_and_countermeasures_for_internet_of_things-based_smart_business_applications_in_industry_40.

[21] Microsoft.¿Qué es el phishing? | Seguridad de Microsoft. Microsoft. Retrieved Nov 21, 2022, from https://www.microsoft.com/es-es/security/business/security-101/what-is-phishing.

[22] David.Marchal, "El coste medio del phishing se ha casi cuadruplicado desde 2015", Redseguridad, el 27 de agosto de 2021. https://www.redseguridad.com/actualidad/el-coste-medio- de-los-ataques-de-phishing-para-las-empresas-se-ha-casi- cuadruplicado-desde-2015_20210827.html (consultado el 25 de noviembre de 2022).

[23] N. C.M. Latinoamérica, "Marsh y Microsoft: ingeniería social o phishing es el ciberataque que más aumentó en Latinoamérica a raíz de la pandemia," 2021 [Online]. Available: https://news.microsoft.com/es-xl/marsh-y-microsoft-ingenieria.