UNIVERSIDAD DON BOSCO
VICERRECTORÍA ACADÉMICA
FACULTAD DE INGENIERÍA

TRABAJO DE GRADUACIÓN PARA OPTAR AL GRADO DE

Maestro en Seguridad y Gestión de Riesgos Informáticos

PROYECTO

Estudio sobre los riesgos en ciberseguridad causados por personas neófitas en Tecnologías de Información y su impacto en las organizaciones.

PRESENTADO POR

Lic. Salvador Antonio Mena Menéndez
Lic. Wilber Leonel Reyes Ventura.

ASESOR

Dr. Carlos Bran.

Antiguo Cuscatlán, La Libertad, El Salvador, Centro América

Junio 2024.

CONTENIDO

AGRADECIMIENTOS.

A Dios:

Por permitirnos desarrollar en nosotros la Sabiduría, Buena Salud y la fortaleza de afrontar los retos de la vida y así culminar uno de nuestros más grandes logros.

A Nuestros Padres:

Por ser nuestros guías, en enseñarnos el sentido de la vida y la forma de afrontar todas las adversidades que a diario podemos encontrar en nuestras vidas, por su apoyo incondicional en nuestro proceso formativo.

A nuestras Familias:

Quienes fueron fuentes de impulso y motivación, en el desarrollo de las distintas etapas de este proceso de beneficio para nuestras vidas.

A nuestros Maestros:

Quienes, con sus sabios conocimientos y consejos, nos incentivaron en nuestros deseos de superación y nos orientaron para buscar en nosotros mismos la forma adecuada de solventar cada situación que puso a prueba en todo momento la capacidad resolutiva individual y grupal.

RESUMEN.

En el presente trabajo se demuestra que en la actualidad la mayoría de personas en las administraciones (pública y privada) que han sido objeto de prueba para el desarrollo de este trabajo, descuidan de manera continua los procesos de seguridad que deberían aplicar para el uso de las Tecnologías de Información de las cuales son responsables, los procesos de formación en materia de ciberseguridad resultan ser demasiado “costosos” para muchas de las empresas, por lo cual centran su atención en otros problemas de seguridad, generalmente relacionados con lo físico, pero el problema real es el costo generado a las empresas tras un ciberataque según cifras presentadas por IBM son de hasta 4.5 millones de dólares, entonces a raíz de un problema tan recurrente surge la hipótesis “A mayor cantidad de personas neófitas en seguridad de Tecnologías de Información con bajo índice de escolaridad, mayor riesgo de ciberseguridad para las empresas a las que pertenecen”, siendo un problema grave para los activos de información de las mismas, ya que corren el riesgo de verse involucradas en perdida de datos sensibles para la organización y por consiguiente daño a la reputación percibida por los usuarios finales.

Para comprobar la hipótesis planteada, se aplicó la metodología de investigación a través del método descriptivo con su variante cuantitativa, realizando encuestas y posteriormente aplicando un ejercicio de ingeniería social (Phishing) para comprobar el nivel de conocimiento en el tema y conocer las vulnerabilidades que estas personas representan a las empresas respectivamente. al finalizar esta investigación se concluye que el impacto generado por las personas neófitas en TI es un riesgo no aceptable para las administraciones públicas y privadas, ya que representa una de las peores amenazas actuales, así mismo se emiten recomendaciones para la solución de estas situaciones a corto plazo y se genera una guía de buenas practicas para los usuarios de Tecnologías de Información, para reducir los impactos negativos en la ciberseguridad.

ABSTRACT.

Currently, the majority of people in the administrations (public and private) that have been tested for the development of this work, continually neglect the security processes that they should apply for the use of the Information Technologies of which are responsible, cybersecurity training processes turn out to be too “expensive” for many companies, which is why they focus their attention on other security problems, generally related to the physical, but the real problem is the cost generated. The companies after a cyber-attack according to figures presented by IBM are up to 4.5 million dollars, so as a result of such a recurring problem, the hypothesis arises “The greater the number of people who are neophytes in Information Technology security with a low level of education, the greater the risk. cybersecurity for the companies to which they belong", being a serious problem for their information assets, since they run the risk of being involved in the loss of sensitive data for the organization and consequently damage to the reputation perceived by the end users.

To verify the proposed hypothesis, the research methodology was applied through the descriptive method with its quantitative variant, conducting surveys and subsequently applying a social engineering exercise (Phishing) to check the level of knowledge on the subject and to know the vulnerabilities that these people represent the companies respectively. At the end of this research, it is concluded that the impact generated by IT neophytes is an unacceptable risk for public and private administrations, since it represents one of the worst current threats. Likewise, recommendations are issued for the solution of these situations. short term and a good practice guide is generated for Information Technology users, to reduce negative impacts on cybersecurity.

Palabra clave: Ciberseguridad, Tecnología, Costos.
Keyword: Cybersecurity, Technology, Costs.

INTRODUCCIÓN.

Desde la introducción del internet en la década de los 80/90's, en El Salvador como en muchos países las Tecnologías de Información, se han convertido no únicamente en una herramienta de trabajo, estudio o entretenimiento sino más bien en parte de la vida cotidiana de toda la población.

Basado en la circunstancia antes descrita se ve la necesidad de que las personas que hacen uso de las mismas, tengan formación al menos básica en cuestiones de seguridad cibernética y de esa manera evitar continuar siendo el eslabón más débil en esta cadena de seguridad, para las asociaciones debe imperar la necesidad de capacitar a su personal, ya que es la única forma de evitar ataques de ciber-criminales.

El presente trabajo de investigación se elaboró con el propósito de identificar la situación actual en El Salvador, en lo relativo a la cantidad de personas neófitas en TI que, aunque pueden tener estudios de diferentes niveles, no tienen mayores conocimientos en el tema.

Se investigo tanto en la administración pública como en la empresa privada y de esa forma se obtuvo una radiografía especifica de la situación en seguridad de tecnologías actual que genera un panorama de lo que sucede en El Salvador.

En el Capítulo I, se describe la situación de la problemática actual, se conoce que a partir del año 2019 la digitalización en El Salvador ha ido a paso rápido, en la actualidad hasta los niveles de educación primaria cuentan con tecnologías de información, acceso a internet y otros recursos digitales que generan directamente productividad en los diferentes sectores en el presente y para el futuro, pero indirectamente son un peligro inminente.

En el Capitulo II, se presenta la fundamentación teórica que da paso a nuestras hipótesis sobre la situación actual y futura en cuanto a la ciberseguridad, de continuar en la misma situación de desconocimiento y poca importancia a los posibles impactos que esto genera.

En el Capitulo III, se describe la metodología utilizada para este estudio, el cual sienta un precedente en la investigación sobre uno de los mas grandes problemas para la ciberseguridad, siendo este el desconocimiento de los usuarios intermedios y finales, la metodología empleada ayuda a describir un universo bastante amplio de usuarios y de igual manera nos permite emplear, de forma muy acertada la ingeniería social posterior a la obtención de los resultados iniciales, lo que resulta muy satisfactorio ya que ayuda a comprobar nuestras hipótesis y genera de igual forma un parámetro sobre que corregir o implementar para la empresa privada que nos abrió sus puertas y de igual manera para la entidad de administración pública, en este capítulo también se presentan los resultados y sus respectivas discusiones que resultan ser la esencia de nuestra investigación.

La ciberseguridad es tarea de todos y es una de las ramas de la ciencia que actualmente, esta tomando un auge superior a muchas otras, lo cual debería de generar preocupación por parte de los diferentes actores en el sector productivo de la sociedad, en el sentido de informarse y mantenerse actualizado en tan importante recurso, pues en El Salvador estamos en un camino acelerado y muy acertado hacia la digitalización y continuidad en el uso de las tecnologías de información.

CAPITULO I.
PLANTEAMIENTO DEL PROBLEMA

1. Situación Problemática.

El desarrollo tecnológico en El Salvador desde sus inicios durante la década de los 80 y 90, ha evolucionado constantemente, lo que supone un problema amplio en cuanto a la seguridad informática, ya que está en una gran parte depende de su administración y de los usuarios finales, las personas neófitas en temas de tecnologías de información [En adelante TI] se convierten en uno de los puntos débiles de las organizaciones y a través de las mismas es posible para los cibercriminales ejecutar ataques con altas probabilidades de éxito.

La ciberseguridad se ha convertido en una de las prácticas que más está siendo utilizada en las empresas para proteger y defender las redes, los procesos de comercio electrónico, computadores, dispositivos móviles y servidores de ataques cibernéticos. En la actualidad es un hecho que las empresas al igual que todas las organizaciones tienen que enfrentar a diario cientos de amenazas y entre las 7 principales encontramos:

- El robo de datos de establecimientos minoristas

- Seguridad móvil y amenazas que aprovechan las vulnerabilidades de los teléfonos

- Ataques de phishing[1] e ingeniería social[2]

- Robo de identidad

[1] **Phishing:** Forma de ciberataque en la cual los atacantes intentan engañar a las personas para que divulguen información personal.

[2] **Ingeniería Social:** Técnica de manipulación que aprovecha el error humano para obtener información privada, acceso a sistemas u objetos de valor.

- Pirateo de datos médicos

- Depredadores sexuales que acosan a los niños

- Ataques a bancos (KASPERSKY, 2024)

Los cuales generan degradación en la experiencia de los usuarios y una constante desmejora en la calidad de los servicios ofrecidos.

Las ciberamenazas generan pérdidas económicas masivas, afectan el bienestar de los individuos y generan un desbalance en todas las estructuras de seguridad de las empresas y organizaciones. Cabe mencionar que muchos de los ataques recibidos en las empresas, conllevan un denominador en común, el cual es el usuario final (neófito), muchas veces por desconocimiento, o el no empleo de buenas prácticas en el uso de Tecnologías de Información, una problemática que puede ser solucionada a corto plazo con la adecuada capacitación de personal.

La situación educativa según estudios de UNICEF[3] durante el año 2016 (CONED-UNICEF, 2016) indican las edades y cantidades en las cuales las personas no han asistido a centros escolares y por lo tanto la educación en temas de T.I han sido nulos, un parámetro importante a considerar es que aunque las personas no tengan ningún grado de escolaridad, si hacen uso de T.I específicamente de teléfonos celulares según encuestas realizadas por la SIGET[4] hasta el año 2020 existían unas 9.3 millones de líneas telefónicas en comparación a la densidad poblacional del país y a la cantidad de personas alfabetizadas, situación que genera un panorama amplio sobre la cantidad de potenciales victimas de cibercriminales y a las cuales se les

[3] **UNICEF:** United Nations Children's Fund [Fondo de las Naciones Unidas para la Infancia]
[4] **SIGET:** Superintendencia General de Electricidad y Telecomunicaciones de El Salvador

debería capacitar a través de todos los medios disponibles, con el propósito de evitar el mal uso de los dispositivos a nivel nacional.

Por otro lado, la tenencia de computadora en los hogares salvadoreños se duplicó en 2022 e incluso alcanzó una cobertura del 74 % entre las familias con estudiantes de escuelas públicas, pero no hubo mayor avance en el acceso a Internet, revelan estadísticas gubernamentales.

La Encuesta de Hogares de Propósitos Múltiples (EHPM) de 2022, realizada por el Gobierno, señala que el 41.66 % de las familias, con o sin estudiantes, dijo tener computadora en casa. Este porcentaje se duplicó en comparación con el 18.41 % de 2021 y además experimentó el crecimiento más alto desde 2008. Antes de 2022, el mayor aumento había ocurrido en 2012, cuando de 15.87 pasó a 19.6 %.

Los costes para las empresas en lo relativo a ciberseguridad y ciberataques, son sumamente significativos según el informe “The cost of cybercrime”, el cual señala que para las empresas los malware[5] y los ciberataques relacionados con información privilegiada maliciosa aumentó en un 12% en 2018 y representó un tercio de todos los costes derivados de los ciberataques. Se basa en entrevistas a más de 2.600 profesionales de seguridad y Tecnologías de la Información de 355 organizaciones de todo el mundo, las infecciones por malware aumentaron en un 11%, hasta alcanzar un promedio de más de 2,6 millones de dólares por empresa, y el coste debido a las personas con información privilegiada maliciosa -segmentados por los perfiles de empleados, personal temporal, contratistas y socios comerciales- se incrementó un 15%, hasta alcanzar un promedio de 1,6 millones de dólares por organización. En

[5] **Malware:** Software malicioso, son programas diseñados específicamente para dañar, alterar, robar información o infiltrarse en sistemas informáticos

conjunto, estos dos tipos de ciberataques representaron un tercio del coste medio (13 millones de dólares) para las empresas de los delitos cibernéticos en 2018, lo que representa un aumento de 1,3 millones en el último año. Del mismo modo, el coste para las empresas del phishing y de la ingeniería social aumentó a 1,4 millones de dólares por organización, en promedio (Ponemon, 2018)

En El Salvador a raíz de la pandemia del COVID-19[6], que obligó a cerrar escuelas y adoptar modalidades de educación a distancia, el Ministerio de Educación de El Salvador (MINED) se comprometió a entregar tabletas a los estudiantes de hasta tercer grado y computadoras portátiles para aquellos que cursan de cuarto grado en adelante. También prometió laptops a los docentes.

Según IBM[7] durante el 2023, se dio a conocer que la mitad de las empresas afectadas por un ciberataque no está completamente segura de incrementar sus gastos operativos en seguridad, esto pese a haber sido víctimas de estos ataques.

IBM revela que el promedio global del costo de una violación de datos ha aumentado a 4.45 millones de dólares en 2023, alcanzando un récord histórico y específicamente, un crecimiento del 15% en los últimos 3 años, asimismo, los costos derivados de la detección y el escalado han aumentado un 42% en el mismo periodo, lo que representa la mayor parte de los gastos generados por las violaciones de datos, e indica que ha habido un cambio hacia investigaciones de ataques más complejos (IBM-Informe Coste de la vulneración de datos., 2023), el ahorro medio para las

[6] **COVID-19**: La enfermedad por coronavirus de 2019.

[7] **IBM:** International Business Machines Corporation, también conocida como IBM, es una de las mayores empresas de informática y consultoría del mundo.

organizaciones que utilizan ampliamente la IA y la automatización de la seguridad es de 1,76 millones de USD en comparación con las organizaciones que no lo hacen.

Ante este escenario tan complejo, se generan mayores incertidumbres en cuanto a la puesta en práctica de buenas costumbres para el uso de T.I, pero en la actualidad no existe un documento comprensible sobre las mismas para personas neófitas, razón por la cual hemos realizado la investigación respectiva con el propósito de emitir un

2. Enunciado del problema.

Con base en lo anterior descrito surge el cuestionamiento sobre: ¿Cuáles son los riesgos en ciberseguridad causados por personas neófitas en Tecnologías de Información en la administración pública – empresa privada y su impacto en estas organizaciones en los Dptos. de Santa Ana y San Salvador?

3. Objetivos de la investigación.

3.1 Objetivo General.

Establecer de forma puntual la metodología para medir el impacto de las malas prácticas de personas neófitas en Tecnologías de Información, en el nivel de riesgo de ciberseguridad de las organizaciones.

3.2 Objetivos Específicos.

- Definir la metodología a utilizar para generar un proceso de ingeniería social y obtener datos en tiempo real.

- Medir el impacto negativo causado por usuarios neófitos en TI a nivel organizacional, en un entorno controlado.

- Diseñar una guía de buenas prácticas para usuarios de las TI para reducir los riesgos de ciberseguridad.

4. Contexto de la Investigación.

El estudio está enfocado a obtener datos estadísticos de los delitos informáticos y conexos, posterior a la implementación de la LEDIC (2016) de El Salvador y sus reformas (2022), donde inicialmente se refleja un claro incremento de las actividades criminales en el ciberespacio, así mismo se centra en obtener datos a través de encuestas e ingeniería social sobre el problema de las personas neófitas en T.I que laboran en la administración pública y empresa privada.

La ubicación geográfica está enmarcada en dos cabeceras departamentales densamente pobladas de El Salvador (San Salvador y Santa Ana), se consultaron datos, se realizaron encuestas y prácticas de ingeniería social con el propósito de conocer los riesgos de ciberseguridad que la población (muestra) representa para la administración pública y la empresa privada.

En la actualidad a través de la influencia de las redes sociales y los medios de información abiertos, las personas neófitas en temas de ciberseguridad son altamente propensas a sufrir ataques de cibercriminales, vulnerando su información personal y generando con ello pérdidas económicas y en casos graves daño a la reputación en las instituciones para las que ellos laboran o de las que son parte; asimismo según estadísticas realizadas por encuestadoras nacionales el 74% de la población cuenta con computadora y un 90% con teléfono inteligente con acceso a internet, lo que hace una sociedad vulnerable por sus malas prácticas en cuestiones de seguridad de T.I.

5. Justificación.

El propósito fundamental del presente proyecto es la solución del problema generado por el desconocimiento de los usuarios finales (neófitos) de las tecnologías de información, quienes a causa de la falta de cultura tecnológica vulneran sus sistemas informáticos constantemente y son un blanco fácil para los cibercriminales que operan y se mantienen en constante acecho en busca de víctimas potenciales.

Se realizó una investigación documental, técnica – experimental que nos permitió identificar la situación actual en cuanto a diferentes características de los usuarios finales, se realizaron encuestas y asimismo se ejecutaron experimentos basados en ingeniería social, para comprobar en tiempo real el nivel de vulnerabilidad al que se encuentran expuestos los usuarios neófitos de las tecnologías de información en la actualidad.

Los usuarios de las T.I se encuentran expuestos a diferentes tipos de amenazas cibernéticas y en muchos casos, no poseen conocimientos si quiera básicos en cuanto al cuido de sus dispositivos de información, para evitar ser víctima de amenazas tanto actuales como emergentes.

Ante la problemática previamente descrita, se busca resolver a corto o mediano plazo la situación desfavorable para los usuarios de TI en Santa Ana y San Salvador causadas por la falta de conocimiento del uso adecuado de las mismas.

Los aportes finales del presente estudio son una estadística actualizada en cuanto a el nivel de riesgo actual en temas de ciberseguridad al que se enfrenta la administración pública y empresa privada Salvadoreña en los departamentos bajo estudio a causa del desconocimiento de las buenas prácticas, para la manipulación

de las tecnologías de información (computadoras o smartphones) y cuál es el potencial riesgo para las empresas y el Estado.

De igual manera se crea una guía amigable, con parámetros para identificar amenazas y, asimismo; de lo que no se debe hacer al momento interactuar dentro del ciberespacio, para darla a conocimiento público y sea aprovechada por los usuarios finales.

CAPITULO II.

FUNDAMENTACION TEORICA.

6. Estado actual del hecho o situación.

A principios de 1990 en El Salvador, ANTEL[8], el proveedor estatal de telecomunicaciones, no satisfacía la demanda de abonados. Los salvadoreños debían esperar hasta una década para que les fuera asignada una línea telefónica. Los números de teléfono se consideraban activos fijos y era común encontrar en los clasificados de los periódicos anuncios de compra y venta de líneas telefónicas por miles de colores.

La primera conexión a internet en El Salvador se instaló en el Consejo Nacional de Ciencia y Tecnología (CONACYT) de El Salvador, en 1994. El ingeniero Rafael Ibarra fue quien hizo la instalación con el apoyo de colegas de Guatemala y Costa Rica, algunas universidades junto a La UDB[9], la UCA[10] y formaron la Asociación SVNet.[11] El Salvador obtuvo el dominio '.sv' que permitía diferenciar a los sitios web salvadoreños de los demás. (Martinez, 2017)

La primera conexión de Internet en el país ocurrió en diciembre de 1995 en el edificio de la Administración Nacional de Telecomunicaciones, la primera conexión a Internet era del tipo Unix to Unix Copy Program (UUCP) Para lograr lo conexión, se hizo un acuerdo con UUNet, un proveedor de internet de Estados Unidos. El envío o recepción de los correos no era instantáneo ya que el servidor de El Salvador se conectaba cada media noche con los servidores de UUNET (Hoy Verizon Business)

[8] **ANTEL:** Asociación Nacional de Telecomunicaciones de El Salvador.
[9] **UDB:** Universidad Don Bosco [El Salvador]
[10] **UCA:** Universidad Centro Americana [El Salvador]
[11] **SVNet:** Administrador de nombres de dominio e IP para El Salvador.

para sincronizar los correos entre El Salvador y Estados Unidos, por lo que para enviar o recibir un correo electrónico podían pasar hasta 24 horas.

Las primeras conexiones dedicadas a Internet se establecieron con la ayuda de la Red Hemisférica Universitaria de Ciencia y Tecnología de la OEA [Organización de los Estados Americanos] Estas conexiones dedicadas se establecieron con Sprint y Racsa (Radiográfica Costarricense) una conexión dedicada permanece siempre conectada y permitió que los primeros sitios web se alojaran en servidores ubicados en el país.

Para el año 1996 aparecen los primeros sitios web y están establecidos los dominios competentes al país, entre los primeros sitios se encuentra el de la Universidad Don Bosco (UDB: udb.edu.sv), posteriormente tras la disolución de ANTEL en El Salvador se da paso a la empresa privada en las telecomunicaciones y con ello llega la modernización constante del servicio de internet y por consiguiente el desarrollo de las Tecnologías de Información, las cuales son diseminadas a lo largo y ancho del país de forma rápida (a pesar de sus costos).

Después de una etapa de calma relativa en cuanto a los delitos informáticos en el desarrollo temprano de las Tecnologías de Información e Internet, durante los primeros años no se registran delitos informáticos en El Salvador ya que no había surgido el interés posiblemente por la falta de denuncias y porque aún para 1998 y hasta 2003 no existían las redes sociales como en la actualidad, las cuales son terreno fértil para los delincuentes informáticos de la creación de leyes para combatir y castigar este tipo relativamente nuevo de delitos.

El 26 de febrero de 2016 se aprobó la Ley Especial contra Delitos Informáticos y Conexos, mediante el Decreto Legislativo No. 260, publicado en el Diario Oficial No.

40 Tomo No. 410, de la misma fecha; la cual sistematiza los tipos penales relacionados con la ciberdelincuencia, generando en los operadores de justicia nuevos desafíos para su aplicación y sanción penal, por cuanto la referida normativa se encuentra relacionada con la utilización de tecnologías de la información y comunicación; de tal manera que la investigación, procesamiento y juzgamiento, están condicionadas a la aplicación de actividades técnicas y periciales informáticas. (Fiscalia General de la Republica de El Salvador y UNODC, 2018)

Pero el uso de las TI en su máxima expresión surge en el año 2020, la pandemia detonó el uso de la internet en El Salvador. Según un estudio de la consultora iLifebelt, la aceleración fue de más del 25 % y los usos que la población hace de ella impulsaron actividades en el ámbito social y económico, Rodolfo Salazar, CEO[12] de Idea Works International y represente iLifebelt en el país, los resume así: “Lo que sucedió es que nos aceleramos 10 años”.

El Salvador cerró 2020 con 3.8 millones de internautas, 400,000 más que los que tenía hace cuatro años (2017) y alcanza una penetración del 57 %, una cantidad de usuarios que accede a la red por varios motivos, desde el entretenimiento hasta el teletrabajo, durante este periodo la consultora llifebelt establece un fenómeno que se plasma en tres perfiles: exiliados digitales, huérfanos digitales y herederos digitales.

El exiliado se vio en la necesidad de acelerar el uso de la internet (e invertir) por la pandemia, los huérfanos tenían algún grado de inversión, pero con las cuarentenas y el paro de su operación tuvieron que validar sus procesos y empezar de cero, mientras que los herederos son casos que ya estaban listos para afrontar desafíos como los que planteó 2020 en materia digital, sin traumas.

[12] **CEO:** Chief executive officer [Director General]

En temas comerciales, Salazar explica que las ventas en el canal digital para algunos rubros crecieron.

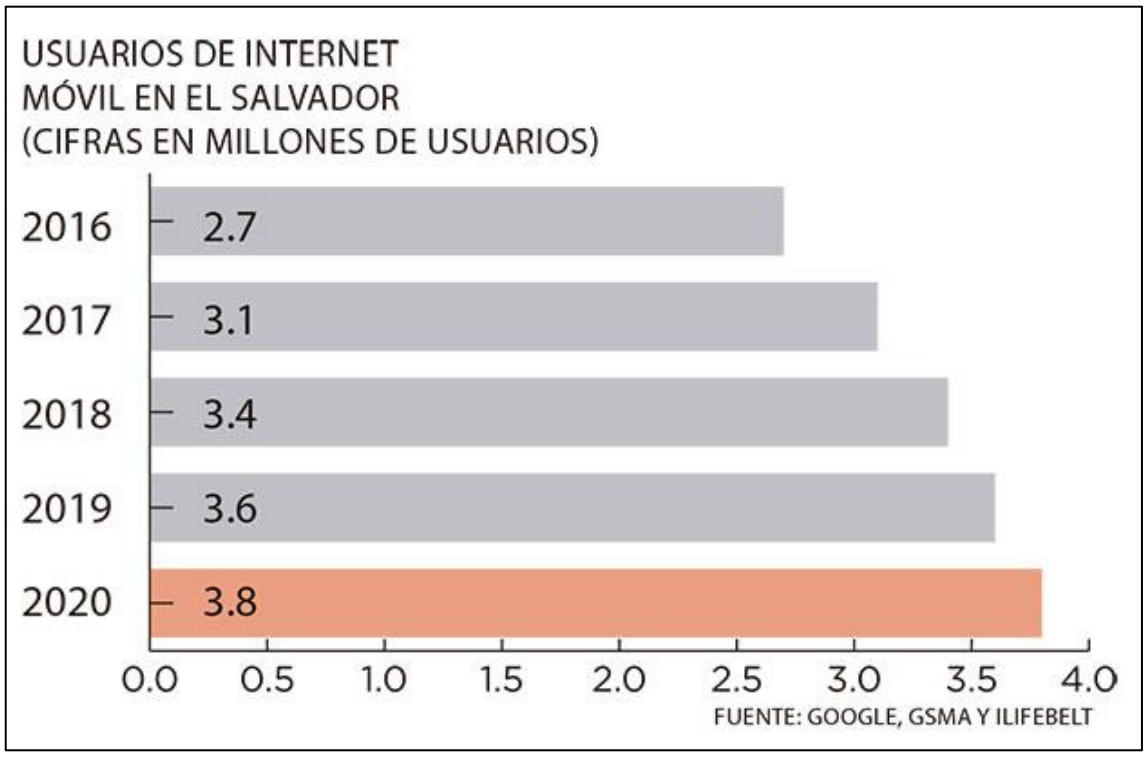


Imagen 001: Usuarios de internet móvil en El Salvador 2020.

La pandemia no solo trajo nuevos usuarios, sino que llevó a otros a buscar mejor velocidad de acceso. Kantar Worldpanel[13] da un panorama regional del consumo de internet en Centroamérica, la firma revela que en 2020 la demanda de banda ancha creció en un 11 % en promedio en la región, un ritmo similar al que tuvo el país, pero por debajo del 17 % que tuvo Costa Rica y del 14 % de Panamá obviamente la población es menor y hasta ese momento no todos tenían a su disposición un teléfono o computadora propios, el confinamiento también elevó en 2 % la compra de computadoras y se estima que un 48 % de los centroamericanos ya posee una.

[13] **KANTAR World Panel**: Empresa mundial de datos, insights y consultoría sobre economía y mercados.

En el caso de El Salvador, durante las cuarentenas un 36 % dijo que usaba el internet principalmente para navegar por redes sociales, un 26 % para usar aplicaciones o sitios de entretenimiento (como Netflix) y solo un 6 % para estudiar cursos en línea.

La pandemia de COVID-19, llevó a más personas de mayor edad a interesarse en hacer uso de tecnologías de información y los hábitos se están modificando desde ese año, el crecimiento fue distinto dependiendo de las edades. El más acelerado fue en las personas de 40 años en adelante. En algunos casos con crecimientos de hasta el 106% en el uso de internet que el año previo. (Diario El Mundo, 2021)

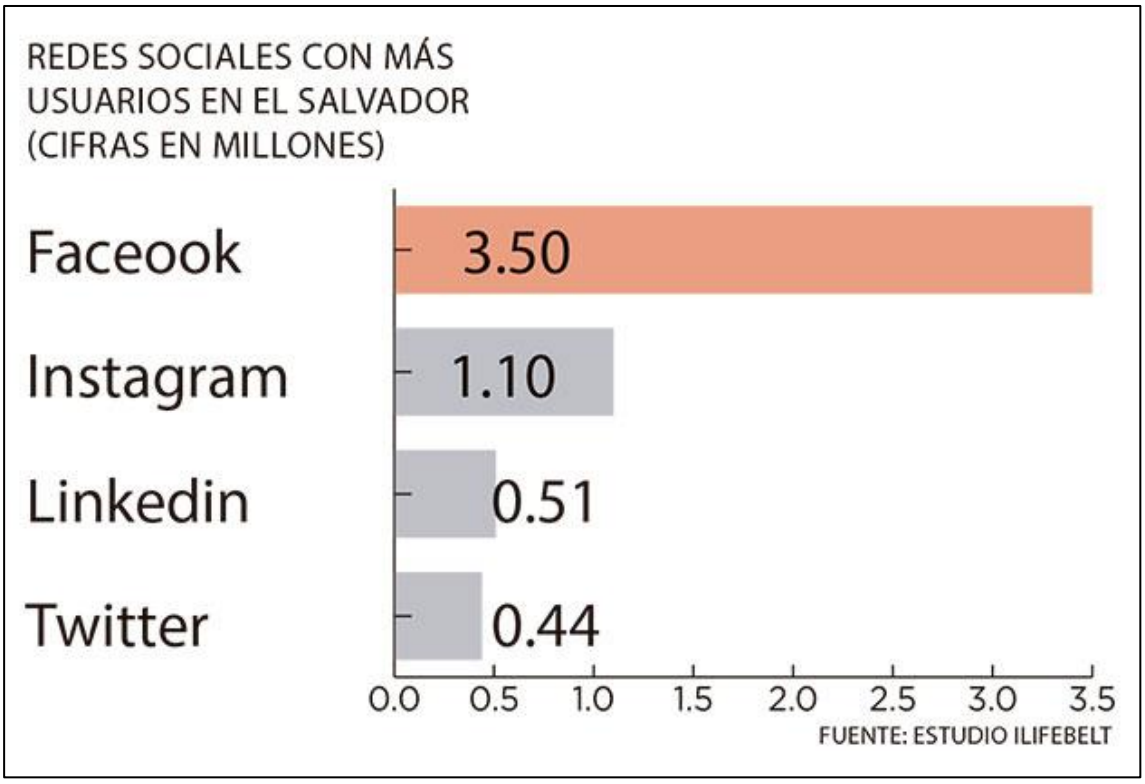


Imagen 002: Redes sociales con más usuarios en El Salvador 2020.

En el 2021, estudios revelan que junto con un mayor uso del internet también hay una mayor exposición a cibercriminales, se revela que una de cada tres empresas en América Latina aseguró ser víctima de algún tipo de infección por malware durante el mismo año, Más del 70 % de los usuarios asegura que en el primer año de la pandemia recibió o tuvo contacto con noticias falsas relacionadas al COVID-19, el

40% de los consumidores en el mundo tiene hasta tres aplicaciones financieras, pero solo la mitad de ellos cuenta con un software de seguridad pagado, el resto aseguran tener pero es gratis.

Otro punto importante es que, la mayoría de personas que utilizan tecnologías de información de forma inconsciente a los riesgos y pese a la vulnerabilidad de sus contraseñas “123456” es la más utilizada en la web en 2020 con más de dos millones y medio de usuarios. (ESET, 2021)

Las reformas a la LEDIC[14] fueron aprobadas por la Asamblea Legislativa a finales de 2021, sancionadas y publicadas por el Presidente Nayib Bukele en el Diario Oficial el 12 de enero de 2022, en las reformas se incorporan definiciones como código malicioso, virus informático.

Se reforman algunos tipos penales relativos a: interferencia de sistema informático; daños a sistemas informáticos; posesión y uso de equipos o prestación de servicios para la vulneración de la seguridad; estafa informática; fraude informático (incorpora la afectación de transacciones en bitcoin y otras criptomonedas); falsedad de documento y firmas (descifrado de documentos); hurto por medios informáticos; hurto de identidad; obtención y divulgación no autorizada de códigos o contraseñas de acceso a programas o datos; utilización de datos personales; obtención y transferencia de información de carácter confidencial (criminaliza la mera obtención y transferencia de información confidencial); secuestro de sistemas, programas o datos informáticos.

[14] **LEDIC:** Ley Especial de Delitos Informáticos de El Salvador.

Se agregan artículos en el capítulo III, relativo a los delitos informáticos relacionados con el contenido de los datos, y en el capítulo IV, relativo a delitos informáticos contra niños, niñas, adolescentes, o personas con discapacidad. (Rivera, 2022)

Para el año 2023 el 89% de personas encuestadas a nivel nacional por la Encuesta de Hogares de Propósitos Múltiples de El Salvador (EHPM) afirmaron tener en uso tecnologías de información (computadoras-smartphone) en las cuales se identificaron hogares los cuales no tienen personas que se encuentren estudiando, pero utilizan las tecnologías de igual forma para otros propósitos, el gobierno de El Salvador hizo incrementar las cifras de personas con TI ya que desde 2020 realizo entregas de computadoras y tabletas para alumnos a nivel nacional.

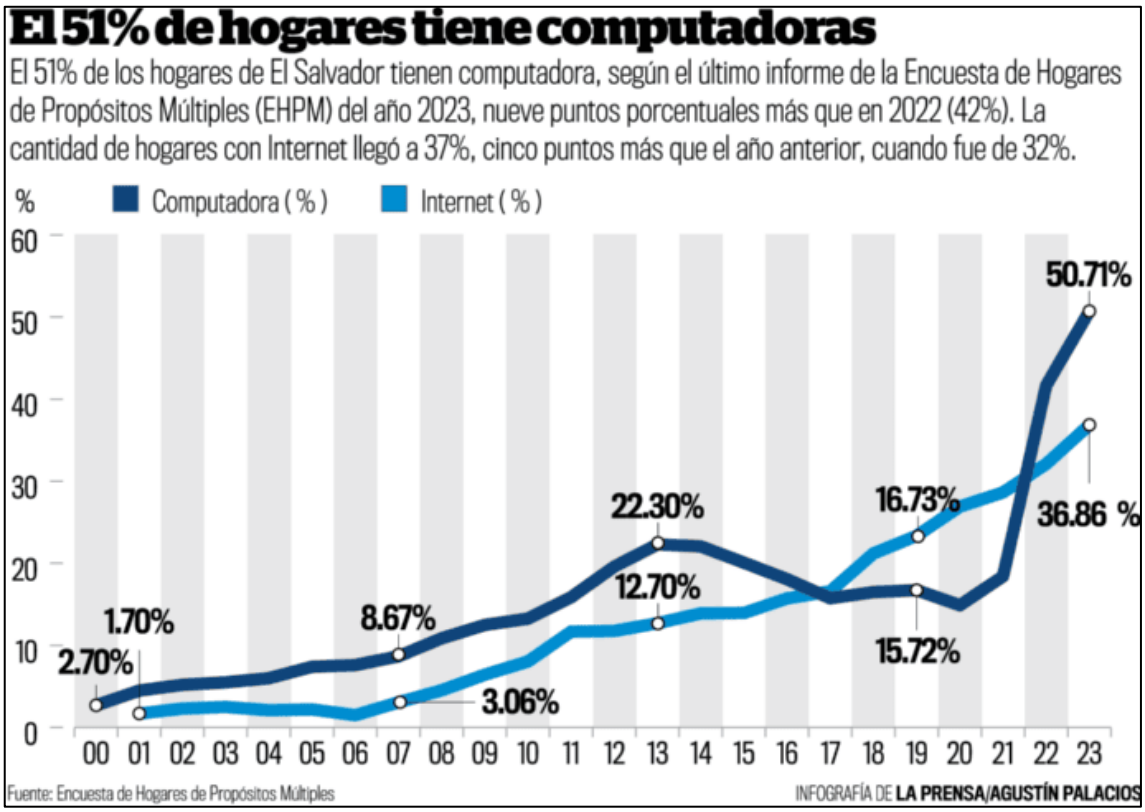


Imagen 003: Hogares con computadoras en El Salvador 2023.

Posterior al incremento de usuarios de tecnologías de información y así mismo personas que navegan en la web, los delitos informáticos han alcanzado cantidades superiores en El Salvador, esto inicialmente se debe a que los usuarios finales son neófitos en el correcto uso de sus dispositivos y en el cuidado de la información personal, en la fecha que este documento se realiza incluso se pudo ver a nivel nacional el ataque más reciente por grupos de cibercriminales en el cual se publicó información personal de una gran parte de la población nacional y los ataques a vallas publicitarias previo a la toma de posesión del actual presidente de la Republica.

Puede considerarse actualmente que, en El Salvador, las tecnologías de la información están experimentando un crecimiento significativo y una mayor adopción en varios sectores, por ejemplo:

- ✓ Infraestructura de Telecomunicaciones.
- ✓ Emprendimiento y Startups.
- ✓ Sector Financiero (Banca digital)
- ✓ Educación y Capacitación: Hay un esfuerzo por integrar más tecnología en la educación, aunque los desafíos de acceso y capacitación persisten, especialmente en áreas rurales y entre poblaciones menos favorecidas.
- ✓ Gobierno Electrónico: Hay iniciativas en curso para mejorar los servicios gubernamentales a través de plataformas electrónicas, se han realizado varios cambios hasta la fecha, pero es un tema extenso para su total implementación.

Y finalmente la Seguridad cibernética o informática que es un área en desarrollo, con un aumento de la conciencia sobre la necesidad de proteger los datos y las infraestructuras críticas.

7. Supuestos Teóricos.

7.1 Hipótesis Descriptiva.

En el año 2025, se aumentará el 10% la cantidad de ciberataques en El Salvador.

7.2 Hipótesis Correlacional.

A mayor cantidad de personas neófitas en seguridad de T.I y con bajo índice de escolaridad mayor riesgo de ciberseguridad para las empresas a las que pertenecen

7.3 Hipótesis de diferencia entre grupos.

El efecto de seguridad que generará la guía amigable no será el mismo en las personas que tienen escolaridad superior que en las personas que tienen escolaridad nula.

7.4 Hipótesis Nula.

El efecto de seguridad que generará la guía amable, será el mismo en las personas que tienen escolaridad superior que las personas que tienen escolaridad nula.

7.5 Hipótesis Alternativa.

El efecto de seguridad que generará la guía amable, será menos en las personas que tienen escolaridad superior que en las personas que tienen escolaridad nula.

CAPITULO III.

METODOLOGÍA DE LA INVESTIGACIÓN

8. Enfoque y tipo de investigación.

El enfoque de la investigación se orientó a presentar una perspectiva general a las organizaciones participantes, sobre la problemática que les representa tener personal neófito en T.I y ello les servirá a su vez como alerta temprana para evitar problemas a futuro.

Por otra parte, el tipo de investigación es descriptiva y a su vez empleando su variante cuantitativa, facilitó la puntualización las características de la población que está estudiando. La investigación descriptiva es un método que permitió la recopilación de información cuantificable para ser utilizada en el análisis estadístico de la muestra de población, es una herramienta popular de investigación que permite describir la naturaleza del segmento demográfico.

9. Sujetos y objeto de estudio.

9.1 Unidades de análisis.

Las unidades de análisis (muestra y población) se determinaron de la siguiente forma:

9.1.1 Administración Pública:

- Ubicación geográfica: Santa Ana (Ciudad)

- Universo: 120 personas

- Muestra: 70 personas encuestadas.

9.1.2 Empresa Privada:

- Ubicación geográfica: San Salvador (Ciudad)

- Universo: 160 personas

- Muestra: 80 personas encuestadas.

9.2 Variables e Indicadores.

Las variables e indicadores detectados según cada una de las muestras son los siguientes:

Administración Pública:

N.º	VARIABLE	INDICADOR
1	Neófito	Registros de vulneración de sistemas
2	Administración	Falta de conocimiento de a quien acudir
3	Capacitación	Solicitud de capacitaciones en TI
4	Información	Desconocimiento del tema
5	Ciberseguridad	Vulneración de direcciones y números institucionales
6	Contraseñas	Administración por Dpto. de TI.

Empresa Privada:

N.º	VARIABLE	INDICADOR
1	Seguridad	Reiterada solicitud en encuestas sobre medidas de seguridad que se deben implementar.
2	Información	Falta de información en empleados
3	Capacitación	Solicitud de capacitaciones en encuestas
4	Medidas	Control descentralizado
5	Desconocimiento	Encuestados sin conocimiento sobre TI
6	Poco interés	Respuestas en encuesta como falta de preocupación en cuanto a ciberataques.

10. Técnicas e instrumentos.

10.1 Técnicas.

10.2 Instrumentos.

10.2.1 Modelo de encuesta realizada a empresa privada y administración pública.

ENCUESTA DE CIBERSEGURIDAD PARA USUARIOS DE T.I (STA.ANA)

* Obligatorio

1. Escriba su numero de whatsapp o correo electrónico *

EJEMPLO@GMAIL.COM

Siguiente

Microsoft 365

Este contenido lo creó el propietario del formulario. Los datos que envíes se enviarán al propietario del formulario. Microsoft no es responsable de las prácticas de privacidad o seguridad de sus clientes, incluidas las que adopte el propietario de este formulario. Nunca des tu contraseña.

Microsoft Forms | Encuestas, cuestionarios y sondeos con tecnología de inteligencia artificial Crear mi propio formulario

El propietario de este formulario no ha proporcionado una declaración de privacidad sobre cómo utilizarán los datos de tus respuestas. No proporciones información personal o confidencial. | Términos de uso

* Obligatorio

INFORMACIÓN GENERAL

2. **Edad:** *

- ○ 20 -
- ○ 20-30
- ○ 31-40
- ○ 41-50
- ○ 50+

3. **Género:** *

- ○ Masculino
- ○ Femenino

4. **Nivel académico:** *

- ◯ Secundaria
- ◯ Bachiller
- ◯ Tecnico
- ◯ Licenciatura
- ◯ Postgrado

5. **¿En qué industria trabaja?** *

- ◯ Tecnología/TI
- ◯ Finanzas/Banca
- ◯ Educación
- ◯ Salud
- ◯ Gobierno

6. **¿Ha recibido formación formal sobre ciberseguridad?** *

- ◯ Si
- ◯ No

Atrás | Siguiente

* Obligatorio

CONOCIMIENTO SOBRE BUENAS PRÁCTICAS DE CIBERSEGURIDAD

7. **¿Con qué frecuencia actualizas tus contraseñas?** *

- ◯ Mensualmente
- ◯ Cada 3 o 6 meses
- ◯ Anualmente
- ◯ Nunca

8. **¿Utiliza autenticación de dos factores (2FA) para sus cuentas?** *

- ◯ Sí, para todas las cuentas importantes
- ◯ Sí, pero sólo para algunas cuentas
- ◯ No, pero estoy considerando implementarlo
- ◯ No

9. **¿Conoces algunos de los ataques más comunes a los que estamos expuestos en ciberseguridad?** *

- ◯ Si
- ◯ No

10. **En caso de que su respuesta anterior sea afirmativa, por favor marque los que conoce:** *

- ☐ Malware
- ☐ Ransomware
- ☐ Phishing
- ☐ Man in the middle
- ☐ Ingeniería Social
- ☐ Amenazas internas
- ☐ DoS/DDoS
- ☐ Suplantación de identidad

11. **¿Cual es su nivel de preocupación sobre los ataques de phishing?** *

- ◯ Muy alto
- ◯ Alto
- ◯ Medio
- ◯ Bajo
- ◯ Nulo

12. **¿Ha sido víctima de algún tipo de incidente de ciberseguridad (Malware, Phishing, etc...) en los últimos 12 meses?** *

- ◯ Si
- ◯ No

13. **Si su respuesta es afirmativa ¿Qué hizo al respecto?** *

- ◯ Reporté al departamento de TI
- ◯ Lo ignoré
- ◯ Respondí al mensaje
- ◯ Otras

14. **¿Cómo evaluarías las medidas seguridad de TI en tu lugar de trabajo?** *

- ◯ Muy seguras
- ◯ Seguras
- ◯ Moderadamente seguras
- ◯ No muy segura
- ◯ Insegura

15. **¿Qué métodos utiliza su empresa para proteger los datos sensibles? (Selección múltiple)** *

- [ ] Encriptación
- [ ] Autenticación multifactor
- [ ] Seguridad física (Candados, Guardias, etc.)
- [ ] Redes privadas virtuales (VPN)
- [ ] Ninguno
- [ ] No lo se

16. **¿Recibe regularmente capacitaciones sobre ciberseguridad en tu trabajo?** *

- ( ) Si
- ( ) No

17. **En concordancia con sus habilidades en ciberseguridad, ¿Se siente preparado para gestionar un incidente de seguridad informática?** *

- ( ) Si
- ( ) No

18. **¿Que medidas de ciberseguridad crees que podrían implementar o mejorar en tu lugar de trabajo?** *

Escriba su respuesta

Puede imprimir una copia de su respuesta después de enviarla

Atrás | Enviar

Microsoft 365

10.2.2 Ingeniería social en entorno controlado:

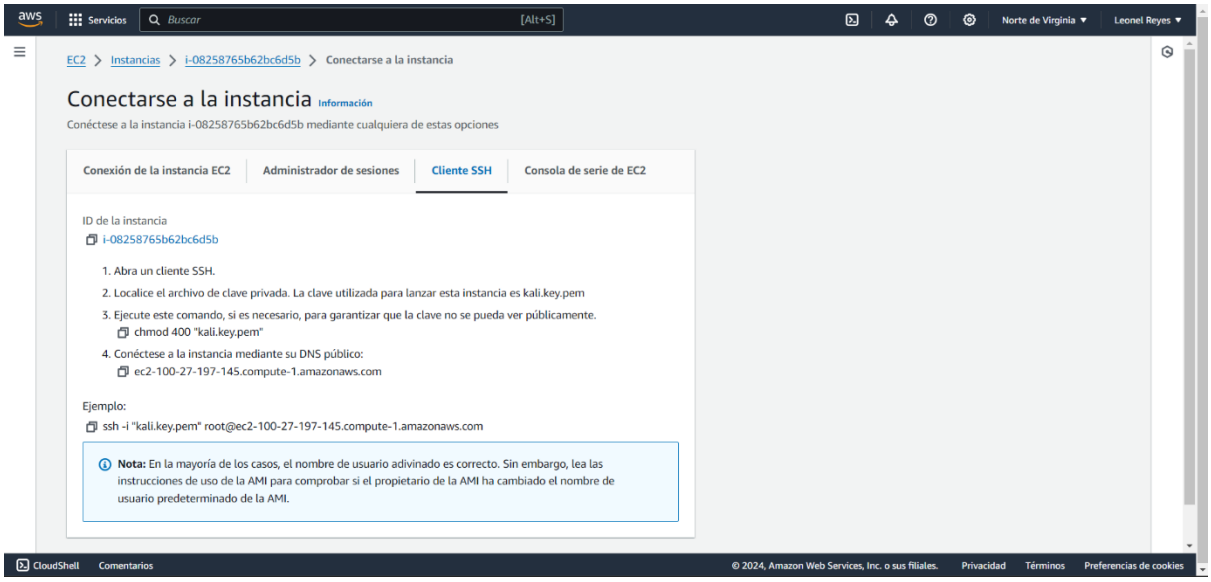


Imagen 004: DNS para conexión a instancia.

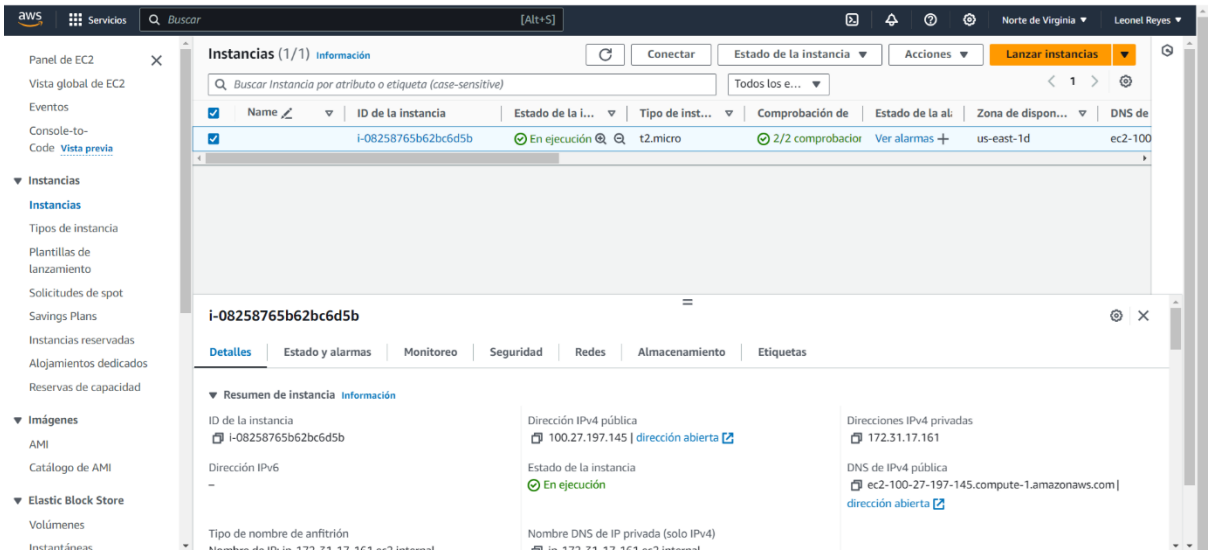


Imagen 005: Instancia lista para conexión.

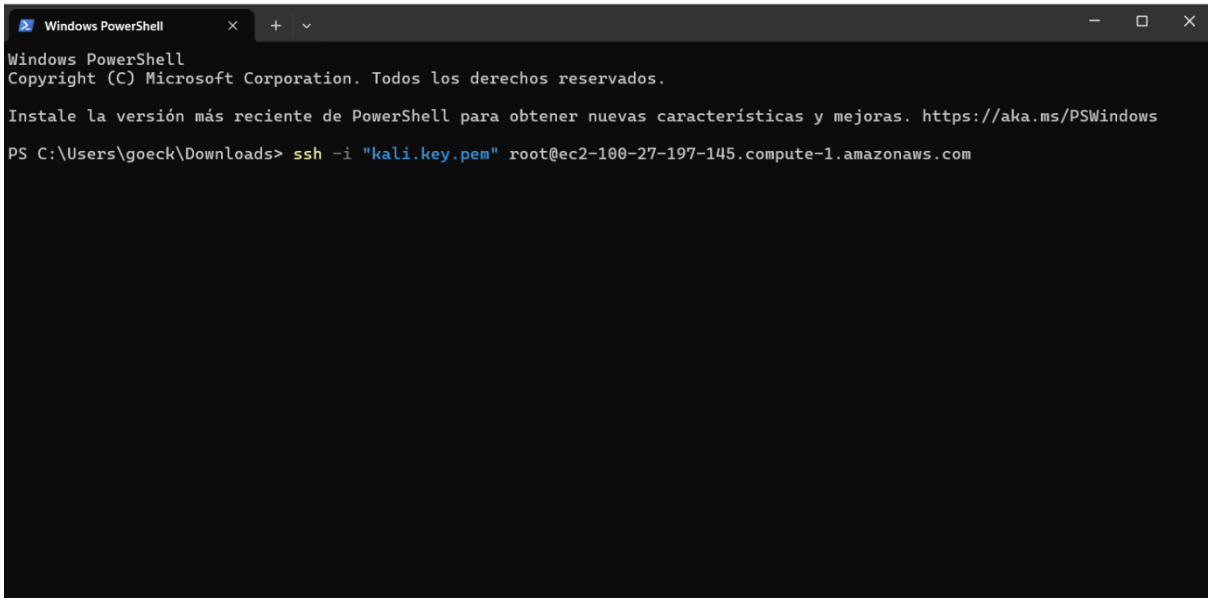


Imagen 006: Conexión a instancia a través de PowerShell con SSH (ssh -i "kali.key.pem" root@ec2-100-27-197-145.compute-1.amazonaws.com)

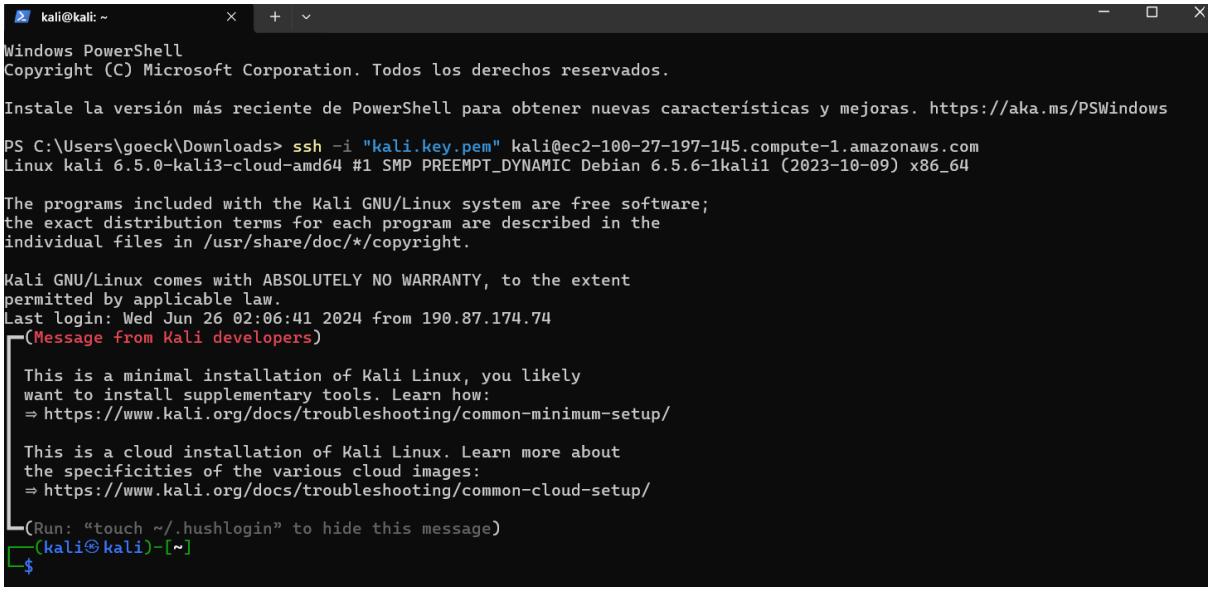


Imagen 007: Establecimiento de conexión con instancia en AWS (Kali Linux)

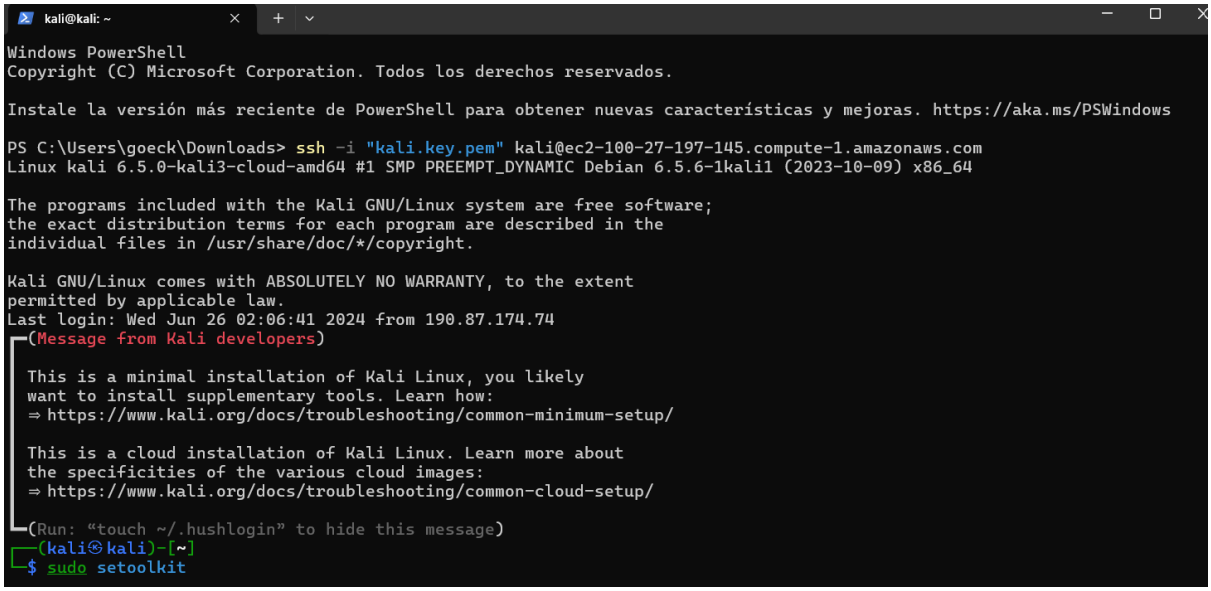


Imagen 008: Ejecución de [sudo setoolkit] para iniciar el proceso de clonación.

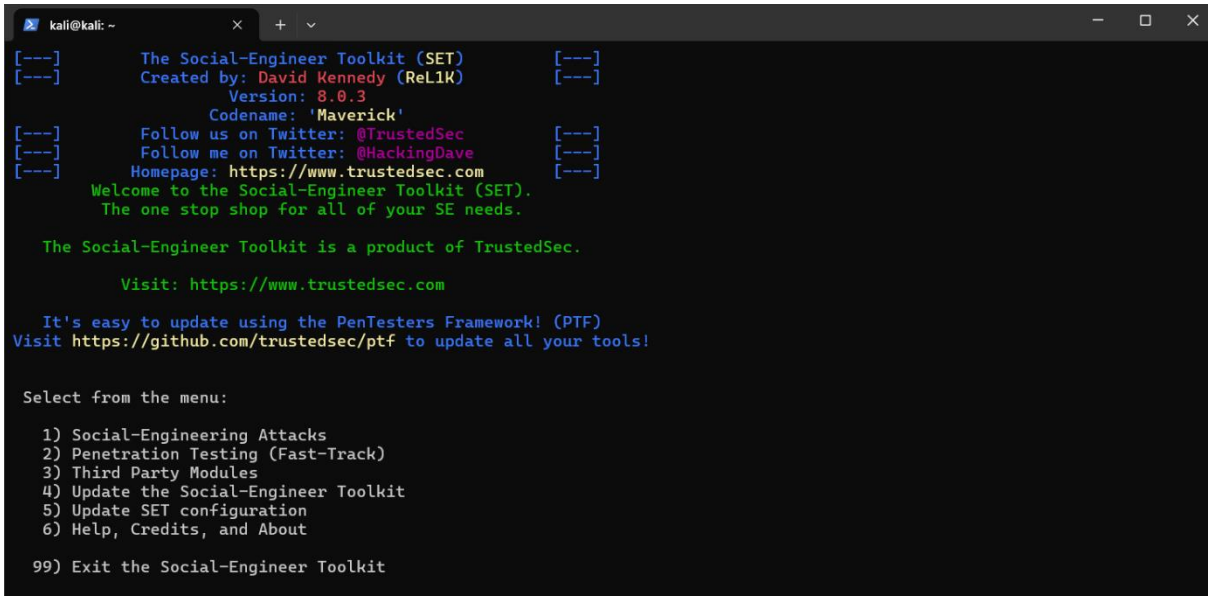


Imagen 009: Selección de herramientas de Ingeniería Social para ejecutar la clonación a través de: [Social Engineering attacks] [Web site attack vectors] [Credential harvester attack method] [Site cloner]

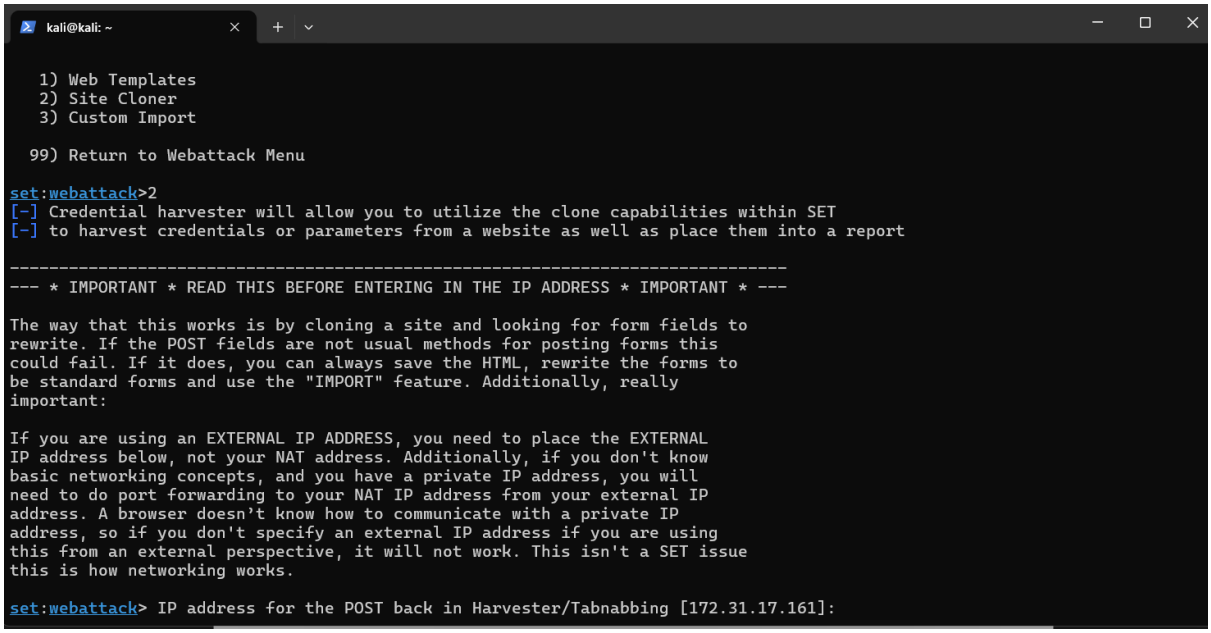


Imagen 010: Establecimiento de dirección IP para Harvester/Tabnabbing.

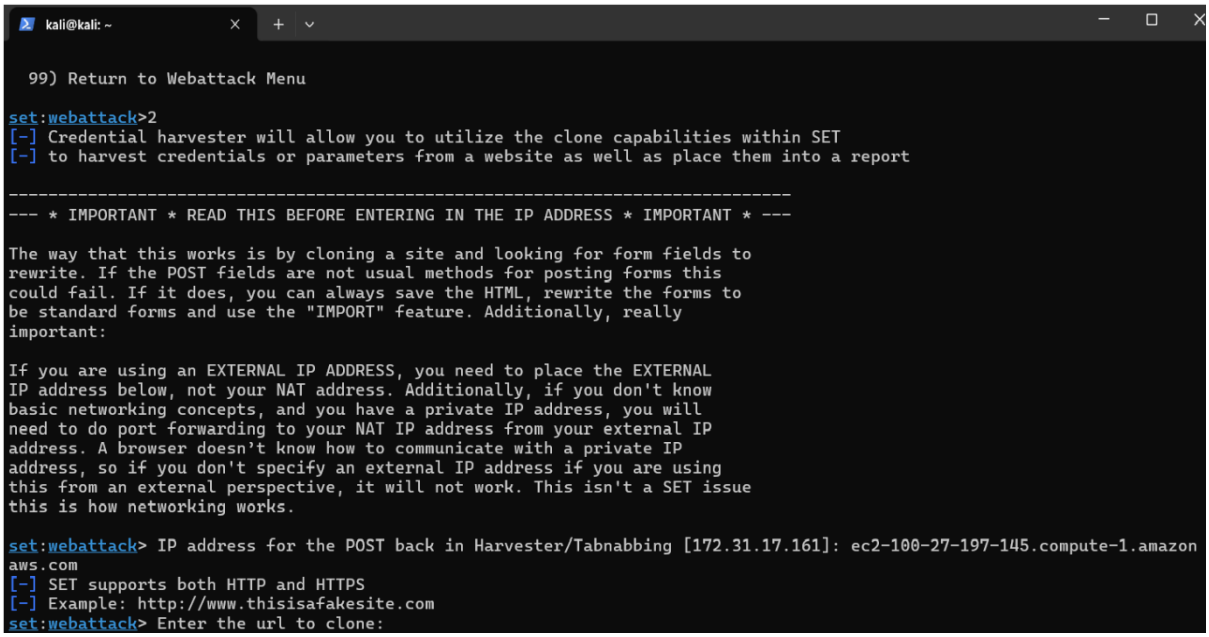


Imagen 011: Ingreso de URL a clonar [https://www.linkedin.com/login/es]

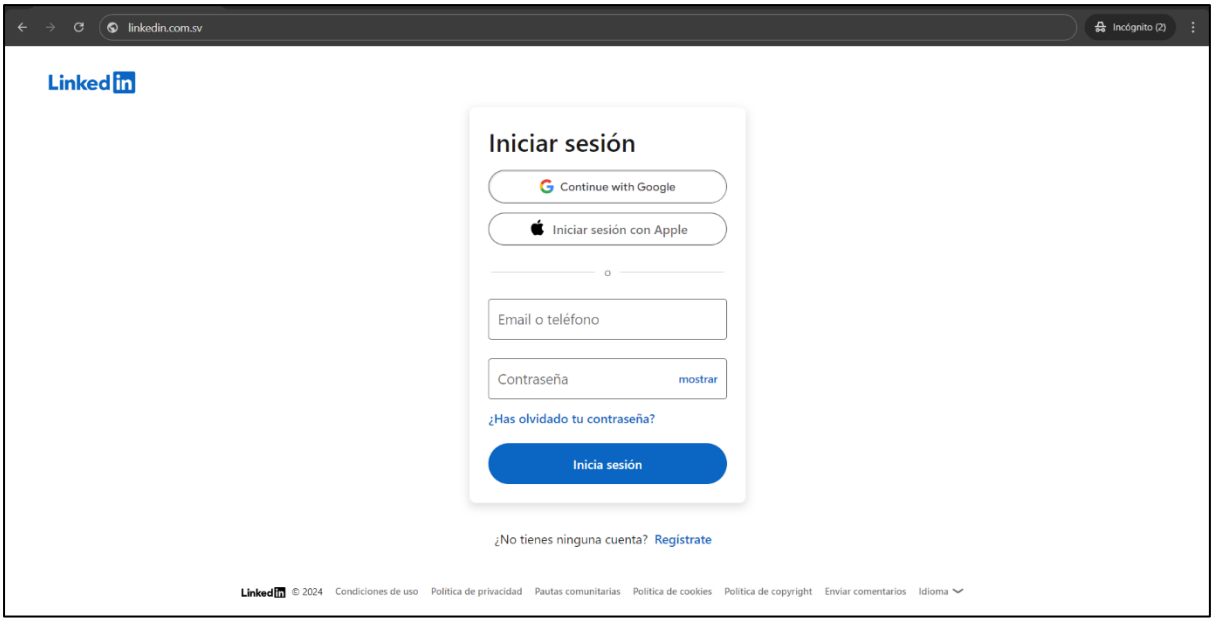


Imagen 012: Sitio web original.

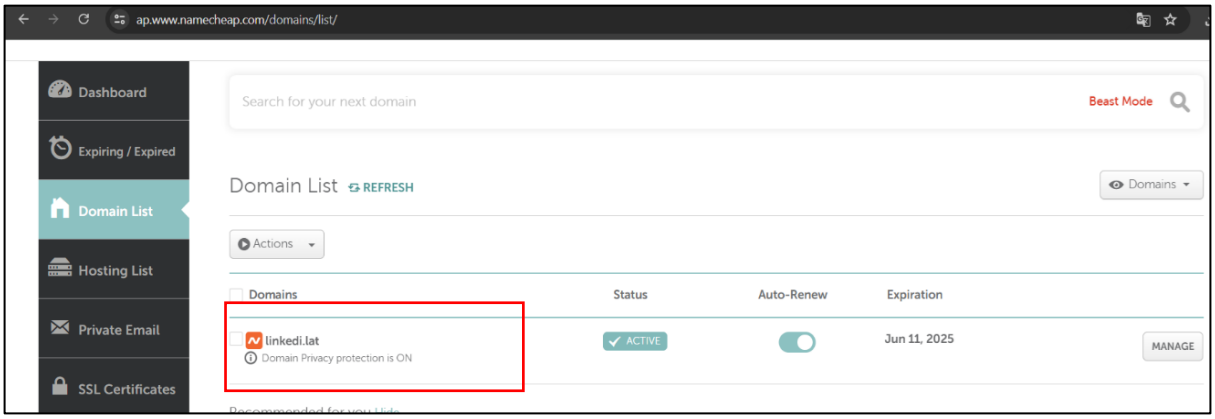
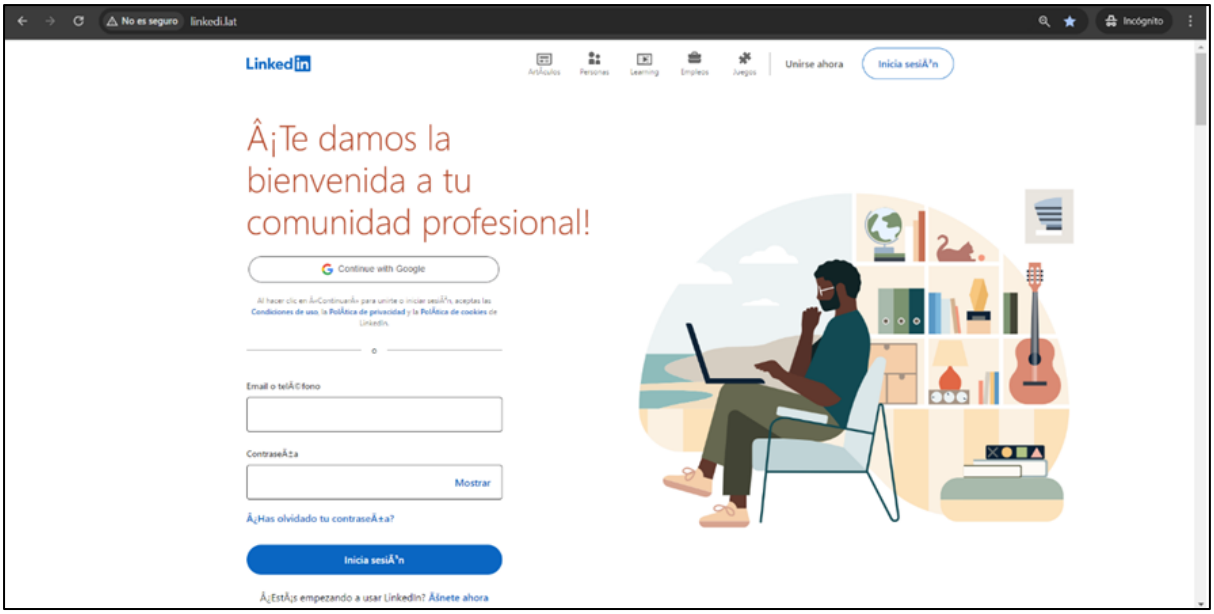


Imagen 013: Selección y compra de dominio similar al URL clonado [Linkedi.lat]



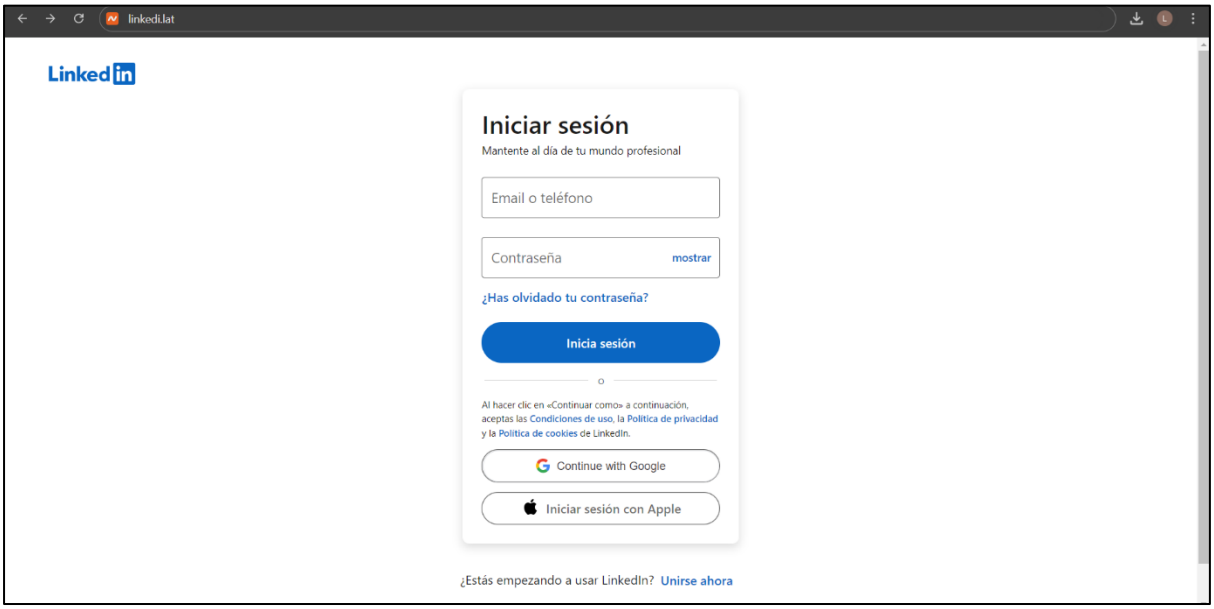


Imagen 14: Sitio web clonado (para evitar desconfiguración ir a pantalla de ingreso de credenciales y clonar ese URL)

11. Técnicas y procedimientos para la recopilación de la información

11.1 Técnicas

Las técnicas utilizadas fueron:

- Recolección de información a través de formularios en línea a través de Microsoft FORMS.

- Recolección de información sobre direcciones IP y credenciales (Dependiendo de que grado de seguridad estuvo dispuesto a arriesgar el usuario) a través de un ejercicio de ingeniería social enviado por WhatsApp y direcciones de correo electrónico.

11.2 Procedimientos.

- ✓ Recolección de información
- ✓ Creación de máquinas virtuales en AWS
- ✓ Lanzamiento de instancias en AWS
- ✓ Compra de dominio
- ✓ Selección de sitio a clonar y estructuración del plan para realizar el ejercicio de ingeniería social.
- ✓ Clonación del sitio y puesta a prueba
- ✓ Finalización de plazo para recolección de información
- ✓ Creación de URL (Link) con vista previa para volver atractiva la propuesta
- ✓ Envío de URL de sitio clonado a través de números y correos de encuestados
- ✓ Monitoreo constante con la instancia conectada
- ✓ Finalización del plazo del ejercicio
- ✓ Generación de reporte de PowerShell
- ✓ Documentación de los resultados.

Considerar dentro de los procedimientos datos importantes como:

- ✓ Clonar URL cuando ya se haya pasado al ingreso de credenciales.
- ✓ Comprar un dominio lo mas parecido a lo que se desea clonar
- ✓ Mantener la máquina virtual encendida durante el proceso de registro ya que si se sale el dominio se cae y por consiguiente no registra ingresos.
- ✓ Registrar de inmediato el correo en NAMECHEAP para evitar que sea suspendido y que no se pueda realizar el experimento.
- ✓ Mantenerse monitoreando constantemente los costos por el uso de la instancia.
- ✓ Redirigir automáticamente para que el objetivo no se entere que fue víctima de phishing.
- ✓ Se pudo identificar que cuando el URL es enviado a usuarios Android es más fácil que sean victimas ya que la URL se mantiene enmascarada con el dominio, caso contrario en el SO IOS ya que automáticamente se abre el URL en el buscador desenmascara el DNS de IPv4 Publico.
- ✓ Para el envío del URL a los objetivos a través de correo electrónico utilizar técnicas de esteganografía u ocultamiento de URL en imágenes que se vean distorsionadas para que la curiosidad del usuario haga que crackeé la imagen.

12. Instrumentos de registro y medición.

Todos los registros y mediciones se obtuvieron a través de los resultados de las encuestas, reportes de loggeo de PowerShell y gráficos generados automáticamente por Microsoft FORMS.

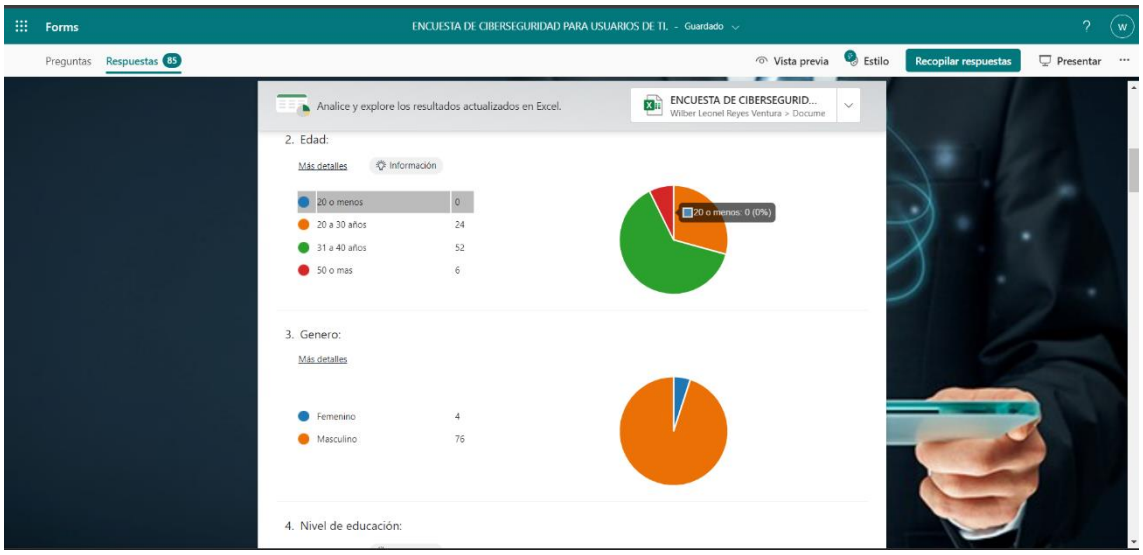
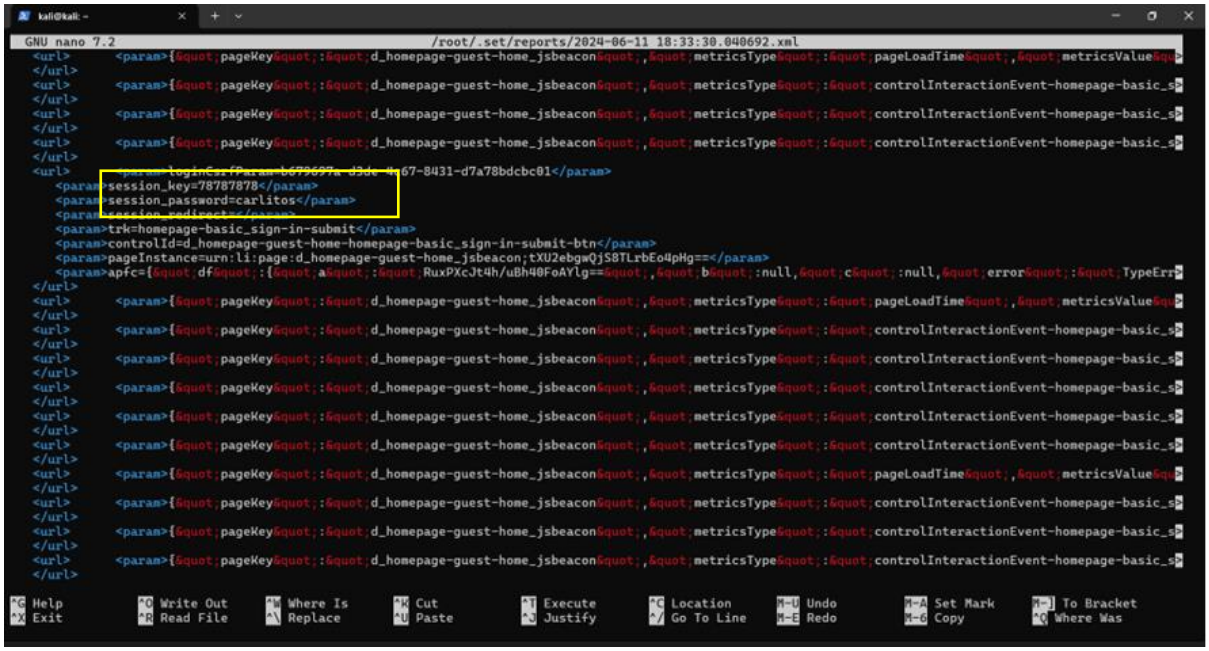


Imagen 015: Gráficos generados en encuestas realizadas.



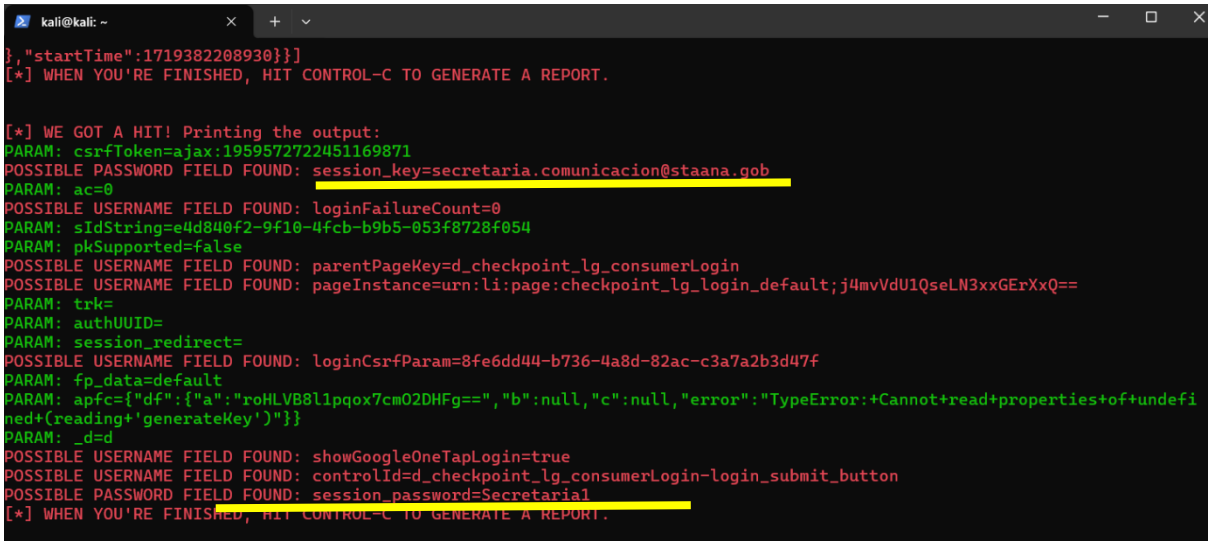


Imagen 016: Reporte generado por Kali Linux de personas que ingresaron al link enviado (Todo el personal vulnerado en sus credenciales fue notificado)

CAPÍTULO IV
ANÁLISIS DE LA INFORMACIÓN

13. Resultados.

13.1 Análisis descriptivo.

Administración Pública:

En lo relativo a la administración pública ha sido notable que en los grupos etarios considerados no existe uno especifico el cual no se arriesgue a darle clic a links desconocidos ya que el 70% de los objetivos controlados para la prueba de ingeniería social (phishing) accedieron al link enviado, no importando hacerlo incluso de medios institucionales, lo que genera un panorama claro de que esta institución en la actualidad tiene una escaza cultura de ciberseguridad y al momento de digitalizar todos sus servicios tendrá problemas de seguridad generados únicamente por los usuarios ya que se convertirán en blancos fáciles para los ciberdelincuentes.

En ningún momento en la página clonada se aplicaron seguros o se utilizó el protocolo HTTPS, lo que debió ser la primera advertencia para los usuarios, pero aun con este aviso el 50% vulnero sus credenciales.

Empresa Privada:

Por otro lado, la empresa privada tuvo un incremento significativo del 2% (72% total) de personas que decidieron ingresar al link enviado a través de WhatsApp y correos electrónicos proporcionados por los encuestados.

El único detalle a considerar es que cuando ingresaron al link y vieron algunos detalles de la página clonada, decidieron colocar “credenciales falsas” y dejar hasta ahí el proceso, es apto reconocer que, aunque escriban credenciales falsas eso no asegura

que no hayan sido infectados, pero eso es lo que comúnmente creen los usuarios que no tienen conocimiento de malwares como las variantes de keyloggers.

En general ambos grupos manifestaron en sus encuestas que no reciben entrenamientos o capacitaciones en materia de ciberseguridad, pero de igual manera manifestaron en varios casos que los ciberataques no son preocupantes para ellos, ambas administraciones deberán hacer un esfuerzo grande para lograr solventar esta falencia que en la actualidad es muy peligrosa para las personas que utilizan tecnologías de información, un error de magnitud considerable, podría afectar la credibilidad de la empresa y eso va a generar diversas pérdidas económicas como materiales.

13.2 Análisis inferencial.

Tanto en la administración pública como en la empresa privada se determinó, que los usuarios más vulnerables son los de 30 a 50+ años, siendo ellos la población mayoritaria encuestada, las estadísticas muestran que este grupo etario es el que menos conocimiento de ciberseguridad posee, posiblemente esto esté vinculado al hecho de creer que se es demasiado “viejo” como coloquialmente se conoce, para adquirir nuevos conocimientos.

Por otra parte, se presentan los datos en los cuales se identifica que el grado académico entre (técnicos y posgrados) fueron víctimas en el ejercicio, muy posiblemente ligado a que, en las universidades o institutos de nivel superior, en la actualidad las medidas de seguridad para dispositivos móviles o computadoras (de forma general) no son parte de los diferentes planes de estudio, es necesario formar parte de una carrera afín a las tecnologías de información para poder tener conocimiento en el tema.

14. Discusión de resultados.

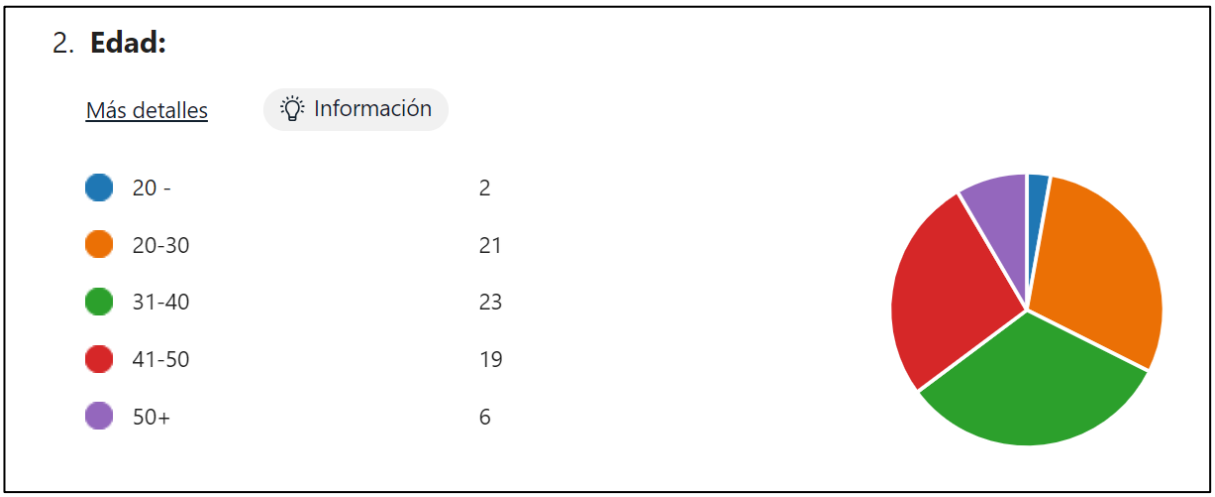
Administración Pública.

Empresa Privada.

Pregunta #1:

En la pregunta inicial en ambos casos (público y privado) se obtuvo datos de correos o números de WhatsApp, vinculados directamente a la empresa a la que pertenecen, posiblemente se deba a que el método de diseminación de la misma fue en coordinación con los respectivos departamentos de tecnología, pero es necesario resaltar que existieron algunos que decidieron vulnerar su información personal y no institucional.

Administración Pública.

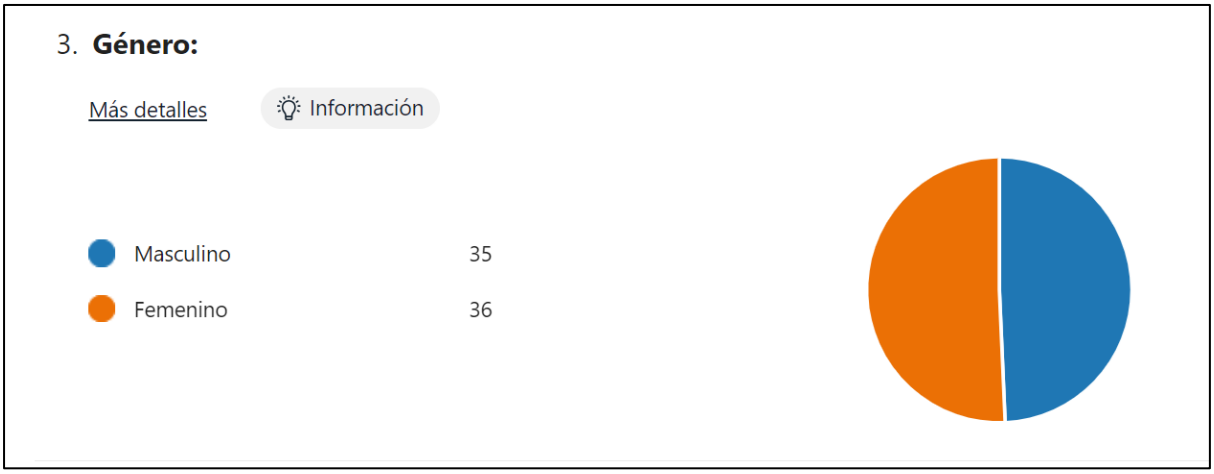


Empresa Privada.

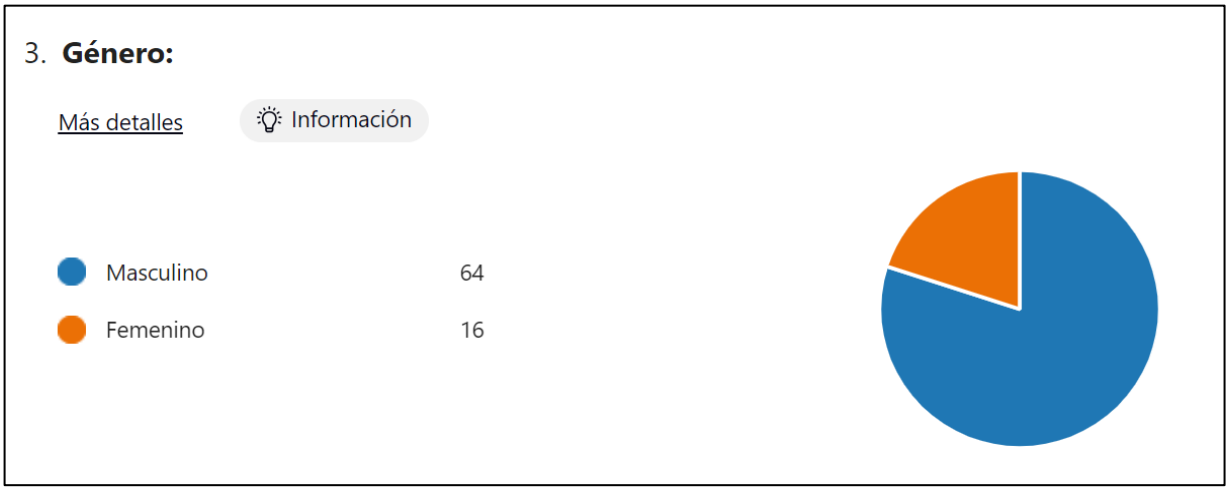
Pregunta #2:

En esta pregunta en ambos sectores (público y privado), se puede observar que la mayoría de sus empleados son mayores de 20 años, importante para conocer el grado de responsabilidad y madurez con la que realicen su empleo.

Administración Pública.



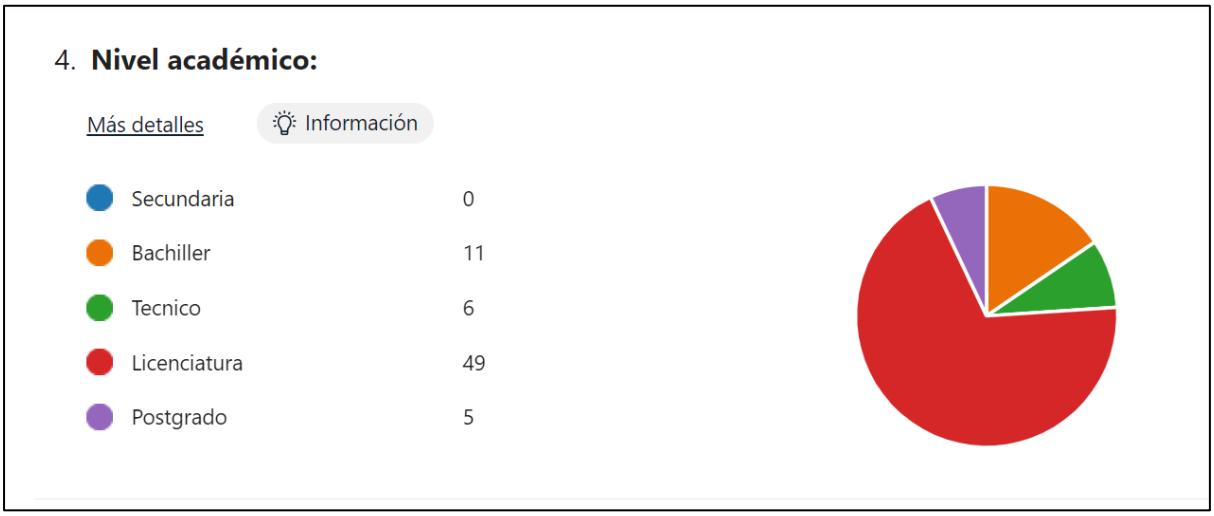
Empresa Privada.



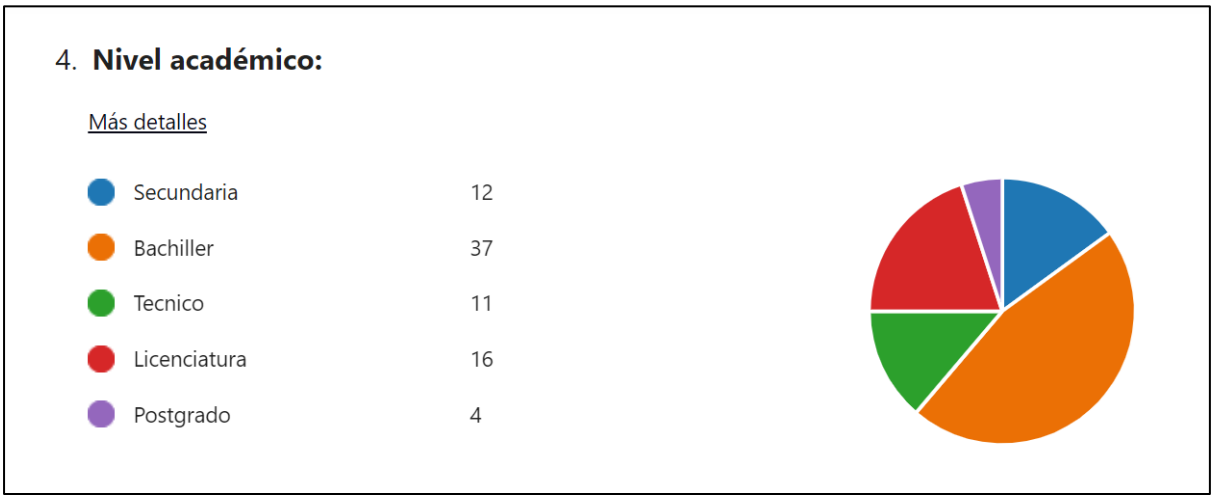
Pregunta #3:

En lo relativo Al género en ambos sectores (público y privado) se puede observar que existe un numero equitativo entre hombres y mujeres en la administración pública y es totalmente marcada la diferencia en la empresa privada, ya que existen mas hombres que mujeres, teniendo en cuenta que no es una empresa que requiera por alguna naturaleza en particular únicamente presencia de hombres.

Administración Pública.



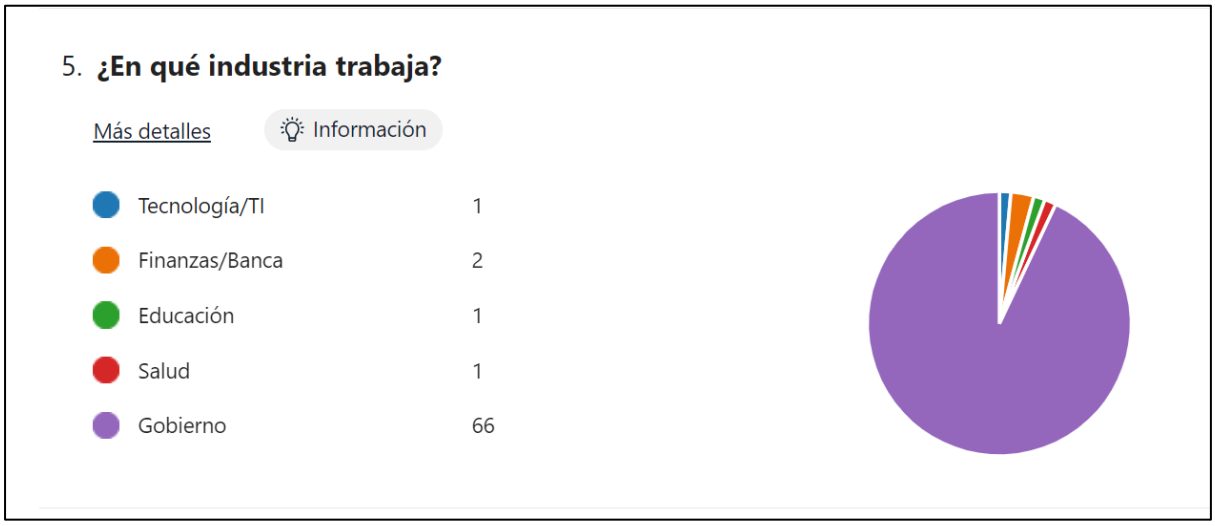
Empresa Privada.



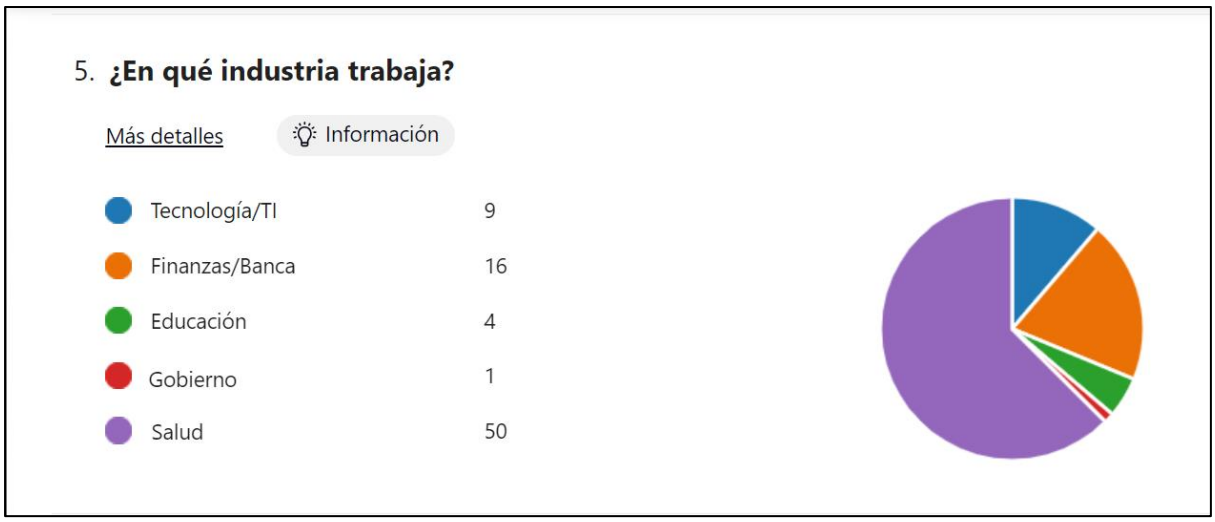
Pregunta #4:

Es preciso destacar que en la actualidad la mayoría de profesionales que laboran tanto en la administración pública como privada, cuentan con estudios de nivel superior, siendo la minoría los estudios de secundaria y bachillerato, por lo cual será un trabajo menos complicado, la comprensión y concientización de una cultura de buenas prácticas en lo relativo a la ciberseguridad.

Administración Pública.



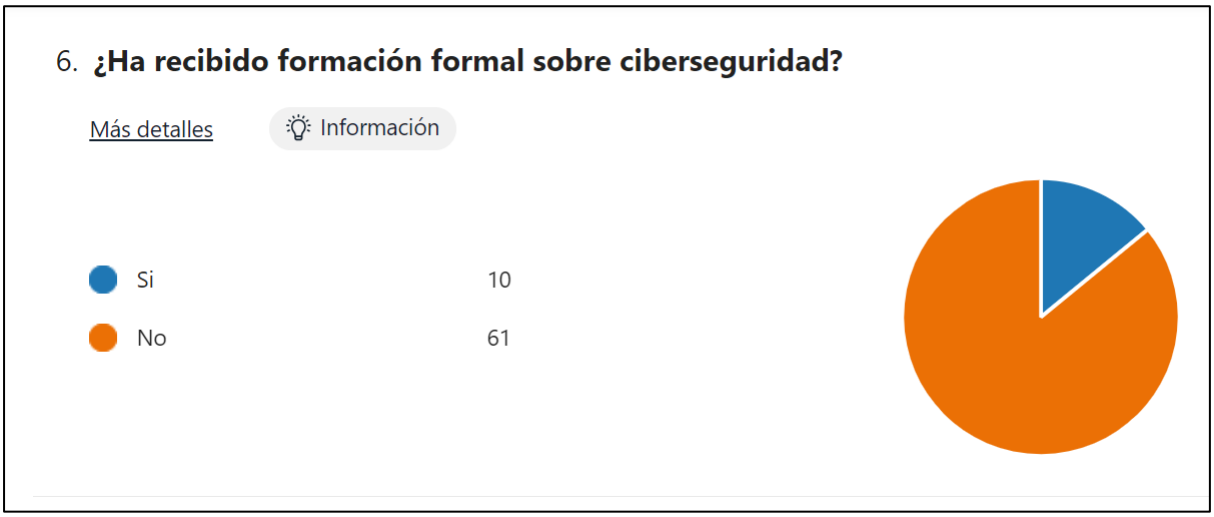
Empresa Privada.



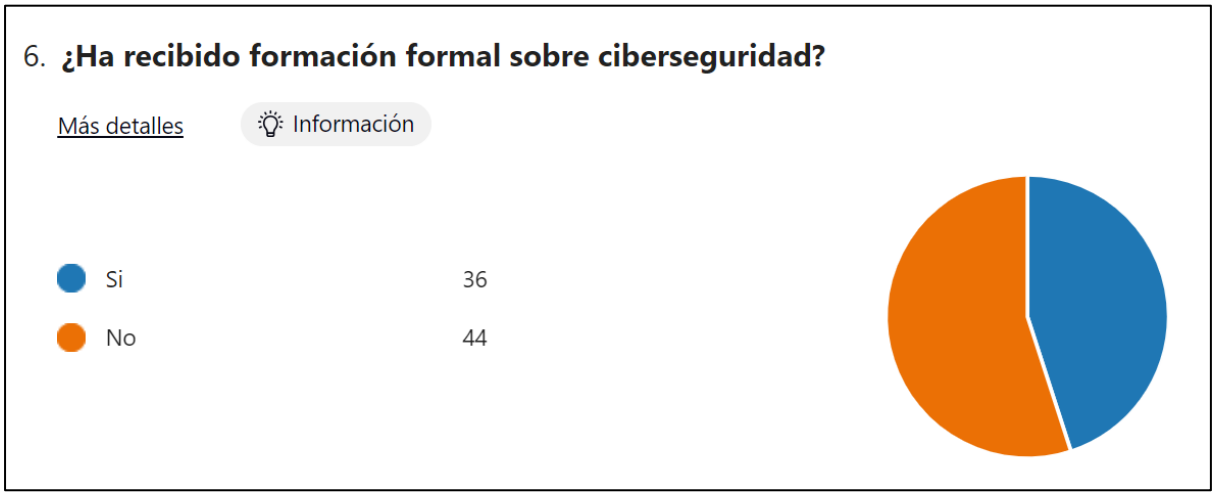
Pregunta #5:

En las respuestas reflejadas se puede apreciar que no se han centrado las encuestas en una población de un departamento especifico de la organización, sino en una diversidad del universo disponible.

Administración Pública.



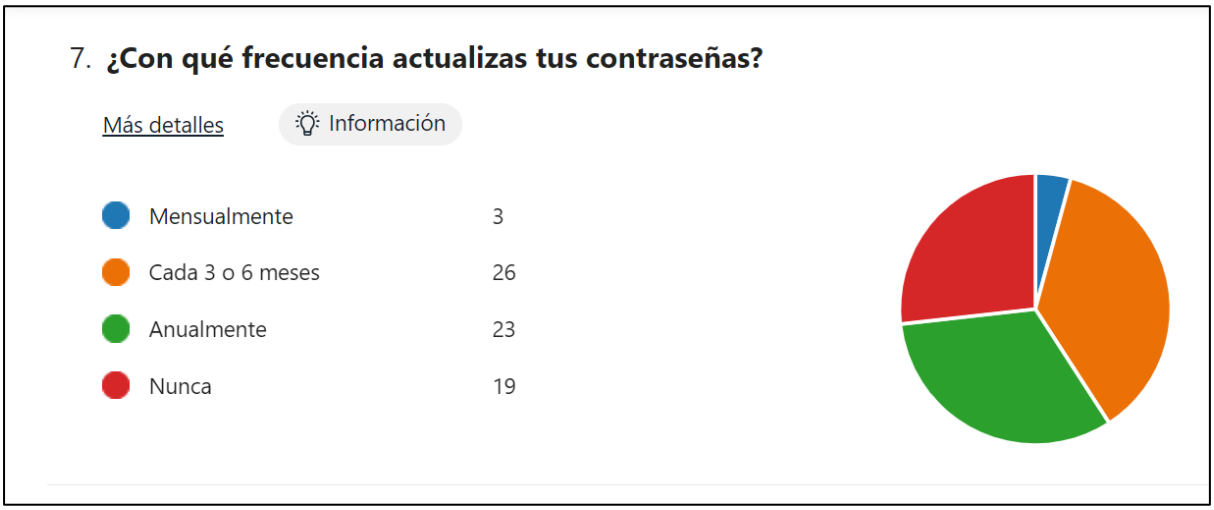
Empresa Privada.



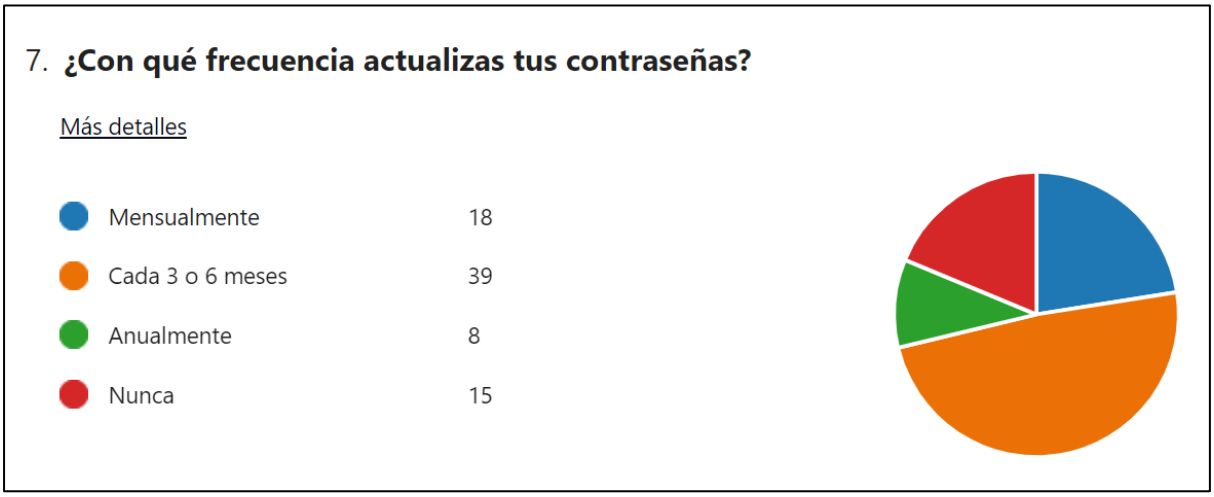
Pregunta #6:

En las respuestas reflejadas en la pregunta #6, se puede observar el porqué de las malas prácticas reportadas por los respectivos departamentos de TI, es un error grave para la época tecnológica que estamos viviendo, dejar de lado las capacitaciones para el personal de las diferentes áreas que utilizan activos con o sin acceso a internet y que poseen información de la organización para la que laboran, en alguna medida el personal de la empresa privada refleja haber recibido formación formal en temas de ciberseguridad.

Administración Pública.



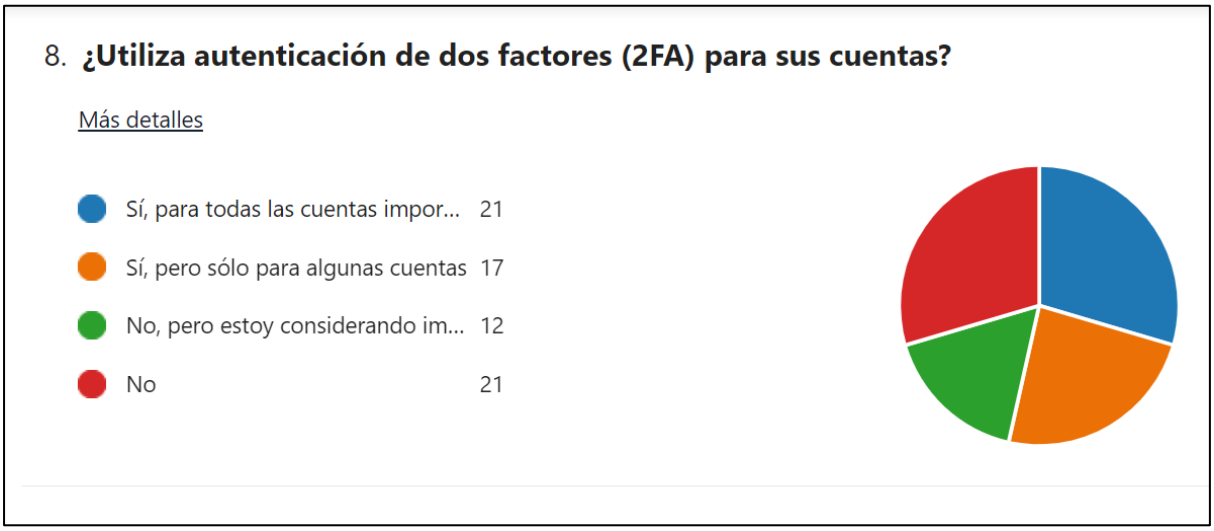
Empresa Privada.



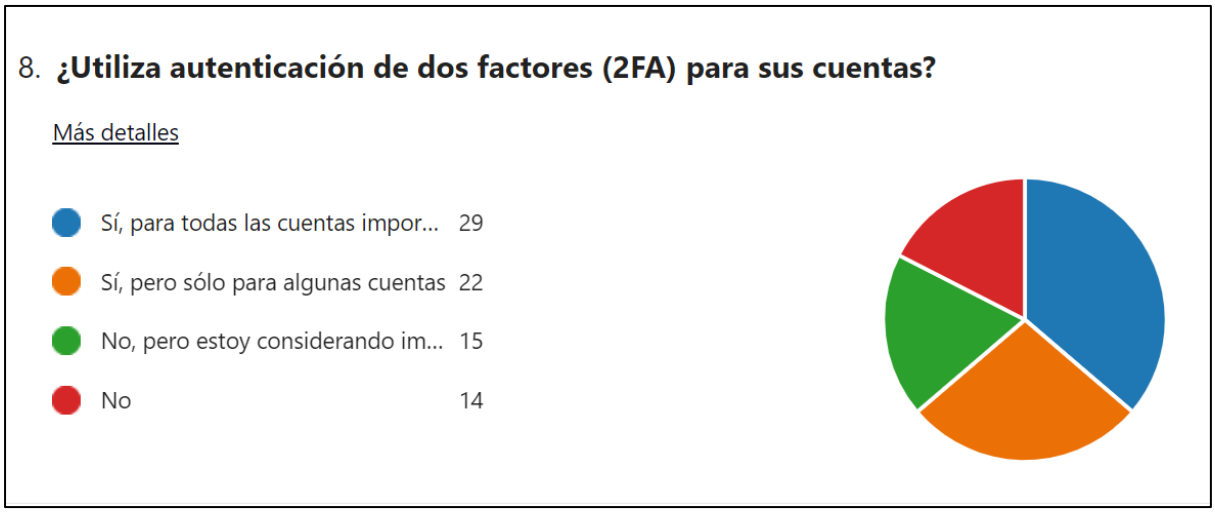
Pregunta #7:

La falta de actualización de contraseñas tanto en lo laboral como en lo privado puede resultar cómodo, pero en cuestiones de seguridad informática, la comodidad y la tibieza en los procedimientos orientados a la prevención son errores que pueden generar problemas serios para las organizaciones, a través de estos gráficos podemos observar que es uno de los problemas que deben corregirse de manera inmediata en ambos sectores.

Administración Pública.



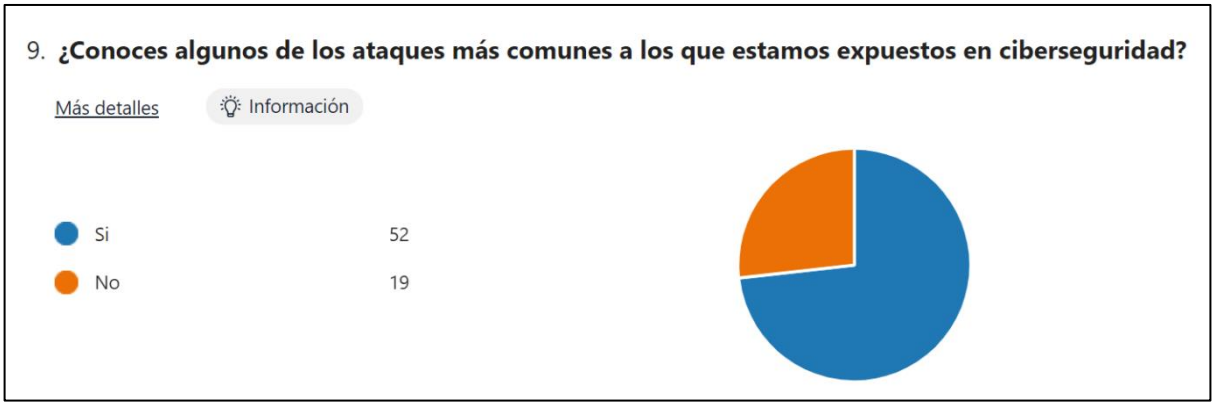
Empresa Privada.



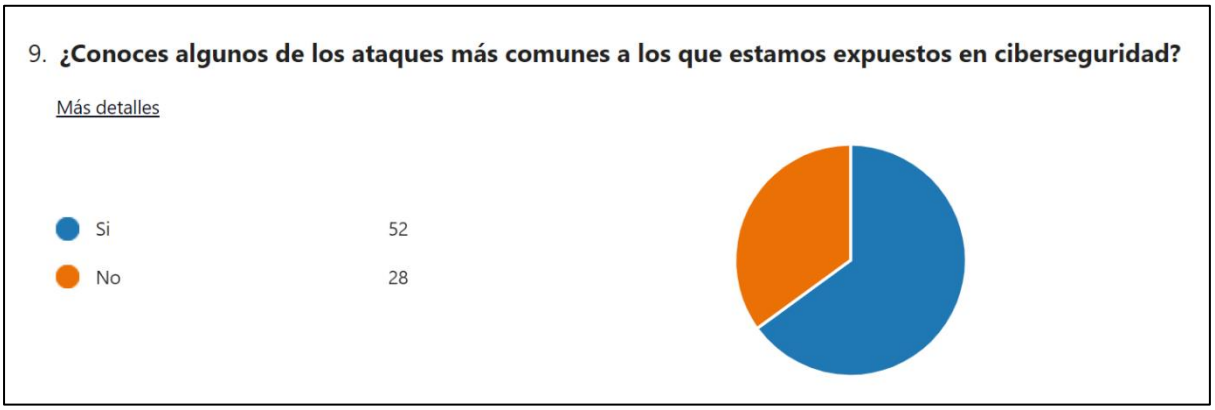
Pregunta #8:

La autenticación de dos factores es un procedimiento el cual, debería en la actualidad ser uno de los procedimientos normales en los parámetros de ingreso a las diferentes plataformas, pero resulta que se ha convertido en algo voluntario y que para los que desconocen su importancia resultara un proceso engorroso e innecesario.

Administración Pública.



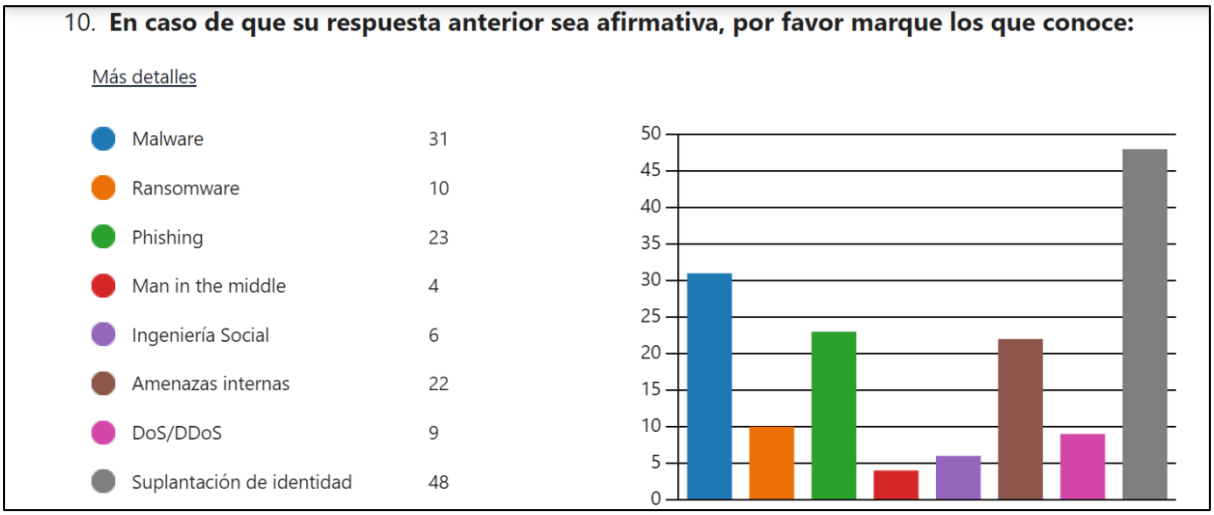
Empresa Privada.



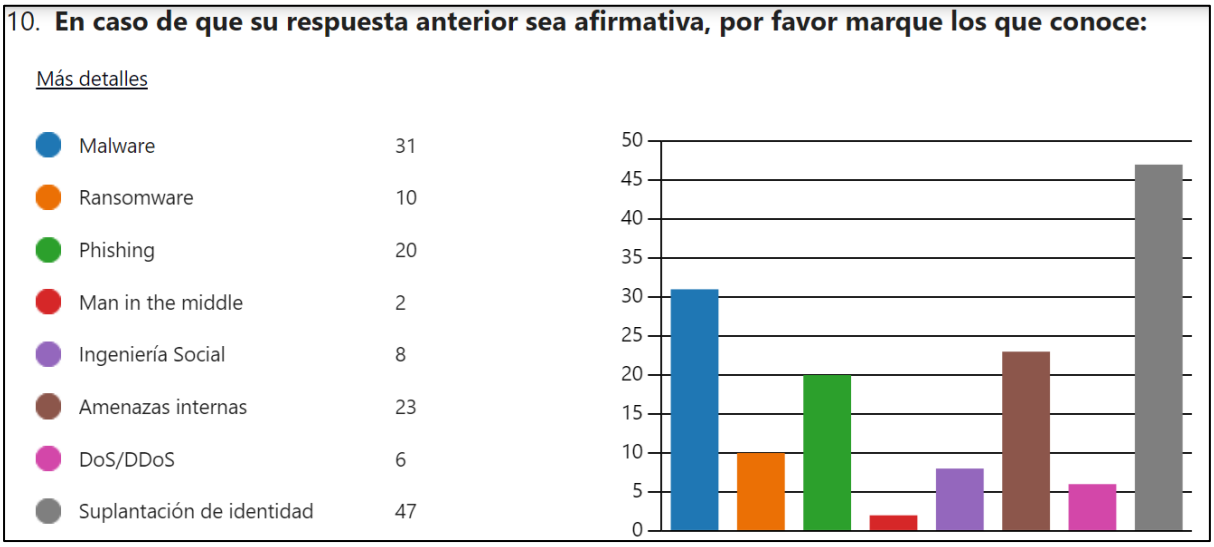
Pregunta #9:

En la pregunta 9 se percibe que de forma leve los participantes han orientado su respuesta únicamente a la suplantación de identidad, de lo cual consideran tener conocimiento, pero existen amenazas mucho más complejas y peligrosas de las cuales no tienen conocimiento y por lo tanto no podrán identificar cuando sean víctimas de los mismos.

Administración Pública.



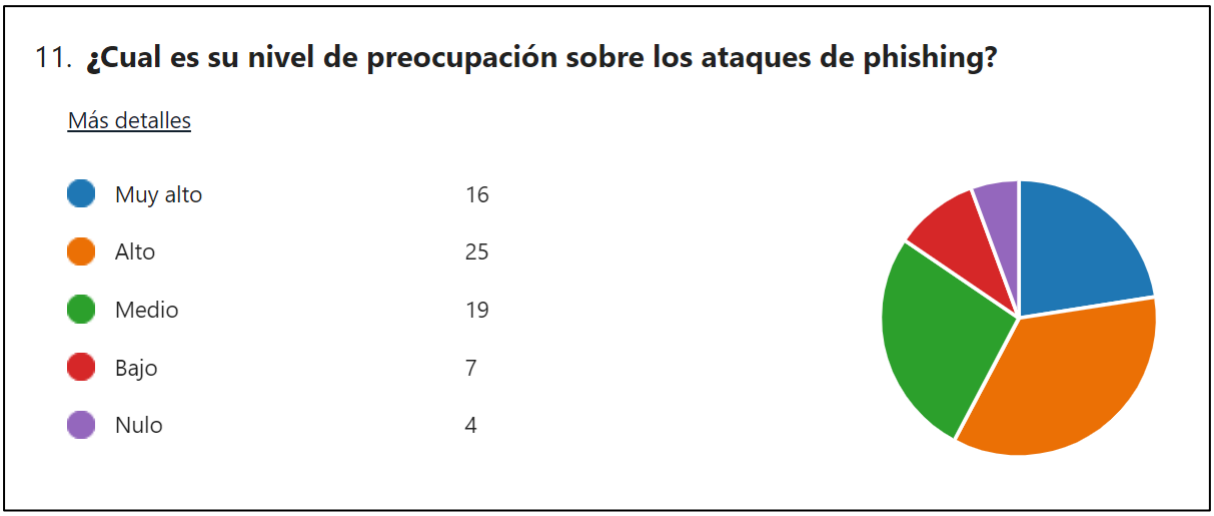
Empresa Privada.



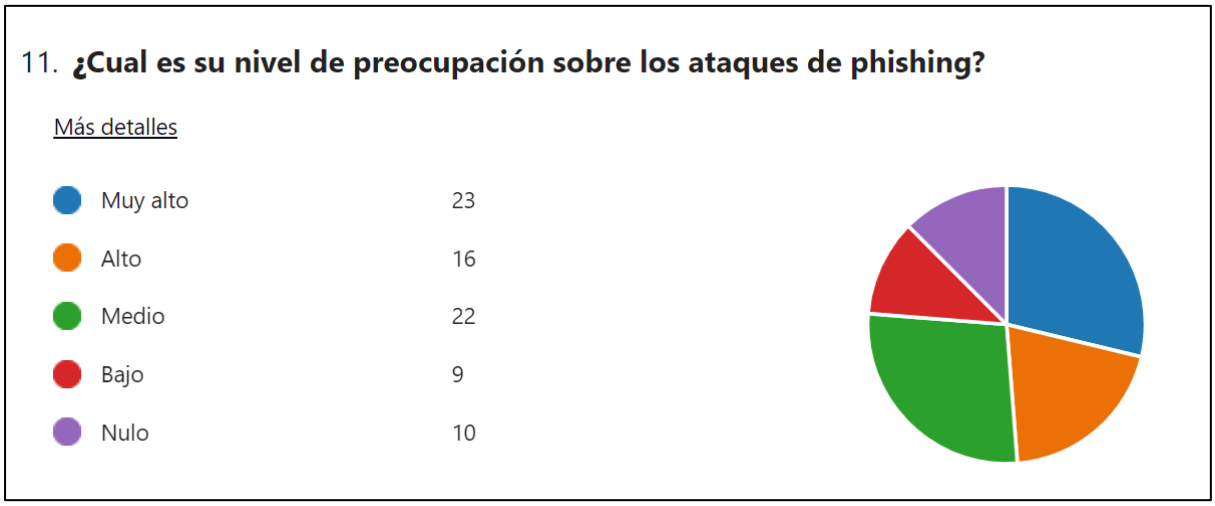
Pregunta #10:

En las respuestas vertidas en la pregunta #10, el grafico nos da un panorama amplio en el cual se puede observar por qué las personas fueron víctimas durante el ejercicio; ya que no poseen conocimiento sobre phishing que es uno de los ataques más comunes en la actualidad por sus efectos positivos para el atacante, aprovechando el desconocimiento del objetivo.

Administración Pública.



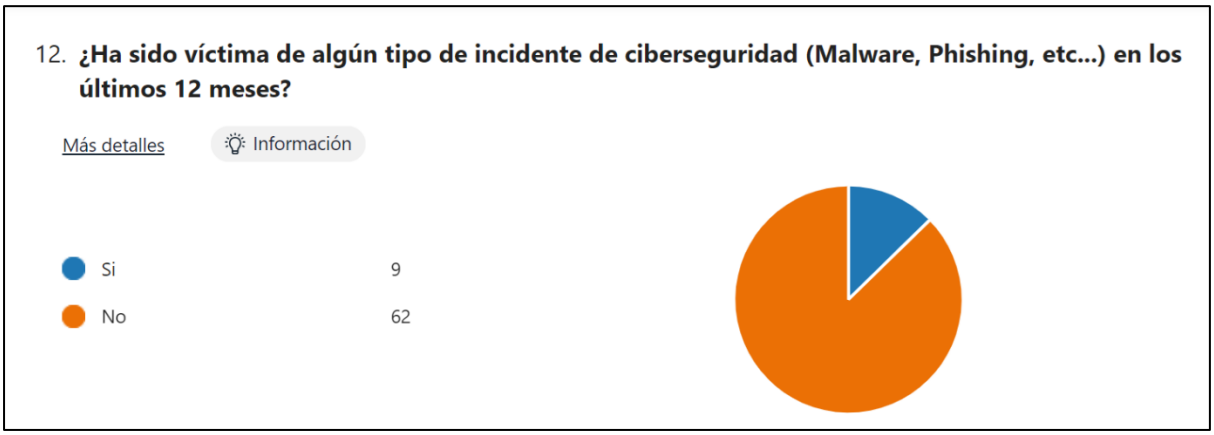
Empresa Privada.



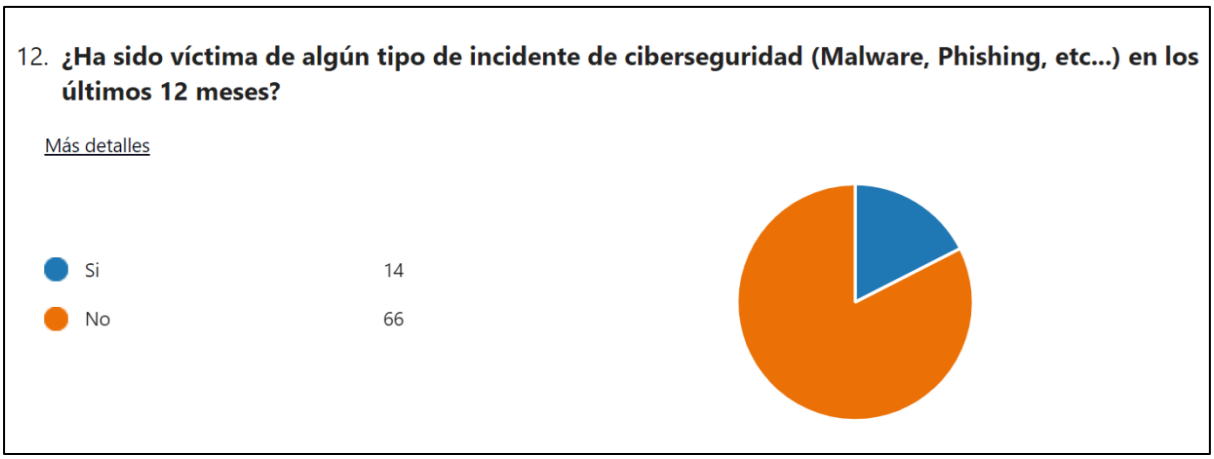
Pregunta #11:

Los gráficos resultados de la pregunta #11, reflejan de forma impactante la preocupación de los usuarios en cuanto al phishing, aunque en las anteriores podemos observar que no conocen cual es el comportamiento o la forma de ataque que se utiliza, es posible que exista una idea general de los usuarios, la cual debe ser aprovechada para orientar los esfuerzos de capacitaciones en el tema.

Administración Pública.



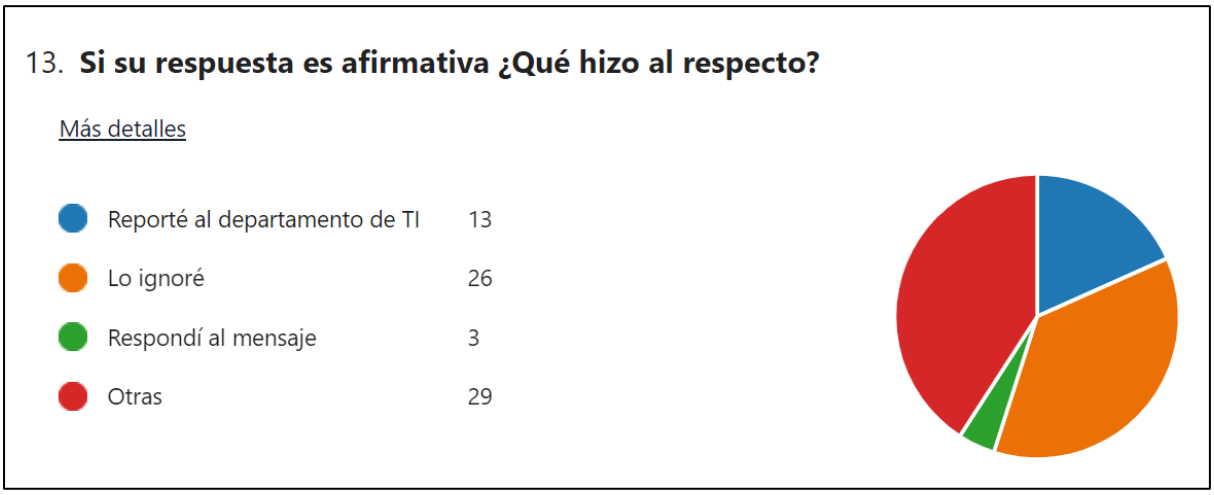
Empresa Privada.



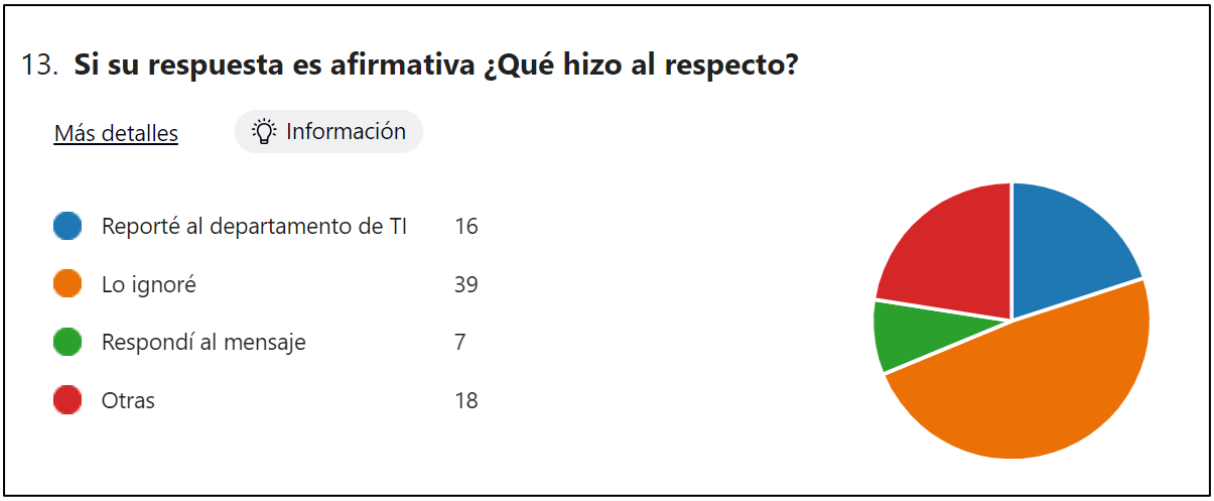
Pregunta #12:

En los grafico de las respuestas a la interrogante #12, se puede interpretar que las personas desconocen si realmente han sido víctimas de ataques de phishing y eso nos queda claro en los reportes generados por PowerShell, al final del ejercicio controlado, ya que fácilmente en una hora teníamos comprometido a más del 60% de los participantes.

Administración Pública.



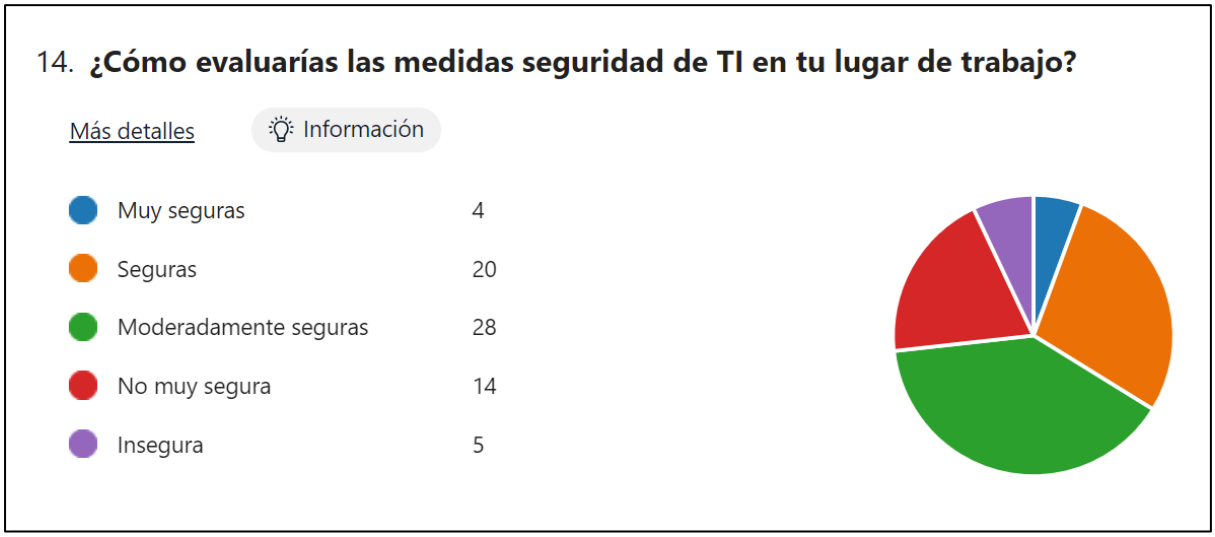
Empresa Privada.



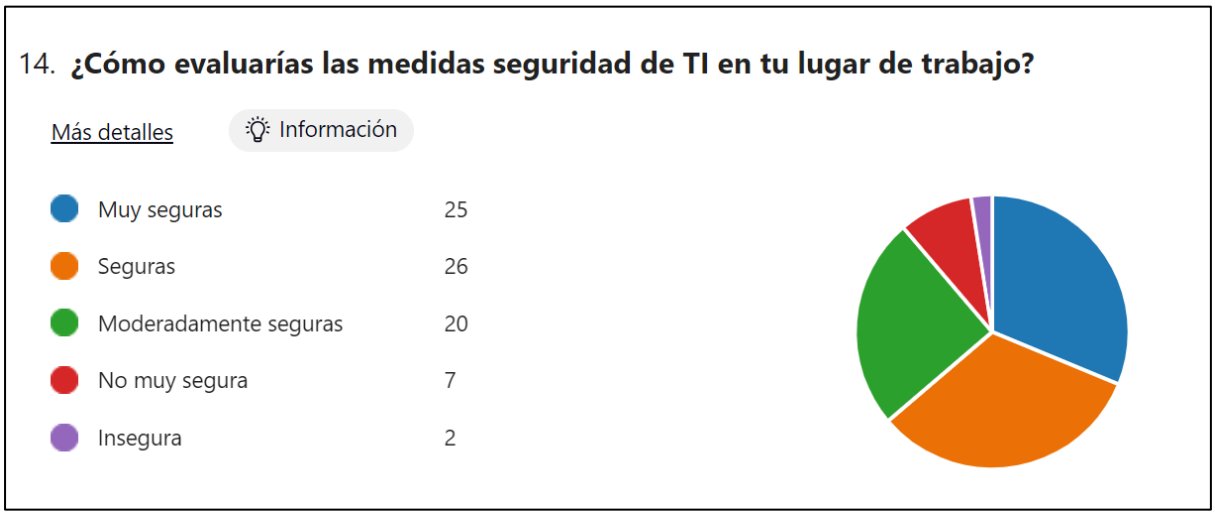
Pregunta #13:

Tras haber dado respuesta positiva a la pregunta #12, los usuarios reflejan en este grafico que lejos de informar a sus respectivos departamentos de tecnologías de información, decidieron tomar otras acciones para intentar y posiblemente resolver el problema de haber sido víctimas de ciberataques.

Administración Pública.



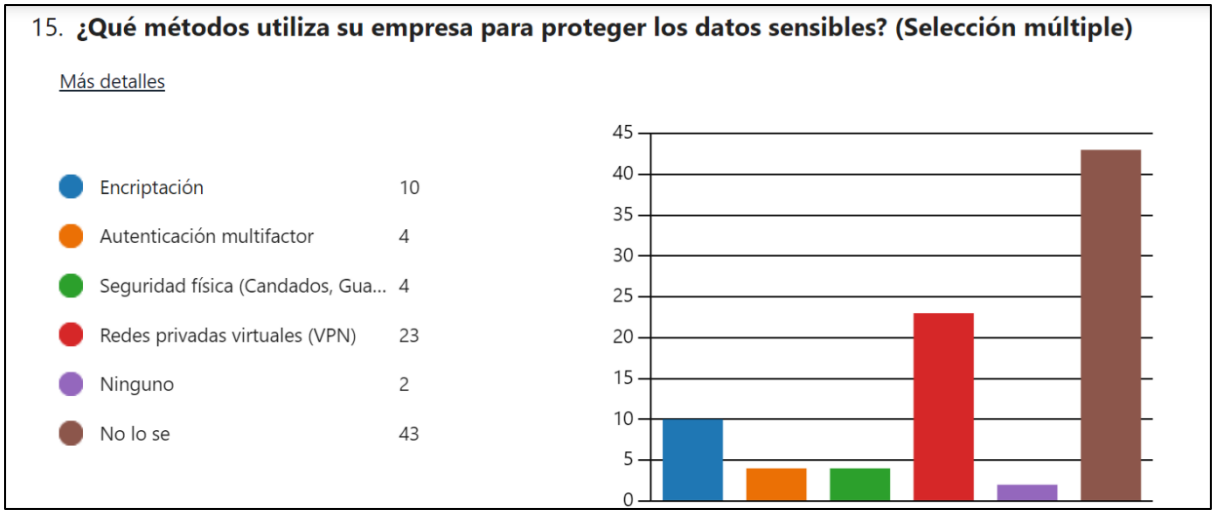
Empresa Privada.



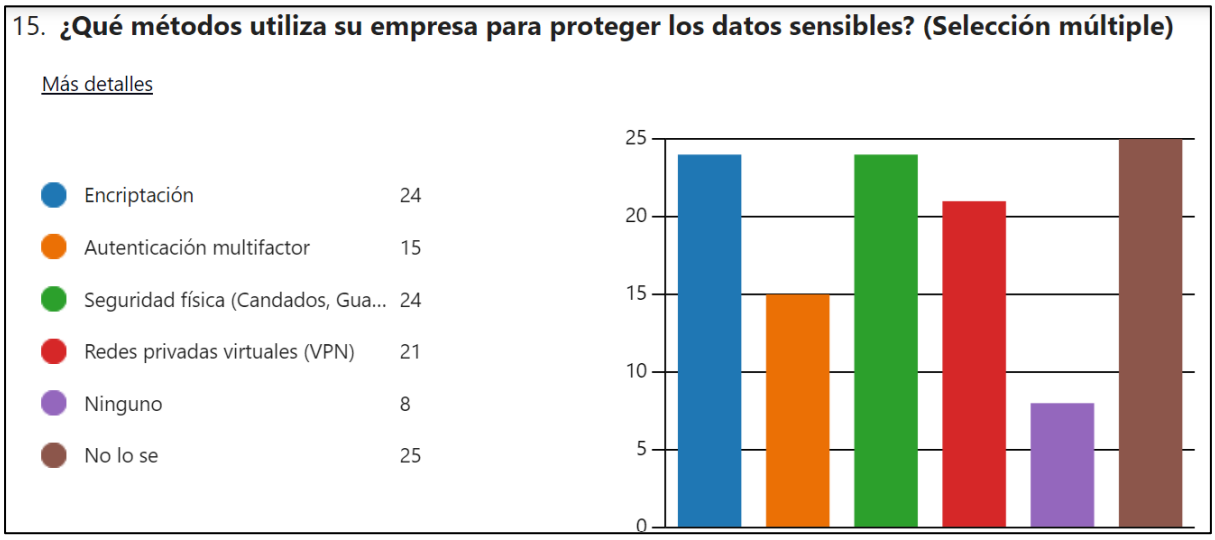
Pregunta #14:

Con respecto a las medidas de ciberseguridad en ambos entornos, se puede concluir que son medianamente aceptadas y percibidas por el universo total de ambas administraciones, esto posiblemente este ligado a la falta de capacitaciones impartidas y a la falta de charlas informativas para tener comunicadas a las personas sobre las acciones que realizan los departamentos de TI, en beneficio de la administración.

Administración Pública.



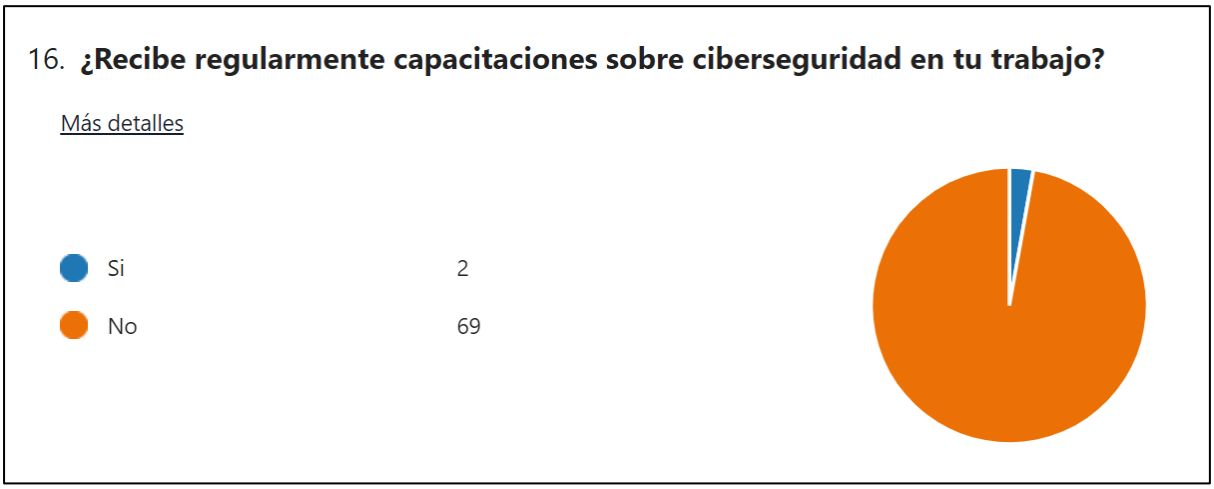
Empresa Privada.



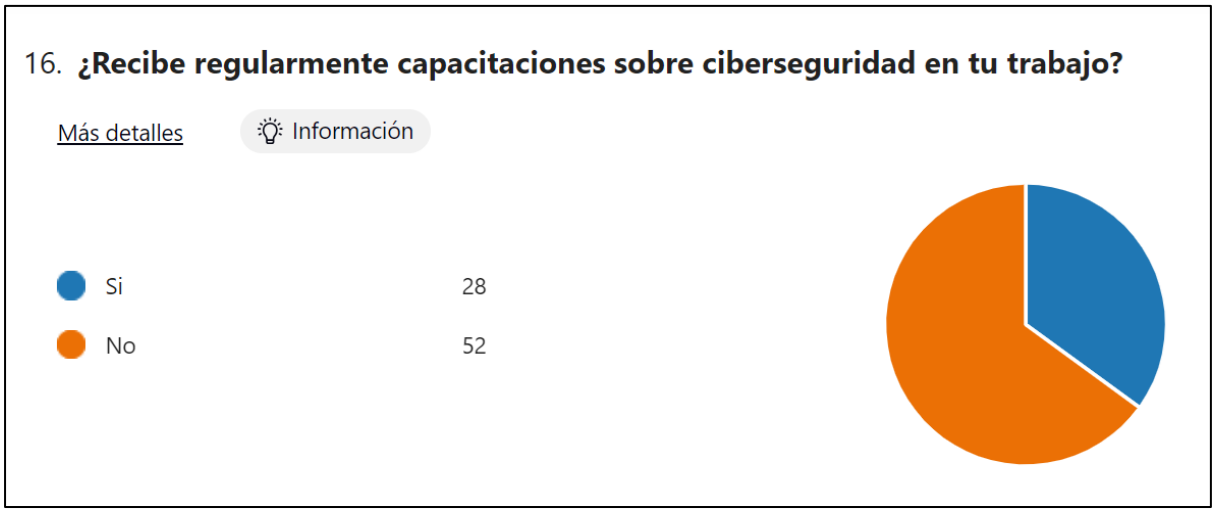
Pregunta #15:

Las campañas de concientización, capacitación y charlas informativas en temas de ciberseguridad son necesarias para evitar panoramas como el acá presentado, en el cual, los miembros de la organización desconocen los esfuerzos constantes realizados por los departamentos de T.I, posiblemente atribuido a la falta de comunicación entre ambas partes (usuarios / técnicos).

Administración Pública.



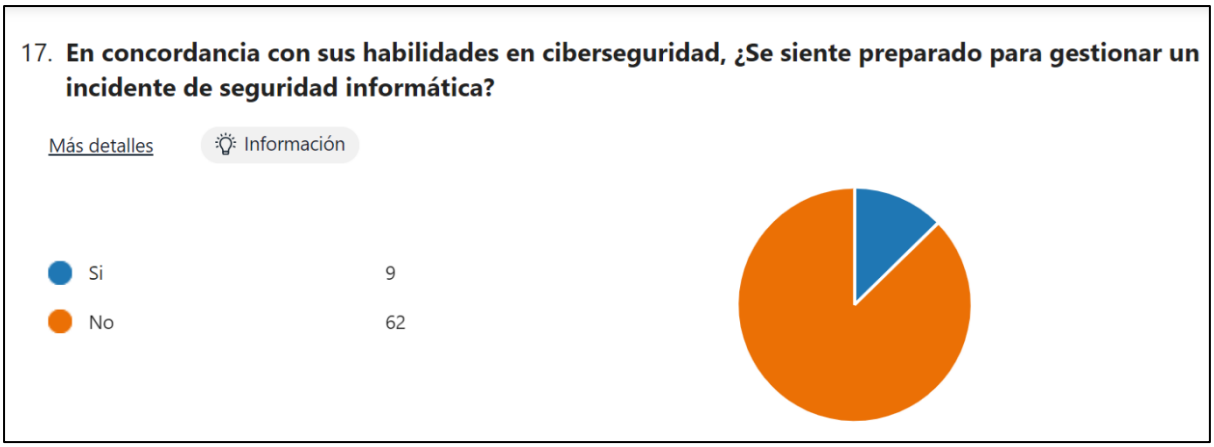
Empresa Privada.



Pregunta #16:

En esta pregunta, las respuestas vertidas son una clara petición a la gerencia institucional, para que el personal sea capacitado en temas de ciberseguridad y de esa forma agudizar sus habilidades en lo relativo a tan importante área.

Administración pública.



Empresa Privada.

Pregunta #17:

Haciendo un vínculo entre pregunta 16 y 17, se observa que el tener un ataque de grandes proporciones, el personal, tomado como muestra de ambas organizaciones, no está preparado para gestionar ningún tipo de ciberataques, lo que debería de preocupar a ambas administraciones, ya que en gran parte de los usuarios depende la seguridad.

Administración pública.

18. **¿Que medidas de ciberseguridad crees que podrían implementar o mejorar en tu lugar de trabajo?**

Más detalles | Información

70
Respuestas

Respuestas más recientes
"Guardar en un servidor municipal"
"."
"capacitaciones"

11 encuestados (**15**%) respondieron **seguridad** para esta pregunta.

Empresa Privada.

18. **¿Que medidas de ciberseguridad crees que podrían implementar o mejorar en tu lugar de trabajo?**

Más detalles | Información

80
Respuestas

Respuestas más recientes
"Hacer un plan sobre ello"
"No tengo idea "
"No se"

7 encuestados (**8**%) respondieron **seguridad** para esta pregunta.

Pregunta #18:

En las respuestas vertidas en la pregunta 18 se puede observar que más del 50% del personal que labora en ambas administraciones (pública y privada) solicitan de forma recurrente, seguridad para sus datos y capacitaciones para todo el personal en materia de ciberseguridad, lo que genera un parámetro amplio en cuanto a las acciones a tomar por el área gerencial y de esa forma evitar posibles incidencias en cuanto a la seguridad informática de sus activos de información (Refiérase a Anexo “C” LISTADO DE SUGERENCIAS POR PERSONAL ENCUESTADO).

CAPÍTULO V

CONCLUSIONES Y RECOMENDACIONES

14. Conclusiones.

En conclusión, en la actualidad tanto en la administración pública como en la empresa privada se necesita que el personal que labora en las mismas, este capacitado para poder desempeñar de forma plena sus funciones y evitar de esa forma caer en errores de seguridad que vulneren información o algún otro activo de valor para la organización, durante nuestra investigación inicialmente tuvimos problemas en cuanto a los permisos ya que en una de las administraciones el personal de TI, trató de evitar que se encuestara al personal de la empresa; porque las encuestas están orientadas a saber el nivel de conocimiento actual y a identificar si el personal es capacitado, ya que los departamentos de TI en su planificación anual reflejan que las capacitaciones serán impartidas, la situación se pudo solventar para la realización de las mismas pero es prudente que en la medida de lo posible se permitan este tipo de estudios que no son invasivos en sus sistemas, para poder tener una opinión externa sin necesidad de entrar en auditoria.

Las ciberamenazas son cada vez mayores y en una sociedad que tuvo que avanzar a pasos gigantes hacia una digitalización forzada, es imperante que en las universidades y centros de formación en los niveles respectivos se incluyan medidas de seguridad de dispositivos móviles o en otro sentido tecnologías de información como parte de la planificación educativa y así generar un ambiente de buenas prácticas en los alumnos.

El Salvador al ser el único país de la región en poseer el BTC como moneda de curso legal, debe implementar de forma continua la capacitación gratis para todas las personas no importando las edades que sean usuarios de ti, ya se están realizando

algunos esfuerzos a través de su secretaria de innovación, pero es importante que se den a conocer al público en general para que puedan ser aprovechadas, por otro lado la influencia directa de personas con diferentes intenciones que publican contenido en redes sociales se convierten en uno de los principales problemas, ya que los usuarios no escatiman esfuerzo alguno por seguir lo que sus “influencers” favoritos divulgan como tendencia, por tal razón se nos facilitó ya que se crearon diferentes vistas previas en los links enviados que iban desde moda, farándula, accidentes, ciberataques (caso de las vallas publicitarias Mayo 2024) y situación de lluvias en El Salvador.

Finalmente se concluye que las personas neófitas en TI representan un riesgo no aceptable en las empresas para las que laboran (sean públicas o privadas) y eso conlleva a que los cibercriminales se encuentren en constante acoso hacia esas entidades, al conocer que sus empleados no poseen conocimiento sobre cómo gestionar o evitar ser víctimas de ciberdelincuencia.

15. Recomendaciones.

- A las entidades tanto públicas como privadas que nos permitieron desarrollar la investigación sobre las consecuencias del desconocimiento de las buenas prácticas en lo relativo a ciberseguridad, se les recomienda considerar los datos obtenidos en las encuestas y que de esa forma, puedan orientar el esfuerzo particular de cada participante, para formar a sus empleados con conocimientos al menos generales con el propósito de evitar errores en el uso de tecnologías de información, de esa forma igualmente van a prevenir el riesgo de que la empresa para la que laboran vaya a tener pérdida de credibilidad ya que es un parámetro que difícilmente podrían recuperar a la vista de los usuarios finales.

- La Educación en materia de tecnología, no debería de privarse únicamente a las carreras afines o a niveles educativos específicos, ya para el año 2024 puede considerarse un error grave que personas de diferentes edades (niños, jóvenes, adultos y ancianos) no tengan al menos conocimiento general de los riesgos que supone la manipulación de tecnologías de información, sin tomar las medidas de seguridad básicas, si bien es cierto en la actualidad existen diferentes tipos de controles de las empresas sobre sus activos de información, pero las excepciones a las reglas que se atribuye el personal técnico es una de las fallas más comunes.

- Las normas de seguridad para las personas que utilizan tecnologías de información, se encuentran a disposición de quien quiera leerlas en la web pero esto no resulta ser atractivo pues nadie se encuentra impulsando el efecto (consecuencia) a los diferentes tipos de audiencia, por eso es recomendable que posterior a la emisión de la guía amigable para la gestión de riesgos informáticos, se dé a conocer si es posible

a nivel nacional, para que pueda ser aprovechada por personas de diferentes organizaciones y edades.

16. Fuentes De Información Consultadas.

1. CONED-UNICEF. (2016). *Plan El Salvador educado.* Obtenido de https://www.unicef.org/elsalvador/media/1236/file
2. Diario El Mundo. (Febrero de 2021). *El Salvador alcanzó los 3.8 millones de usuarios de internet en 2020*. Obtenido de https://diario.elmundo.sv/Econom%C3%ADa/el-salvador-alcanzo-los-3-8-millones-de-usuarios-de-internet-en-2020
3. ESET. (2021). *Informe tendencias en ciberseguridad 2021.* Obtenido de https://www.eset.com/fileadmin/ESET/ES/Landings/Whitepapers/Tendencias_en_ciberseguridad_ESET_2021_opt.pdf
4. Fiscalia General de la Republica de El Salvador y UNODC. (2018). *Escuela FGR.* Obtenido de https://escuela.fgr.gob.sv/wp-content/uploads/leyes-nuevas/analisis-juridico-de-la-ley-especial-contra-los-delitos-informaticos-y-conexos-COMPLETO-CAP-I-II-III-V.pdf
5. IBM-Informe Coste de la vulneración de datos. (2023). *IBM.COM.* Obtenido de https://www.ibm.com/es-es/reports/data-breach
6. KASPERSKY. (2024). *Las siete amenazas principales de ciberseguridad a las que debes estar atento.* Obtenido de https://latam.kaspersky.com/resource-center-threats/top-7-cyberthreats
7. Martinez, C. D. (24 de Octubre de 2017). *MEDIUM-Historia del Internet en El Salvador*. Obtenido de https://medium.com/@carl.d/historia-del-internet-en-el-salvador-53fc94ba508c
8. Ponemon, A. S. (2018). *The cost of cybercrime. Ninth annual cost of cybercrime study.* Obtenido de https://newsroom.accenture.com/news/2019/malware-and-malicious-insiders-accounted-for-one-third-of-all-cybercrime-costs-last-year-according-to-report-from-accenture-and-ponemon-institute
9. Rivera, L. L. (11 de Febrero de 2022). *Reformas a leyes penales de El Salvador.* Obtenido de https://novislegal.com/%EF%BF%BCciberdelitos-reformas-a-leyes-penales-de-el-salvador/#:~:text=Ley%20de%20Delitos%20Inform%C3%A1ticos%20y%20Conexos%20(LEDIC).,como%20c%C3%B3digo%20malicioso%2C%20virus%20inform%C3%A1tico.

ANEXO “A”

SIGNIFICADO DE SIGLAS Y ACRONIMOS EMPLEADOS EN ESTE DOCUMENTO

IBM : International Business Machines

TI : Tecnologías de la Información

WEB : World Wide Web

UNICEF : Fondo de las Naciones Unidas para la Infancia

SIGET : Superintendencia General de Electricidad y Telecomunicaciones

EHPM : Encuesta de Hogares de Propósitos Múltiples

MINED : Ministerio de Educación Ciencia y Tecnología

FGR : fiscalía general de la Republica

LEDIC : Ley Especial contra Delitos Informáticos y Conexos

ANTEL : Administración Nacional de Telecomunicaciones

CONACYT : Consejo Nacional de Ciencia y Tecnología

FUSADES : Fundación Salvadoreña para el Desarrollo Económico y Social

SVNET : Administración del dominio de nivel superior SV

UUCP : Unix to Unix CoPy

UUNET : Compañía proveedora de Internet estadounidense fundada en 1987

RACSA : Radiográfica Costarricense, S.A.

UDB : Universidad Don Bosco

UNODC	**:**	Oficina de las Naciones Unidas contra la Droga y el Delito
ESET	**:**	Essential Security against Evolving Threats
AWS	**:**	Amazon Web Services
IP	**:**	Protocolo de Internet
URL	**:**	Localizador de Recursos Uniforme
HTTPS	**:**	Protocolo seguro de transferencia de hipertexto
BTC	**:**	Código bursátil y abreviatura del sistema Bitcoin

ANEXO “B”

GLOSARIO DE TERMINOS TECNOLOGICOS EMPLEADOS EN ESTE DOCUMENTO

Tecnologías de la Información: Un conjunto de dispositivos, de servicios y de actividades que se apoyan en equipos de computación para realizar la transformación de datos en información digital. Por esta razón, conocer lo que implican estos equipos, así como la diversidad de aplicaciones, facilita su exitosa implementación dentro de las organizaciones.

Ciberseguridad: Es la práctica de defender las computadoras, los servidores, los dispositivos móviles, los sistemas electrónicos, las redes y los datos de ataques maliciosos. También se conoce como seguridad de tecnología de la información o seguridad de la información electrónica.

Cibercrimen: Es una actividad delictiva que se dirige a una computadora, una red informática o un dispositivo en red, o bien que utiliza uno de estos elementos. La mayor parte del cibercrimen está cometido por cibercriminales o hackers que desean ganar dinero.

Ciber amenaza: Es una acción maliciosa que se realiza en un entorno digital que tiene como objetivo perjudicar la seguridad de la información de una persona u organización y utilizarla con fines lucrativos y malintencionados.

Ciberataque: Es un acto deliberado de infiltración en sistemas informáticos, redes o dispositivos con la finalidad de acceder o dañar sistemas informáticos, redes, dispositivos o datos digitales; y robar o manipular información confidencial o recursos digitales.

Neófito: Persona principiante, recién incorporado a un cargo, oficio o profesión.

Administración Pública: Conjunto de órganos y entidades que, encuadrados en el gobierno estatal, autonómico o local, sirven con objetividad los intereses generales ejecutando las leyes y prestando los servicios públicos correspondientes.

Ingeniería Social: Es una técnica de manipulación que aprovecha el error humano para obtener información privada, acceso a sistemas u objetos de valor. En el caso del delito cibernético, estas estafas de "hackeo de humanos" tienden a hacer que los usuarios desprevenidos expongan datos, propaguen infecciones de malware o den acceso a sistemas restringidos. Los ataques pueden ocurrir en línea, en persona y a través de otras interacciones.

Buenas Prácticas: En ciberseguridad son medidas y acciones diseñadas para proteger sistemas, redes y datos contra ataques cibernéticos.

Hacker Informático: es alguien con habilidades avanzadas en computación y programación que utiliza su conocimiento para penetrar en sistemas informáticos de manera ilegal o no autorizada. Estos hackers pueden realizar actividades como robo de datos, interrupción de servicios, o incluso actividades más peligrosas como sabotaje cibernético.

Malwares: También conocidos como software malicioso, son programas diseñados específicamente para dañar, alterar, robar información o infiltrarse en sistemas informáticos sin el consentimiento del usuario.

Kali Linux: Es una distribución de Linux basada en Debian diseñada específicamente para pruebas de penetración y auditoría de seguridad.

Phishing: Es una forma de ciberataque en la cual los atacantes intentan engañar a las personas para que divulguen información personal, como contraseñas, números de tarjetas de crédito u otra información sensible. Usualmente, el phishing se lleva a cabo a través de correos electrónicos fraudulentos, mensajes de texto, llamadas telefónicas o incluso a través de mensajes en redes sociales.

Lanzar una instancia desde AWS: Refiérase a crear y gestionar máquinas virtuales de manera flexible y escalable en la nube, proporcionando los recursos informáticos necesarios para tus aplicaciones y cargas de trabajo específicas.

Clonación de un sitio web: Es el proceso de copiar o replicar todo el contenido y la funcionalidad de un sitio web existente para crear una réplica exacta o una versión similar. Esta práctica puede tener varios propósitos legítimos y técnicas asociadas, pero también puede plantear problemas éticos y legales si se realiza sin permiso del propietario del sitio original.

Reporte en PowerShell: se refiere a un documento o archivo que contiene información detallada sobre algún aspecto del sistema, procesos, o resultados de ejecuciones de comandos o scripts, es importante considerar la seguridad y la privacidad de la información que se está manejando.

ANEXO “C”

LISTADO DE SUGERENCIAS POR PERSONAL ENCUESTADO.

Administración Publica

¿Qué medidas de ciberseguridad crees que podrían implementar o mejorar en tu lugar de trabajo?

1. Ignoro
2. Monitorear que no haya dos equipos con el mismo usuario
3. Claves
4. Trataría de informarme con la Unidad de Innovación
5. Código QR
6. Proteger el correo electrónico
7. No abrir correos desconocidos o que solicitan información personal
8. Encriptación
9. Accesos limitados a sitios web
10. Seguridad física y autenticación multifactorial
11. Accesos limitados.
12. Elaborar políticas de seguridad, y también instalar antivirus en todos los equipos
13. Actualización y resguardo completa de información en todas las unidades y departamentos,
14. Restricción del acceso tal cual está a nivel de usuarios del sistema informático
15. Protección de Hardware y Software
16. Monitoreo constante de computadoras y alertas de limites
17. Controlar el acceso a la información
18. Capacitaciones constantes y pruebas para testear la capacidad de defenderse ante un ataque. Y boletines informativos para los demás empleados fuera del área de sistemas.
19. La autenticación de multifactorial
20. Implementación de mejores políticas de acceso y actualización de contraseñas
21. Capacitaciones sobre ciberseguridad y elaboración de políticas sobre el tema
22. Las que sean más optimas y eficientes
23. Utilizar un software anti ataques cibernéticos
24. Dar capacitaciones constantes referente a la ciberseguridad
25. Autentificación en 2 pasos y antivirus para malware y ransomware
26. Capacitar a las diferentes unidades para poder identificar ese tipo de problemas.
27. No se tiene conocimiento de cuales medidas se pueden implementar
28. Incorporar medidas de seguridad adicionales a las que ya se cuentan.
29. Más contraseñas
30. Capacitar al personal en cuanto a las medidas de prevención correspondientes para evitar incidentes que se origen cibernético.
31. Capacitar a todo el personal para saber cómo reaccionar ante un cyber ataque
32. Capacitación integral del sistema que se utiliza
33. Capacitaciones sobre cómo protegernos y sobre las repercusiones a las que se podría llegar

34. No abriendo enlaces desconocidos
35. Capacitación
36. Cambiar contraseñas regularmente
37. Respaldo digital de la información de la Institución

38. Capacitaciones y encriptar información
39. Contratar una empresa
40. Capacitación para conocer más del tema
41. No lo sé
42. Mayor restricción a usuarios
43. Fortalecimiento del Firewall
44. Capacitar al personal
45. Capacitaciones enfocadas en medidas para la protección de información y datos.
46. NA
47. Proteger el correo electrónico, hacer copias de seguridad o respaldos, controlar el acceso de información, colocar antivirus
48. Actualizaciones constantes de los programas y poder doblar las medidas de seguridad que comúnmente se tienen
49. Capacitación sobre ciberseguridad al personal
50. No se
51. Implementar sistema de encriptación
52. Implementar capacitaciones formales a los usuarios
53. Capacitaciones con modalidad en línea sobre estas prácticas para saber cómo accionar en caso nos enfrentáramos a algún ataque de ciberseguridad
54. Ignorar correos desconocidos
55. Encriptar información
56. Realizar copias de respaldo de la información, protección de correos electrónicos, uso de antivirus, controles de acceso a la información
57. Proteger correos electrónicos y proporcionar capacitaciones a empleados sobre ciberseguridad.
58. NA
59. Verificación continua de accesos abiertos a servidores y monitorización del tráfico de datos constante del servidor donde se guarda la información, si tiene mucho tráfico de datos, es porque algo está pasando.
60. Tener un buen equipo IT en el lugar de trabajo
61. Uso de programas con seguridad
62. Capacitación
63. Con frecuencia cambiar la contraseña
64. Capacitaciones
65. Capacitar
66. Verificación en 2 pasos
67. Cambiar contraseña regularmente
68. Capacitaciones
69. NA
70. Guardar en un servidor municipal

Empresa Privada.

¿Qué medidas de ciberseguridad crees que podrían implementar o mejorar en tu lugar de trabajo?

1. Mejor manejo de la información personal.
2. Implantación de procesos ISO27001
3. Redes privadas
4. Aislamiento de red interna de internet
5. Chequeos cada mes
6. Protección general
7. Mejorar servidores y métodos de seguridad
8. Utilizar claves seguras
9. Todas
10. Ninguna
11. Contratar servicios de seguridad integral y actualizaciones al día
12. Ninguna es bastante seguro
13. Realizar capacitaciones al personal
14. No se
15. No lo se
16. contraseñas seguras
17. Alta disponibilidad de los sistemas críticos en sitio remoto
18. N/A
19. No abrir correos sospechosos que no son de carácter institucional
20. Implementar las VPN, cambiar mensualmente las contraseñas, evitar tener altas sumas de dinero en cuentas bancarias (checking Account) ya que estas pueden sufrir robos de identidad.
21. El acceso a carpetas compartidas
22. Encriptación
23. NA
24. NA
25. Actualizaciones
26. Todas las medidas necesarias
27. Asesorar al personal
28. Tener todo con contraseñas
29. Quitar el teléfono a los empleados
30. Siempre estar a la expectativa del trabajo q desempeñe
31. Ser más discretos
32. Mejor seguridad en archivos
33. No se
34. Actualización de datos técnicos
35. Comunicaciones
36. Impartir más charlas sobre ciberseguridad
37. Cambiar contraseña de cuentas
38. Ninguna
39. No lo se
40. Ninguna
41. Mayor capacitación
42. No se
43. Intervención celular en llamadas y mensajes

44. Pagar mejor y empleo fijo
45. Información confidencial protegido ante un jaqueo
46. Cámaras
47. No lo se
48. Mantener más informado al personal sobre el tema
49. Cambiar la contraseña un poco más frecuente
50. Desconozco
51. Proteger cuentas
52. No tengo idea
53. Encriptar las contraseñas
54. Claves
55. No sé de ciber seguridad
56. no se
57. No lo se
58. Encriptación, no usar dispositivos
59. Tener precaución con los dispositivos a conectar
60. Claves
61. Red interna
62. Mejor equipo informático con personal capacitado
63. Adecuado uso de la información
64. Más seguridad en contraseñas
65. No sé de eso
66. No sé
67. Muchas
68. Estar protegido con contraseñas
69. No tengo conocimiento.
70. No se
71. Codificación de seguridad
72. Control de cámaras en caso de problemas
73. Notificación por cada acción sospechosa
74. N/C
75. Mejorar la seguridad
76. No proporcionar mucha información
77. Capacitar al equipo informático sobre el tema
78. No se
79. No tengo idea
80. Hacer un plan sobre ello