¿Están las personas conscientes de la importancia de resguardar sus datos personales en la era digital?

Elaborado por:

Fráncico Federico Murillo Villareal - Ingeniería de producción

Universidad Ean

Facultad de Ingeniería

Seminario de Investigación de Pregrado

Febrero, 2023

Bogotá, D.C.

Contenido

Resumen

El presente trabajo de investigación nace de la necesidad de conocer si hay relación entre la edad de las personas y su nivel de conocimiento sobre la posibilidad de ser víctima de suplantación de identidad con fines delictivos principalmente.

Se parte de la realidad que se presenta en la que hay un aumento de los fraudes cibernéticos, donde personas son suplantadas y sus datos financieros caen en manos de delincuentes con fines lucrativos.

La hipótesis es si hay una relación entre la edad y la seguridad de la información que se comparte en el ciber ecosistema, (Termino que se ampliara más adelante) en esta era digital, donde la tecnología supone que realizar transacciones, compra y venta de bienes y servicios es más fácil comparada con la forma del comercio de apenas hace algunos años.

El problema de la investigación es que necesariamente en esta era digital, es necesario compartir información financiera como; números de tarjetas de crédito, débito, pagos por medios electrónicos como Paypal, Nequi, Daviplata, para mencionar algunos de los más utilizados en Colombia.

Este escenario real y tangible que se vive hoy, con plataformas de comercio como Amazon, Ebay, Mercadolibre, por poner ejemplos de empresas con reglas y de comercio y estándares de seguridad que deben cumplir para poder ofrecer servicios de comercio electrónico por un lado y por el lado del sistema bancario está la validación de estas transacciones para asegurar que las transacciones son verificadas mediante estándares internacionales de seguridad de la información, que se fundamente en tres principios que

son. La integridad de la información, La disponibilidad de la información, y la confidencialidad de la información. En el desarrollo del presente trabajo se ampliarán estos conceptos y términos.

Pero desde la perspectiva de las personas como usted y como cualquier persona del común, que hacendó uso de este nuevo paradigma de comercio, donde la ventaja es que, sin salir de casa, puedo comparar precios, productos, calidad, si hay ofertas sobre algún bien o servicio que se necesita y hacer la mejor elección de compra.

Sin embargo, desde la perspectiva del usuario común, en contraparte es que se debe “ceder parte de la privacidad” al necesariamente entregar datos personales para que el sistema financiero pueda verificar la autenticidad de quien realiza la compra.

En este último punto, es donde converge el tema de esta investigación, que tanta información personal comparten la personas en redes sociales que le facilite a los ciber delincuentes hacer “ingeniería social”

Así mismo, que tan fácil seria a un ciber delincuente, que tiene los datos personales que le permitan eventualmente responder las preguntas de validación bancaria, descifrar las contraseñas de la persona que esta puede ser víctima de ataque

Problema de Investigación

En la actualidad, utilizan internet para realizar diversas actividades, desde compras en línea hasta transacciones bancarias, mediante dispositivos digitales fijos y móviles según (Suarez, 2020) lo que implica compartir información personal a través de medios electrónicos. Sin embargo, esta práctica también implica un mayor riesgo de ciberataques y suplantación de identidad. Es importante saber si las personas están conscientes de estos riesgos y si toman las medidas para resguardar su información personal.

Desde las empresas y organizaciones existen normas para las organizaciones como entidades bancarias y medios de pago, para asegurar que los datos desde las empresas están seguros y constantemente monitoreados como la norma ISO 27001 (ICONTEC, 2022) y norma PCI (Security Standards Council, 2023), que son estándares a nivel de empresa que se deben cumplir para poder operar como en este sector de la economía.

Las empresas, son objeto de ciberataques como el caso de EPM (Forbes, 2022), donde represento secuestro de la información afectando a millones de personas, son ejemplo que las empresas son conscientes que deben invertir en seguridad de la información y cerrar las brechas de seguridad.

Pero desde las personas ¿hay conciencia de que pueden ser suplantados? En este escenario, las medidas esblencadas en las normas que las empresas deben cumplir pueden ser vulneradas al suplantar la identidad (Díaz, 2019) de un usuario y realizar transacciones de forma fraudulenta.

Objetivos

Objetivo General

Analizar si están las personas conscientes de la importancia de resguardar sus datos personales en la era digital

Objetivos Específicos

Determinar mediante una encuesta el nivel de conocimiento de las personas sobre los riesgos al realizar transacciones electrónicas.

Identificar que tan seguras son las medidas que utilizan las personas encuestadas para proteger sus datos y su información financiera de ciberataques o suplantación de identidad.

Proponer una metodología de autoevaluación, para que una persona identifique su nivel de vulnerabilidad en el ciber-ecosistema y mitigue el riesgo al que está expuesto frente la suplantación y el robo de identidad.

Justificación

En este estudio se aborda los temas de privacidad, seguridad en línea y manejo de los datos personales. Se analizarán los datos recolectados para cuantificar el conocimiento de las personas sobre el autocuidado que se debe tener para aumentar la seguridad de sus datos personales.

Conocer qué tan vulnerables son las personas a ciberataques y suplantación mediante una encuesta, puede ofrecer información apropiada para toma de decisiones más acertadas para aumentar la seguridad de la información basada en el autocuidado como parte de la construcción de un ciber-ecosistema según (Bailón, 2021) seguro en esta era digital. (Forbes, 2022)

Saber cómo las personas pueden cerrar las brechas de seguridad, como lo describe (Dubout, 2020) donde presenta cifras sobre las brechas se seguridad de la información de las personas.

Es así como, en términos de convivencia, conocer el entorno digital y los posibles riesgos, esta investigación está alineada con el posible un posible aporte para tomar decisiones adecuadas frente a la exposición peligros existentes no solo a fraudes también a la exposición a la pérdida o violación de la privacidad de acuerdo con el trabajo de (Ornelas, 2020).

En términos de relevancia social, conocer las vulnerabilidades y tener una postura activa frente a las posibles amenazas de las personas al dejar expuestos sus datos personales o información sensible a personas inescrupulosas que se dedican a hacer ingeniería social como lo expone (Borghello C. , 2019), la ingeniera social en el arma infalible por la estrecha relación con la vanidad del ser humano

Desde la perspectiva de las implicaciones prácticas una de ellas es como se mencionaba anteriormente, aportar herramientas que pueda adoptan al lector para tener una actitud de autocuidado frente a resguardar sus datos personales su información sensible que le permita reducir ser objeto de ingeniera social y caer en algún tipo de

estada, como lo afirma (Borghello C. , 2019) la única computadora segura es una que este apagada.

Marco Teórico

Antecedentes

En los últimos años, se han publicado artículos sobre la seguridad de la información y el robo de identidad, como por ejemplo (Borghello & Temperini, 2012), expone que en esta era digital, la identidad se puede definir como un conjunto de datos y características que permiten individualizar a una persona, en este contexto la identidad digital presenta la mismas características, pero en el escenario del internet, y sobre esta base sustenta en datos, como en varios países el fraude y el robo de identidad crece en el tiempo.

Cómo han reaccionado los organismos de seguridad, en respuesta a estos delitos, según (Mendo, 2014), desde los cuerpos de seguridad se han creado unidades especiales que vienen combatiendo los delitos cometidos a través de las nuevas tecnologías. Además, cita la cooperación internacional como respuesta a los delitos cibernéticos.

En el trabajo de (Limon Vidal, 2016). A diferencia de los autores citados anteriormente, que abordan el tema de la suplantación de identidad como delito, y la respuesta de los organismos de seguridad, desde la perspectiva del derecho, aquí, a

autora nos introduce en algo más concreto y es el auge de la suplantación y el robo de identidad, mediante las redes sociales y metodologías como el phishing, que más adelante profundizaremos en estos conceptos.

Ahora, nuestra privacidad como derecho fundamental, según (Castro Jaramillo, 2016). En Colombia la corte constitucional mediante la sentencia T-414 de 1992 se pronuncia sobre el derecho a la intimidad donde enfatiza en el derecho a la intimidad y hace énfasis la corte constitucional en que todas las personas tienen derecho a su intimidad personal y familiar.

Mas adelante (Castro Jaramillo, 2016) expone que este concepto de intimidad ha sido transformado debido a la facilidad que tienen las redes sociales para divulgar y difundir la información que era considerada privada.

Desde las organizaciones que se dedican al nicho empresarial de acercar a los negocios con el cliente (Busines to Consmers) o B2C según (Usma Espinel, 2016), hacia donde ha migrado el comercio en esta era digital, la banca ha ganado mucho terreno, antes para abrir una cuenta de ahorros o cualquier tipo de producto financiero, se requería ir a una oficina del banco llevar papeles realizar trámites de manera presencial, ahora todo esto se hace mediante Call Ceneters o empresas de contact center donde acercan al cliente con el banco. Para estas empresas existe una regulación y una normatividad que deben cumplir para asegurar que la información de sensible de los usuarios este resguardada adecuadamente como por ejemplo ISO-27001 (ICONTEC, 2022) y PCI-DSS (Security Standards Council, 2023)

De los trabajos anteriores podemos inferir que, las redes sociales han impactado en la sociedad de forma que lo que antes era confidencial, ahora ya no lo es tanto, pero, cómo puede ser esto posible, el ciber-ecosistema actual se basa en la información digital, y la facilidad que ofrecen los medios digitales para acceder a potenciales clientes mediante redes sociales, ya el comercio puede ofrecer productos y servicios de forma más efectiva a potenciales clientes. Entre otras palabras también se puede difundir información de todo tipo a público de forma segmentada, de acuerdo con los patrones de búsqueda y los hábitos de interacción con las redes sociales de las personas.

Como lo expone (Isaak & Hanna, 2018), Facebook entregó información personal de más de 87 millones de usuarios a Cambridge Analytica que fue una empresa del Reino Unido, que en 2016, se vio envuelta en un escándalo por manipulación indebida de datos personales que fueron proporcionados por Facebook, con la que se manipuló la opinión pública, mediante segmentación de datos, Inteligencia artificial minería de datos psicometría, en la campaña presidencial de Donald Trump en 2016. Su fundador Alexander Nix, fue acusado por mal uso de datos personales.

Por otra parte (Rehman, 2019). Que durante la campaña de 2016 en EE. UU. Cambridge Analytica utilizaron una técnica de “Dark Post” que son mensajes personalizados en redes sociales negativos contra el candidato rival. según el autor esto es un ataque digital.

Este caso de Cambridge Analityca, con esta tecnología de vanguardia, y se evidenció que los datos personales en redes sociales pueden ser manipulados y comercializados en el más alto nivel.

Ahora, Colombia podemos encontrar trabajos como el realizado por (Rangel, 2020). La mayor parte de escritos y trabajos que se encuentran relacionados con ciberseguridad, ataques informáticos se enfocan en organizaciones gubernamentales, organizaciones privadas, empresas, para asegurar la información como activo valiosos para las organizaciones. Para esto se basan en normas internacionales como la ISO 27001. Pero hacia las personas, ¿cómo manejamos cada persona nuestra seguridad informática.

Marco conceptual

Se puede inferir que en estos momentos vivimos dentro de un ciber-ecosistema, que como en todo ecosistema hay varios agentes que interfieren e interactúan.

> Dentro del ciber ecosistema están las organizaciones, sean gubernamentales, sociales, o de comercio, que mediante los medios digitales ofrecen bienes y servicios a usuarios de esos bienes y servicios, hasta aquí podríamos pensar analógicamente en una simbiosis donde dos o más organismos interactúan para convivir y beneficiarse mutuamente, como lo expone (Rangel, 2020) entre los citados en este trabajo.

El punto corazón de esta investigación es, conocer que tan vulnerables somos las personas en este ciber ecosistema, a agentes patógenos para seguir en la misma línea analógica, donde los estos agentes patógenos que causan enfermedades en los ecosistemas, en el ciber ecosistema causan daño como ya se expuso antes, a las organizaciones y a los usuarios para fines desde ideológicos hasta delictivos.

Desde las organizaciones, como ya se expuso, hay una serie de políticas, legislación, normas y buenas prácticas que las organizaciones deben cumplir para segura que la información esta resguardada y segura para el funcionamiento adecuado de las empresas, aun así, las empresas son víctima de ciber ataques constantemente donde se pretende hacer daño al secuestrar información y parar la operación de las organizaciones.

Pero desde las personas, ¿Qué tan preparados estamos para estos ciber ataques? Si se piensa, para continuar con la analogía, en el ecosistema hay peligros con los que debemos convivir, estos peligros en el entorno no lo podemos eliminar, debemos tomar acciones para mitigar el riesgo a esos peligros como; Enfermedades, accedentes, catástrofes para nombrar algunas.

Para centrar más estos conceptos analicemos que es riesgo y que es peligro, estos son términos que a menudo se confunden, pero son diferentes en su esencia.

Riesgo según (Rodríguez, 2011). es la posibilidad de que ocurra un evento o una situación peligrosa y la magnitud del daño potencial que puede causar ese evento.

El peligro o impacto según (Rodríguez, 2011), se refiere a la posibilidad de daño o lesión, entre varios factores el que más nos introduce en esta una condición insegura.

Entonces, podemos decir que el peligro se refiere a la condición o situación que puede causar daño, mientras que el riesgo, es la evaluación de la probabilidad y la magnitud del daño potencial que puede resultar de ese ese peligro. Es así como hay que evaluar tanto los riesgos como los peligros para tomar decisiones y medidas adecuadas de seguridad.

La mitigación del riesgo se refiere e las medidas y acciones tomadas para reducir o minimizar los efectos potenciales del riesgo, partiendo la base que el riesgo no se puede eliminar del todo

Ejemplos:

Peligro de un accidente cerebro vascular: o la obstrucción de una arteria coronaria que puede causar daño al corazón y en casos graves la muerte.

1. El riesgo del accidente cerebro vascular varía entre las personas, depende de varios factores como, la edad, el género, la genética el estilo de vida y las condiciones de salud.
2. La mitigación del riesgo de un accidente cerebro vascular es; identificar los factores de riesgo y contrólalos, como hacer ejercicios, alimentación balanceada, dejar de fumar, controles médicos rutinarios, si el medico lo considera, medicamentos para controlar esta condición.

Peligro de ser víctima de un atraco, es perder el dinero o artículos de valor, en el atraco se pueden recibir lesiones graves o incluso la muerte.

1. El riesgo puede variar del sector, la hora en la que se transite las condiciones que llamen la atención de los delincuentes, como exponer objetos valiosos, dinero, resistirse al atraco.
2. La mitigación del riesgo es, identificar el sector, evitar llevar grandes cantidades de dinero u objetos valiosos, evitar andar solo en la calle, transportase en vehículo o vehículos de confianza cuando se llevan objetos de valor.

Ahora ya en el entorno de ciber ecosistema algunos de los riesgos que debemos tener en cuenta son.

Suplantación de identidad, (Cristian Borghello, 2012) es una técnica comúnmente utilizada en ciberataques para obtener información confidencial o acceso a sistemas de redes, mediante el engaño de los usuarios al hacerse pasar por otra persona o entidad entre los que se encuentran

Phishing: (Ahmed Aleroud, 2017). técnica que consiste en enviar correos electrónicos o mensajes de texto, que parecen legítimos, pero en realidad son fraudulentos y buscan obtener información confidencial como información bancaria, datos de tarjetas de crédito.

Spear phishing: (Ahmed Aleroud, 2017). es una variante del phishing que se dirige a individuos específicos o grupos de individuos que utilizar información detallada para parecer ms convincente, por ejemplo, utilizar la información obtenida en redes sociales para enviar mensajes de correo electrónico a un empleado de una empresa haciéndose paras por un miembro directivo de la organización y extraer información o ingresar a la red de la organización.

Pharming: (Lauren, 2011) es un ataque que dirige a los usuarios a un sitio web fraudulento, aunque hayan ingresado correctamente a la dirección o sitio web en su navegador, es te tipo de ataque se lleva a cabo modificando las DNS o a través de programa maligno.

DNS (Domain Name System) (Lauren, 2011). que asocia el nombre de dominio a direcciones IP,

IP (Internet Protocol) (Lauren, 2011). es un numero único que se le asigna a cada dispositivo conectado a internet.

Las DNS como las IP, son fundamentales para el funcionamiento del internet y las redes informáticas y la comunicación entre usuarios y servidores.

Programa maligno: es un término que en general se refiere a cualquier software malicioso diseñado para dañar, interferir, robar información o tomar el control de un sistema informático sin el conocimiento o consentimiento del usuario: en este grupo se encuentran:

1. Virus: (Castro, 2018) programa maligno que se propaga a través de sistemas informáticos mediante la inserción de copias de sí mismo en programas o archivos legítimos causando daño en sistemas de archivos o redes informáticas y/o afectar la continuidad del negocio
2. Gusanos: (Castro, 2018) es un programa maligno que se propaga automáticamente a través de sistemas informáticos sin necesidad de la intervención de un usuario, estos pueden ralentizar una red, explotando las vulnerabilidades de seguridad del sistema operativo, mediante aplicaciones mediante los puertos abiertos de la red.
3. Troyanos: (Castro, 2018) tipo de programa maligno que se oculta en programas aparentemente legítimos para engañar al usuario y hacerle creer que es seguro descargar e instalar, una vez instalado los atacantes acceden de manera remota para robar información
4. Ransomware: (Castro, 2018)es un programa maligno que se utiliza para extorsionar a los usuarios infectados ya que estos ataques cifran los

archivos de la víctima y exigen un rescate por la recuperación de la información. Estos se propagan mediante el phishing principalmente o sitios web maliciosos. Estos pueden cifrar, bloquear o filtrar la información.

5. Spyware: (Castro, 2018) este programa maligno se utiliza para recopilar información personal y confidencial sin el consentimiento del usuario. Este puede ser instalado de manera oculta para monitorear las actividades como la navegación en internet y recopilar datos como inicio de sesión, grabar las pulsaciones de las teclas que se utilizan, esta información es enviada a los atacantes y ser utilizada con fines delictivos
6. Adware: Este programa maligno se utiliza para mostrar anuncios no deseados en el sistema del usuario. Este tipo de programa maligno no busca robar información o dañar el sistema el objetivo es generar ingresos mediante publicidad no deseada.
7. Rootkis: este tipo de programa maligno proporciona a los atacantes acceso no autorizado y control total del sistema operativo de una computadora. El objetivo es ocultar su presencia y evitar la detección su detección del antivirus. Estos pueden ser instalados mediante phishing o explotando las vulnerabilidades del sistema.
8. Explotar vulnerabilidades: se refiere a aprovechar las debilidades del sistema operativo para obtener acceso no autorizado. Estas vulnerabilidades son atacadas mediante programa maligno principalmente.

Sistema operativo: es el software que administra los recursos y las actividades de un ordenador, teléfono inteligente Tablet, es el programa más importante ya que responde a la gestión de los recursos del sistema como el procesador, memoria, dispositivos de entrada y de salida de datos con los que interactúa el usuario con el entorno informático.

En este sentido, el sistema operativo es la puerta de entrada al ciber ecosistema mediante un dispositivo como computador, Tablet, teléfono inteligente que esté conectado a internet. De allí que todo el programa maligno intenta alterar el funcionamiento del sistema operativo explotando las vulnerabilidades para robar información, suplantar identidad y robar información.

Entre los sistemas operativos más populares están:

1. Windows: es el sistema operativo más utilizado en todo el mundo, en ordenadores de escritorio, portátiles y tabletas, es desarrollados por Microsoft y cuenta con una amplia gama de usuarios y aplicaciones compatibles.
2. macOS: es el sistema operativo de ordenadores Mac de Apple, es conocido por su diseño elegante y su integración con dispositivos de Apple.
3. Android: es el sistema operativo móvil de Google, es utilizado en una amplia variedad de dispositivos, desde teléfonos económicos hasta smartphones de alta gama, cuanta con gran cantidad de aplicaciones
4. iOS: es al sistema operativo móvil de Apple utilizado en los iPhone e iPad.

5. Linux: es un sistema operativo de código abierto utilizado en la mayoría de los servidores web del mundo, es conocido por su estabilidad y seguridad.

Métodos de control del programa maligno:

1. Antivirus: (Castro, 2018). es un software diseñado para detectar, eliminar o bloquear programa maligno en sus diferentes modalidades.
2. VPN (Virtual Private Network) (Ferguson, 1998). o red privada virtual, esta tecnología permite una conexión cifrada entre dos o más dispositivos, creando un túnel cifrado a través de la red pública para proteger la privacidad y la seguridad de las comunicaciones.
3. Firewalls: (Castro, 2018). o cortafuegos es un software o hardware que se utiliza para proteger una red de computadoras contra intrusiones no autorizadas, funciona como una barrera entre el internet y el dispositivo o dispositivos conectados. Se pueden utilizar en redes domesticas o empresariales.

Todo lo anterior a grandes rasgos es el ciber ecosistema y sus los riesgos a ser suplantado, robo de información bancaria, estafa, secuestro de información, extorsión, perjuicios al buen nombre y la privacidad.

La correcta identificación de estos riesgos y su evaluación nos puede llevar a tener un ciber ecosistema seguro, al identificar los fatores de riesgo frente a los peligros y mitigarlos.

En este contexto con los conceptos más claros se debe evaluar los siguientes factores de riesgo:

- Sistema operativo utilizado: ¿es legal? Sí está debidamente licenciado que cuente con las actualizaciones de seguridad periódicas del proveedor, la probabilidad que sea atacado por algún tipo de programa maligno se reduce.
- Antivirus: ¿cuenta con antivirus legal? Los sistemas operativos como Windows 7 en adelante, cuentan con antivirus incorporado y firewalls, los cuales son más efectivos sí el sistema operativo es legal y esta actualizado periódicamente
- ¿Cuenta con un sistema de VPN (Ferguson, 1998),instalado en su red domestica o su dispositivo?
- ¿Abre correos sospechosos, de fuentes desconocidas donde le ofrecen premios, o algún otro incentivo sin cuestionar la procedencia? Esta es la manera que los ciber delincuentes propagan el phishing,
- Desde su smartphone ¿abre enlaces de mensajes de texto donde le informan sobre ofertas de empleo, reclamar premios, cancelación de su cuenta de ahorros, bloqueo de su tarjeta de crédito? Este es otro tipo de propagación de programa maligno o de phishing.
- ¿entrega información personal o financiera a personas que llaman de su entidad financiera sin verificar antes?
- ¿Qué tanta información personal comparte en sus redes sociales?
- ¿Qué tan seguras son las claves de acceso?

- ¿Utiliza la misma clave para varios dispositivos o aplicaciones?
- ¿Sus claves contienen fechas de nacimiento o números de identificación?
- ¿Permite que el navegador guarde automáticamente sus contraseñas?
- ¿Sus contraseñas son alfanuméricas?
- ¿Sus contraseñas tienen algún patrón fácil de deducir para alguien que conoce información personal suya?

En resumen: se encuentra mucha información sobre ciberseguridad y protección de los datos enfocado a las empresas y las organizaciones, sin embargo, de cara hacia las personas comunes, a las personas que todos los días expuestas a ser víctimas de suplantación o vulneración de la intimidad.

Por citar algunos casos, (El Informador.mx, 2023), donde se hacen ofertas laborales directamente a personas, mediante mensajes de texto, WhatsApp, Telegram como herramienta para robar información

Otra modalidad, es recibir mensajes de texto o correos electrónicos, de la entidad bancaria u otra como Amazon donde supuestamente le informan al usuario que su cuanta está bloqueada y le ofrecen un enlace para “desbloquear” su cuanta o sus productos retenidos, pero es una modalidad de fraude según (Owalda, 2021)

Es así, que grupos de ciber delincuentes se dedican a perfilar personas mediante ingeniería social, (Grande, 2015). que consiste en manipular personas, mediante engaños para revelar información financiera entre muchas otras, hacerse pasar por una entidad legitima, para obtener acceso a información bancaria, cuentas de ahorro tarjetas de crédito, medios de pago y obtener ganancias mediante estos medios de suplantación.

Entonces. Las organizaciones tienen la obligación de cumplir con normas internacionales para asegurar tres cosas según (ICONTEC, 2022):

1. La integridad de la información de los usuarios.
2. La disponibilidad de la información de los usuarios
3. La confiabilidad de la información de los usuarios.

Desde aquí, las entidades se aseguran de resguardar la información financiera y los recursos de los usuarios, y cualquier falla de seguridad desde las entidades o empresas de comercio tienen un alto nivel de control de riesgo.

Pero, desde los usuarios, ¿cómo aseguran que sus datos no sean robados?, si se considera que, en este escenario, las personas son suplantadas, que es el objetivo final de los ciber delincuentes, todas las medidas de seguridad de las entidades son atravesadas.

Este es el objetivo de la investigación. Que tan conscientes son las personas del autocuidado frente a los ciber ataques o suplantación de identidad.

Diseño metodológico

Enfoque de la investigación

Esta investigación tiene un enfoque mixto por la naturaleza de la recolección de datos, donde tenemos unos conceptos cualitativos, como los niveles de encriptación de las contraseñas que utilizan los encuestados, que tanta información sensible exponen las personas luego se le asignan valores numéricos a las variables de la investigación, las que vamos a recolectar mediante una encuesta, para posteriormente modelar los datos estadísticamente.

En el presente trabajo nos basaremos en un enfoque mixto, ya que tomaremos unas variables categóricas y se les asigna unos valores numéricos que están clasificadas las categorías.

Se asignan valores para poder segmentar de forma numérica cada nivel de valor asignado a cada respuesta de la encuesta que se realiza, para cuantificar el nivel de riesgo que aceptan las personas en cuanto a ciberseguridad y determinar el conocimiento de las personas encuestadas sobre auto cuidado en sobre seguridad.

Diseño de la investigación

Este diseño se lleva a cabo de forma experimental, mediante un sondeo o prueba de conocimiento de las personas sobre los conceptos de ciberseguridad, mediante una

encuesta donde se hacen preguntas sobre características del tipo de contraseñas que utilizan, qué tanta información personal comparte en las redes sociales los encuestados, de forma longitudinal ya que se hacen las mismas preguntas en varios momentos durante la colección de datos.

Con lo anterior se busca describir que tan vulnerables son las personas encuestadas en el conjunto de datos a ser víctimas de suplantación de identidad, fraude o estafa mediante un ciber ataque.

También entender si hay alguna correlación entre la edad y la vulnerabilidad a ser víctimas de algún tipo de suplantación o robo mediante ingeniería social.

Variables

Las variables con las que se medirá el objetivo principal de la investigación se dividen en tres grupos:

1. Exposición a suplantación, Calidad de las contraseñas utilizadas teniendo como referencias el trabajo de (Montero, 2013)
2. Exposición a ser víctima de phishing, que tan probable es que de clic en un enlace de un correo o mensaje de texto.
3. Exposición a robo de información. Que tanta información personal comparte en internet.

4. Exposición a secuestro de información, están actualizados los sistemas operativos, antivirus, firewalls o VPN.
5. Rangos de edad de los entrevistados

Estas variables se evalúan mediante una matriz de riesgo (Rodríguez, 2011). de acuerdo con la segmentación o los datos que se obtengan de la encuesta, para cuantificar el nivel de consciencia de las personas encuestadas sobre ciber seguridad de acuerdo con los objetivos del trabajo de investigación.

Tabla 1 Matriz de riesgo propuesta para la evaluación Elaboración propia

Variables/Riesgo	Alta	Media	Baja
encriptación de claves	Perdida de información Financiera	Posible robo de información personal	Perdida de información publica
Nivel de información compartida en redes sociales	Exposición de información personal	Riesgo de suplantación de identidad	Posible Spam
Compras o transacciones en línea	Robo de información de medios de pago	Riesgo de suplantación de identidad	Falla de entrega de productos
Apertura de links mediante mensajes de texto o e-mails	Virus y programa maligno, que afecte sus equipos de cómputo y/o robo de información	posible estafa o Phishing	Spam o publicidad no deseada

Fuente elaboración propia mediante Excel

En la tabla 1, se relacionan las variables propuestas con las preguntas realizadas en la encuesta, luego se le asignarán valores numéricos de acuerdo los datos recolectados para determinar si hay variabilidad ente los rangos de edad propuestos como variable dentro de la encuesta. El sexo y el nivel de interacción con el comercio en línea de los encuestados.

Donde se puede cuantificar según (Rodríguez, 2011) mediante:

$$Riesgo = Viabilidad * impacto\ o\ peligro$$

Tabla 2 puntuación de la matriz según el peligro

Puntuación	Viabilidad
1	baja
2	media
3	alta

fuente (Rodríguez, 2011)

En la tabla 2. Se propone según (Rodríguez, 2011) un método de e valoración o de cuantificación de los resultados de las variables que se recopilan en la encuesta en una forma de matriz de riesgo de acuerdo con la tabla1.

Muestra

La población objetivo son personas que tengan acceso a contestar una encuesta por medios electrónicos, con el fin que validar que las personas encuestadas tienen acceso a medios digitales y redes sociales, que es el medio en el que difunde esta encuesta.

La investigación se realiza mediante una muestra no probabilística de 30 personas mediante bola de nieve, difundiendo la encuesta mediante correo electrónico, grupos de WhatsApp, Facebook, a amigos y familiares para alcanzar el tamaño mínimo de la muestra.

Métodos Para la Recolección de los datos

El instrumento para la recolección de los datos a la población objetivo será mediante una encuesta, la cual se difunde entra amigos, familiares y medios de la universidad EAN, la cual pueden responder de forma libre sin recolectar información sensible con el propósito único de desarrollar la pregunta de la investigación

Enlace de la encuesta

https://forms.microsoft.com/Pages/ResponsePage.aspx?id=WbVvwGgbhEuhT0fQ2Delq1G-t4HDww9Iqx3I6JuLDbBUQ0I5WjZNS01ITVMzMlZSOEtSNUpMTUhaMy4u

La encuesta tiene un diseño propio mediante la herramienta forms de Microsoft y se difunde el enlace de la encuesta para la recolección de datos de a las personas que tengan en enlace.

Los datos se almacenan automáticamente a medica que las personas encuestadas responden la encuesta.

Análisis De Los Datos

La encuesta se realizó a 72 personas, que contestaron la encuesta de forma libre y espontanea mediante la difusión de la encuesta, compartiendo el enlace mediante grupos de WhatsApp, Facebook.

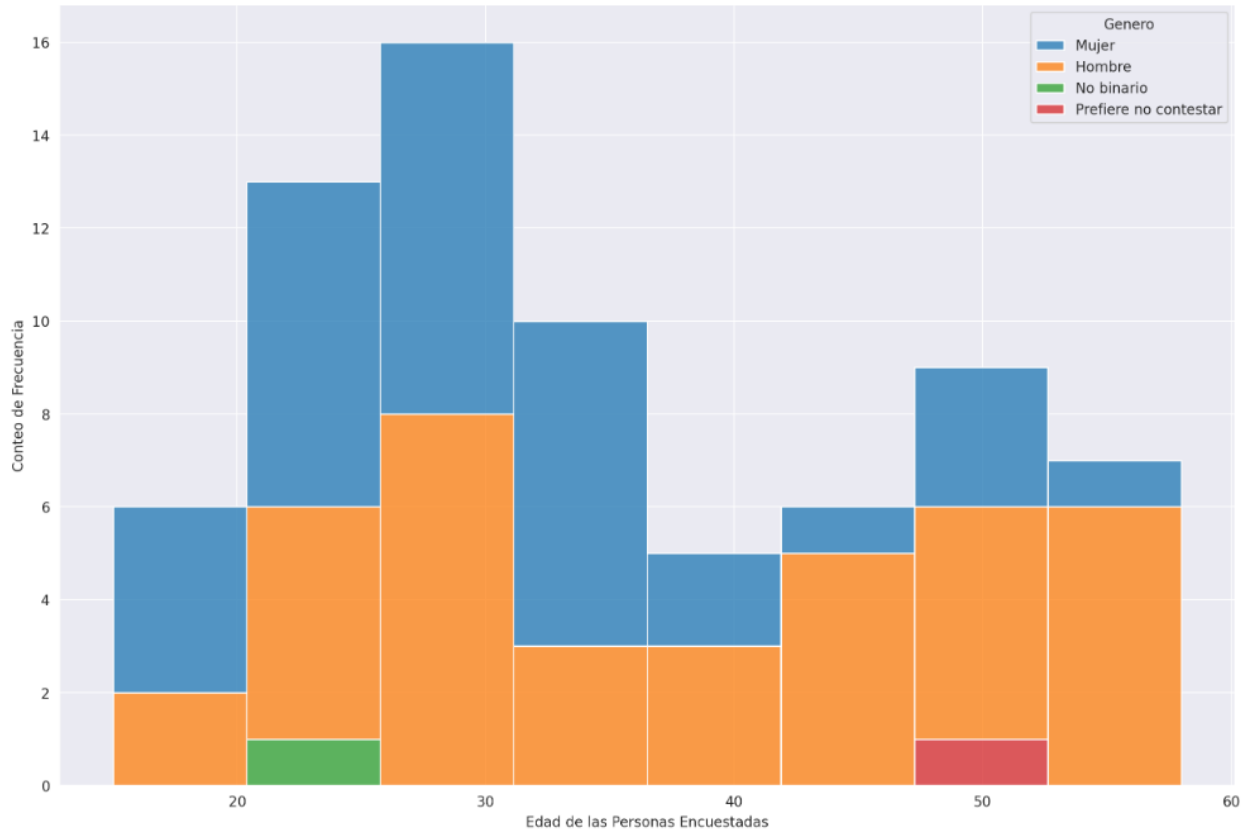
Para el análisis de los datos se utilizaron herramientas como Excel donde se registran los datos iniciales.

Para el procesamiento de los datos, se utiliza Python (Python , 2023) y librerías para análisis de datos como Pandas versión 2.01, (Pandas ORG, 2023) y para en análisis estadístico de los datos se utiliza Seaborn v0.12.2 (seaborn pydata org, 2023) estas herramientas de análisis se utilizan en la plataforma de GoogleColab (Google, 2023)

Para el análisis estadístico se aplica la regla empírica (Triola, 2004) capítulo 2 pagina 83, regla empírica para datos con distribución normal

Exploración y visualización de los datos recolectados en la encuesta

Figura 1 Análisis de Frecuencia Edad y Genero Personas Encuestadas



Elaboración propia mediante Python

En la figura 1, encontramos una descripción demográfica de las personas que contestaron la encuesta de donde se extraen los datos de las variables. Donde se aprecia que la muestra está distribuida de forma equivalente entre hombres y mujeres

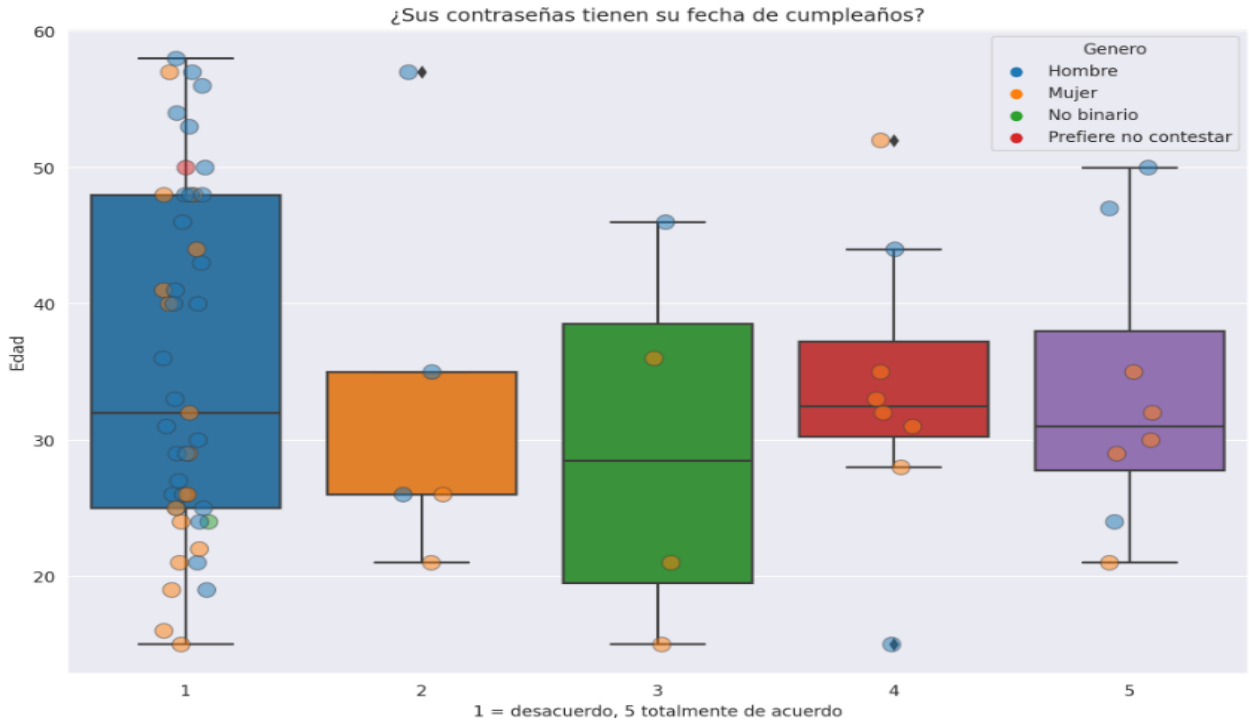
Desarrollo de las preguntas

Todas las preguntas, se modelan, en el eje de las abscisas se encuentra la valoración de la pregunta entre 1 y 5. Donde 1 es en desacuerdo y 5 totalmente de acuerdo.

En el eje de las ordenadas esta la edad, y en puntos de colores se encuentra la distribución del género en cada pregunta.

Esta distribución apunta a determinar su hay diferencias en la muestra de personas que respondió la encuesta.

Figura 2 Análisis estadístico Pregunta 1



Elaboración propia mediante Python,

En la figura 2 se relacionan las respuestas de las personas encuestadas con los siguientes datos estadísticos:

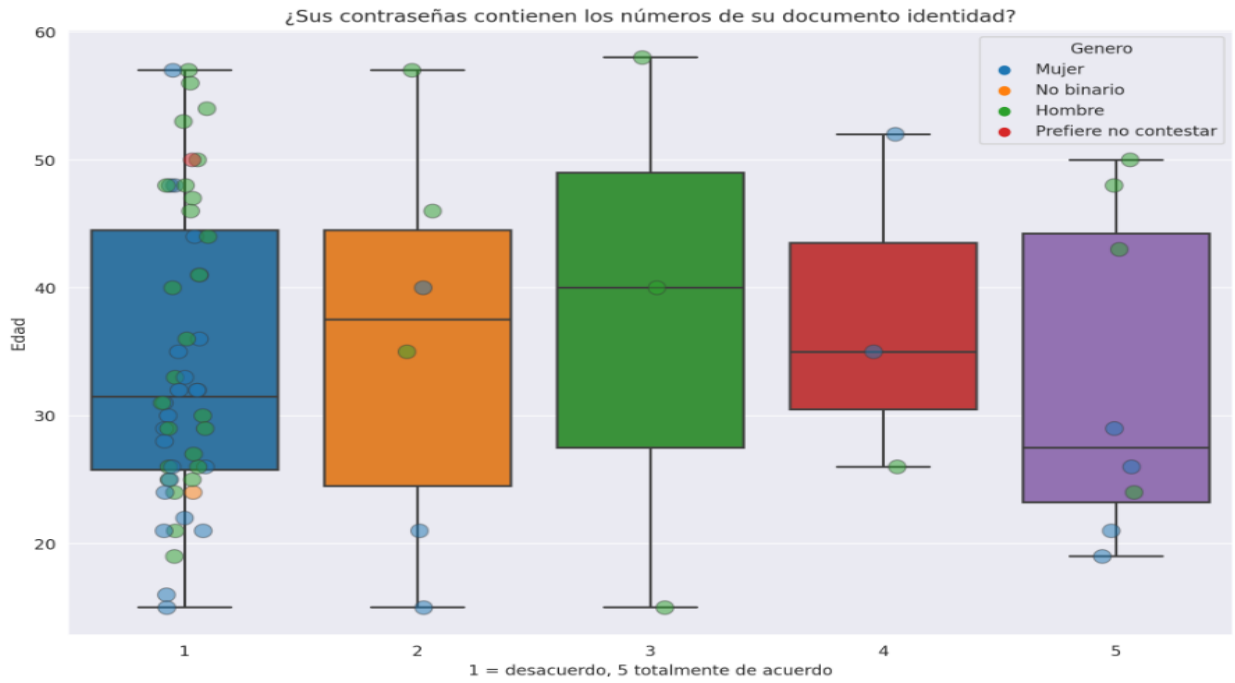
Tabla 3 Resumen estadístico de las respuestas a la pregunta 1

¿Sus contraseñas tienen su fecha de cumpleaños?	
Media	1,95833333
Error típico	0,1740585
Mediana	1
Moda	1
Desviación estándar	1,47693535
Varianza de la muestra	2,18133803
Rango	4
Mínimo	1
Máximo	5
Cuenta	72

Fuente: elaboración propia mediante Excel

De acuerdo con los datos estadísticos de la pregunta 1, las personas encestadas tienden a no utilizar la su fecha de nacimiento en las contraseñas.

Figura 3Análisis estadístico pregunta 2



Elaboración propia mediante Python,

En la figura 3 se relacionan las respuestas de las personas encuestadas con los siguientes datos estadísticos:

Tabla 4 Análisis estadístico pregunta 2

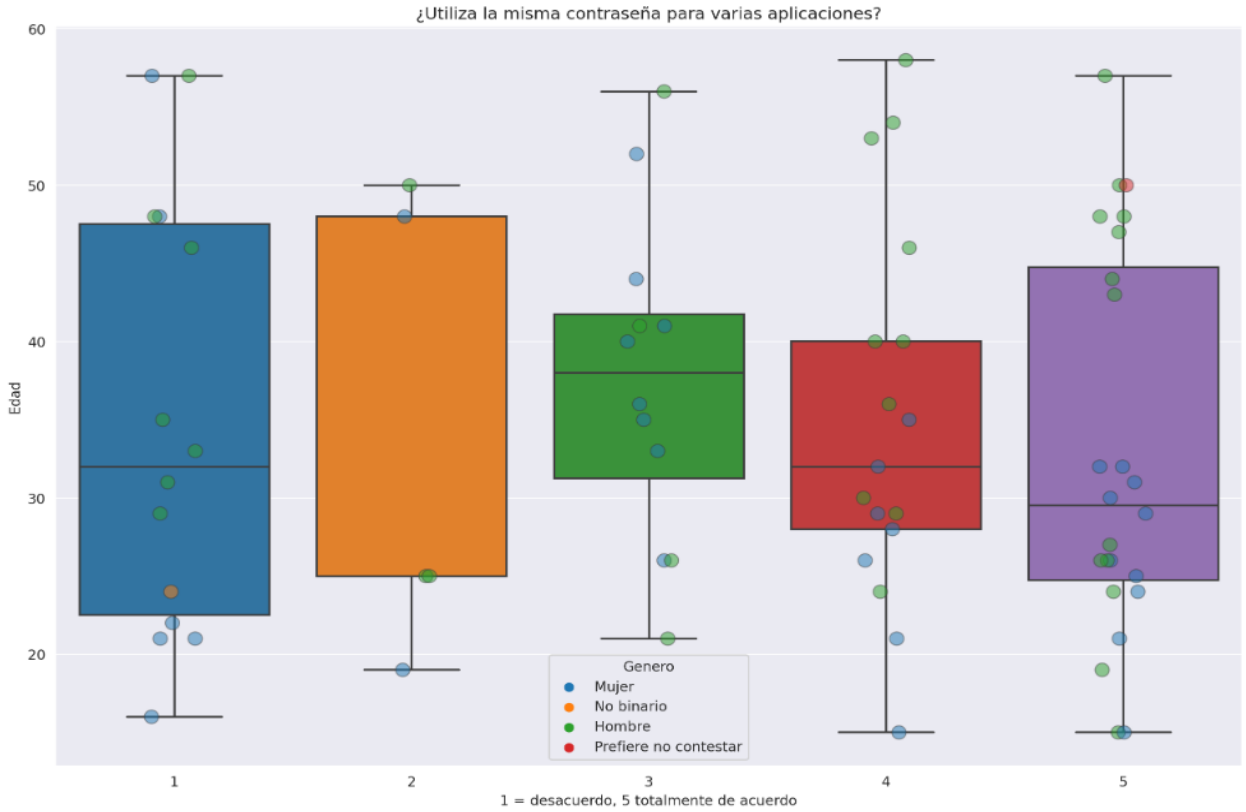
¿Sus contraseñas contienen los números de su documento identidad?	
Media	1,73611111
Error típico	0,16189538
Mediana	1
Moda	1
Desviación estándar	1,37372789
Varianza de la muestra	1,88712833

Rango	4
Mínimo	1
Máximo	5
Cuenta	72

Fuente: elaboración propia mediante Excel

De acuerdo con los datos estadísticos de la pegunta 2, las personas encestadas tienden a no utilizar los números del documento de identidad en sus contraseñas.

Figura 4 Análisis estadístico pregunta 3



Elaboración propia mediante Python,

En la figura 4 se relacionan las respuestas de las personas encuestadas con los siguientes datos estadísticos:

En la figura 4 se relacionan las respuestas de las personas encuestadas con los siguientes datos estadísticos:

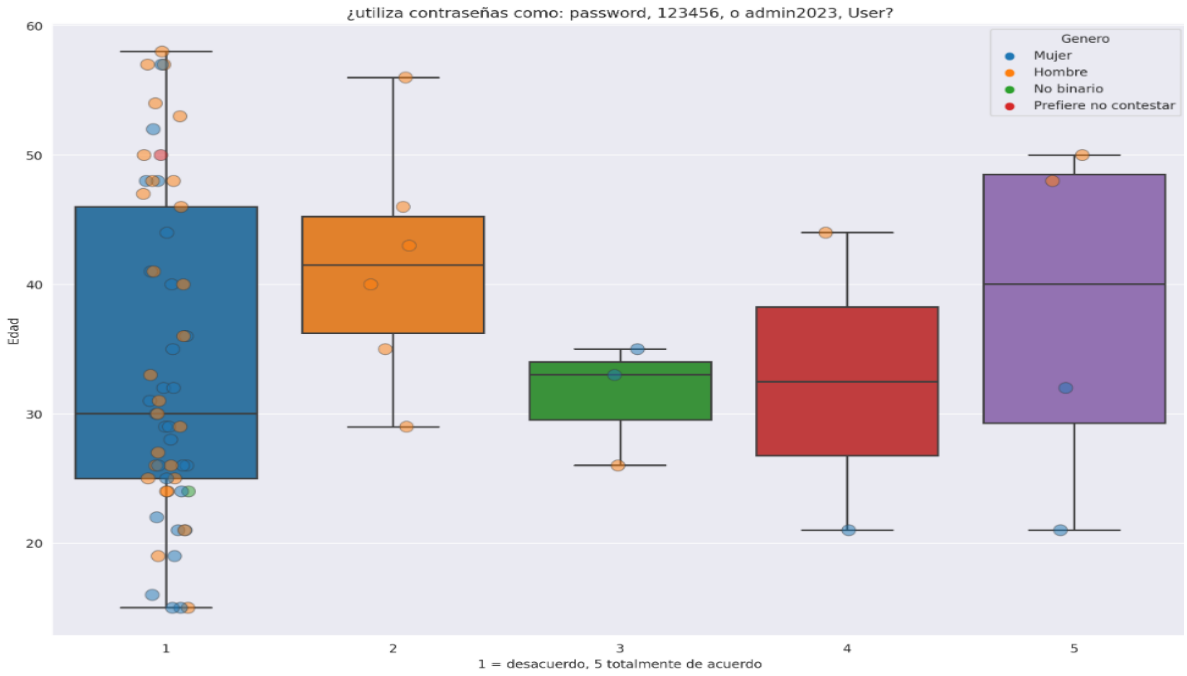
Tabla 5 Análisis estadístico Pegunta 3

¿Utiliza la misma contraseña para varias aplicaciones?	
Media	3,44444444
Error típico	0,17679206
Mediana	4
Moda	5
Desviación estándar	1,50013041
Varianza de la muestra	2,25039124
Rango	4
Mínimo	1
Máximo	5
Cuenta	72

Fuente: elaboración propia mediante Excel

De acuerdo con los datos estadísticos de la pegunta 3, las personas encestadas tienden a utilizar la misma contraseña para varis aplicaciones, esto ya sería una brecha de seguridad ya que, al capturar una contraseña, sea débil o fuerte que se utilice para varias aplicaciones se puede acceder a mucha información personal o financiera.

Figura 5 Análisis Pregunta 4



Elaboración propia mediante Python,

En la figura 5 se relacionan las respuestas de las personas encuestadas se aprecia una concentración de los datos en la opción 1, en desacuerdo, con los siguientes datos estadísticos:

Tabla 6 Análisis estadístico Pregunta 4

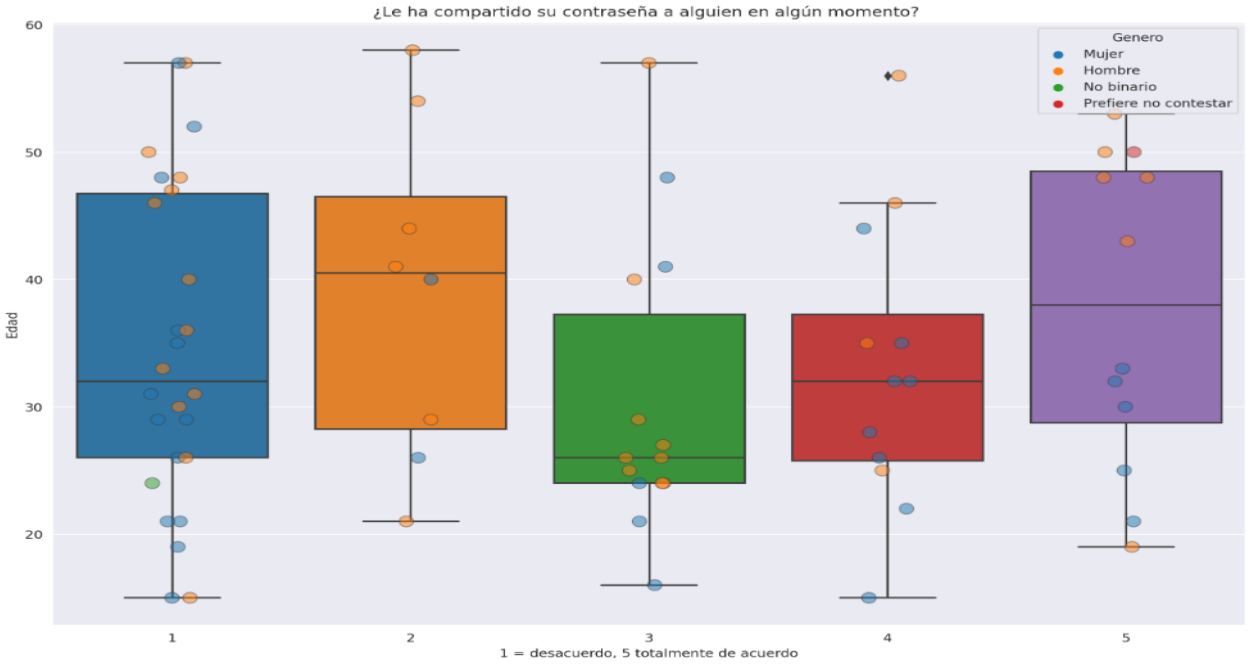
¿utiliza contraseñas como: password, 123456, o admin2023, ¿User?	
Media	1,47222222
Error típico	0,12814467
Mediana	1
Moda	1
Desviación estándar	1,08734361
Varianza de la muestra	1,18231612
Rango	4
Mínimo	1
Máximo	5
Cuenta	72

Fuente: elaboración propia mediante Excel

De acuerdo con los datos estadísticos de la pegunta 4, las personas encestadas tienden a no utilizar contraseñas genéricas o que son más comunes de hallar por los ciber delincuentes ya que en un ataque de fuerza bruta, estas contraseñas son las que primero utilizan

Figura 6

Análisis Pregunta 5



Elaboración propia mediante Python,

En la figura 6 se relacionan las respuestas de las personas encuestadas se aprecia una distribución más o menos uniforme en todo el rango de respuestas, con los siguientes datos estadísticos:

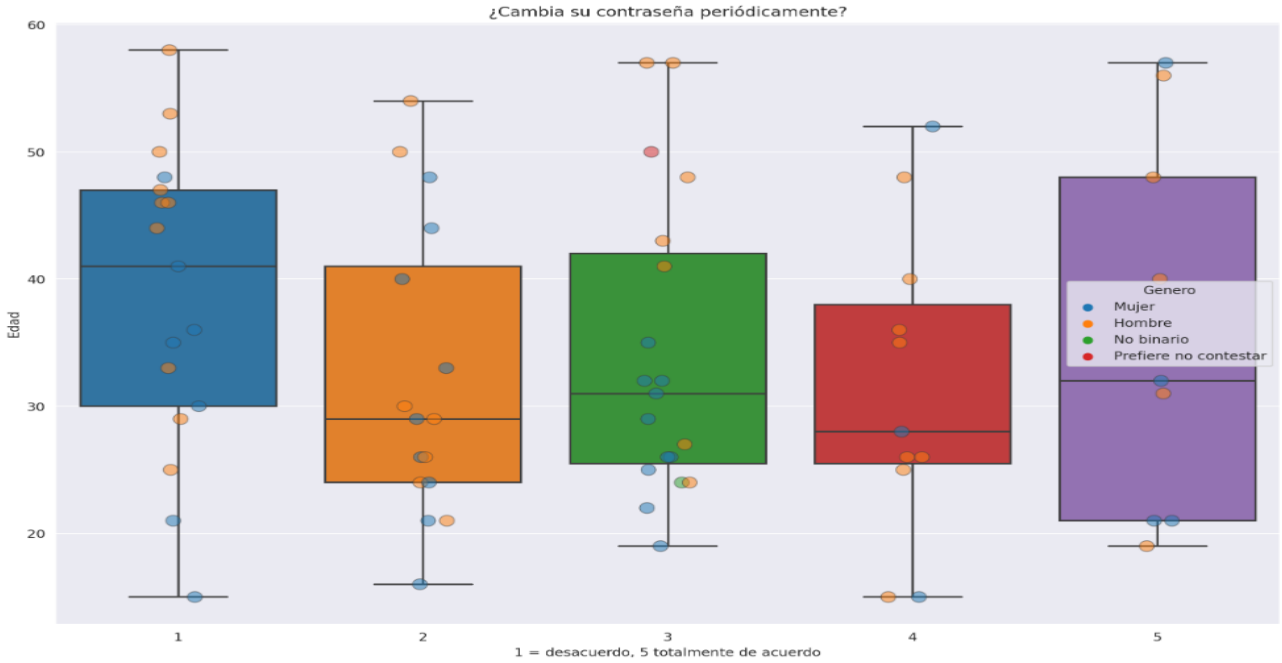
Tabla 7 Análisis Pregunta 5

¿Le ha compartido su contraseña a alguien en algún momento?	
Media	2,66666667
Error típico	0,17911275
Mediana	3
Moda	1
Desviación estándar	1,51982208
Varianza de la muestra	2,30985915
Rango	4
Mínimo	1
Máximo	5
Cuenta	72

Fuente: elaboración propia mediante Excel

Por la distribución de las respuestas, no hay un patrón o tendencia definidos, la distribución de las respuestas al estar en todo el rango de elección nos da una media de 2.6. y la desviación estándar 1.51, nos indica que el 68% de los encuestados comparte o ha compartido sus contraseñas en algún momento, esto también es una brecha de seguridad ya que puede quedar expuesta a ser copiada

Figura 7 Análisis Pregunta 6



Elaboración propia mediante Python,

En la figura 6 se relacionan las respuestas de las personas encuestadas se aprecia una distribución más o menos uniforme en todo el rango de respuestas, con los siguientes datos estadísticos:

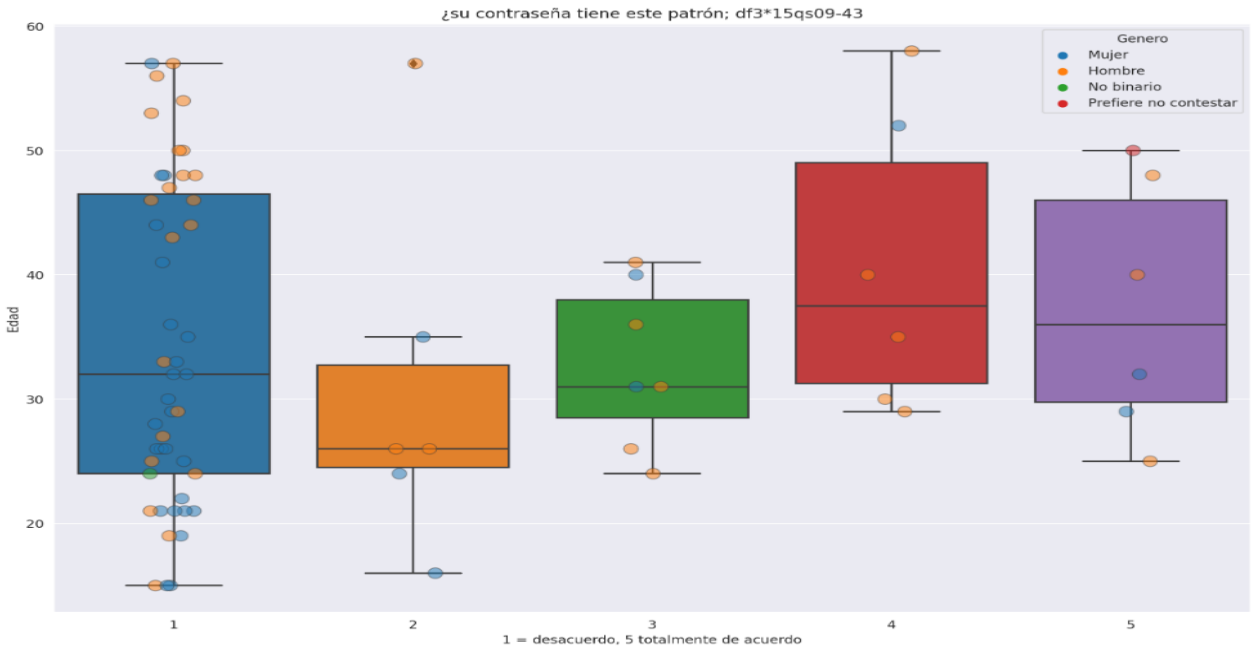
Tabla 8 análisis estadístico Pregunta 6

	¿Cambia su contraseña periódicamente?
Media	2,70833333
Error típico	0,15629401
Mediana	3
Moda	3
Desviación estándar	1,32619863
Varianza de la muestra	1,75880282
Rango	4
Mínimo	1
Máximo	5
Cuenta	72

Fuente: elaboración propia mediante Excel

Por la distribución de las respuestas, no hay un patrón o tendencia definidos, la distribución de las respuestas al estar en todo el rango de elección nos da una media de 2.7. y la desviación estándar 1.70, nos indica que el 68% cambia sus contraseñas si se les obliga de alguna manera a cambiar sus contraseñas, esto se podría interpretar como que los que el 23% de las personas que están en la opción 1, no cambian las contraseñas y apenas el 12.5% de las personas que están en la opción 5, cambian sus contraseñas.

Figura 8 Análisis Pregunta 7



Elaboración propia mediante Python,

Se aprecia una tendencia marcada de las personas encuestadas por la opción 1, aquí en esta pregunta, es una de las más importantes ya que se les pone un modelo de encriptación de una contraseña, lo que se define como una contraseña segura o muy difícil de vulnerar.

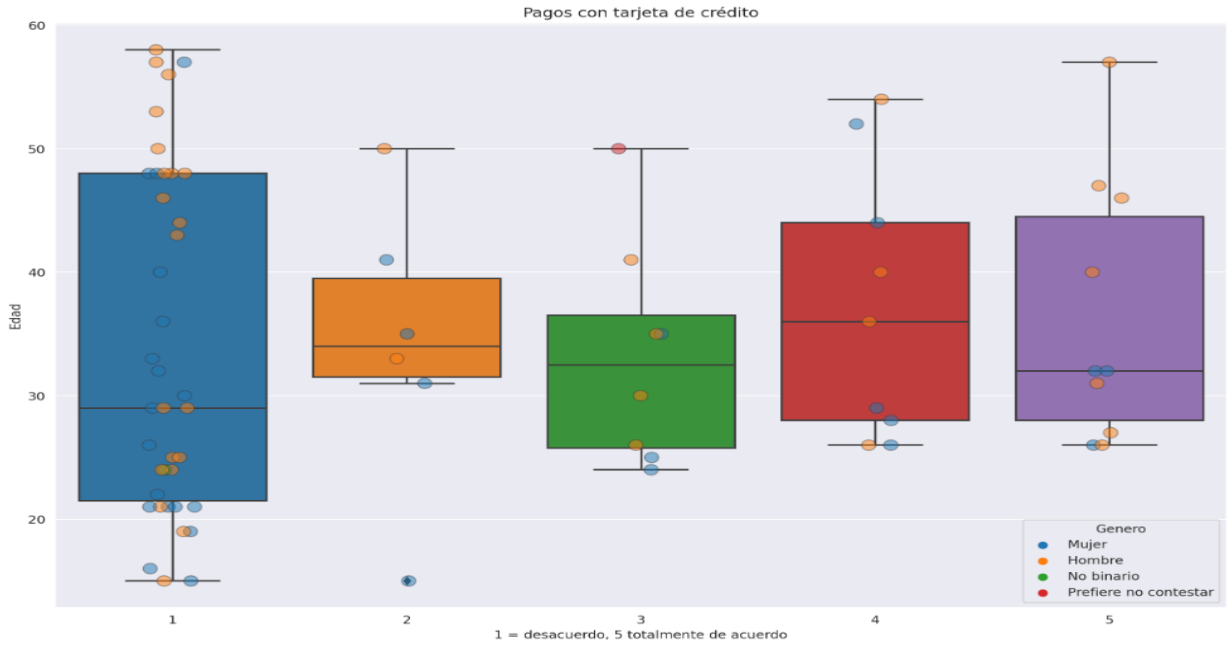
Tabla 9 Análisis pregunta 7

*¿su contraseña tiene este patrón; df3*15qs09-43*	
Media	1,86111111
Error típico	0,15984337
Mediana	1
Moda	1
Desviación estándar	1,35631601
Varianza de la muestra	1,83959311
Rango	4
Mínimo	1
Máximo	5
Cuenta	72

Fuente: elaboración propia mediante Excel

Por la distribución de las respuestas, hay un patrón o tendencia definidos, la distribución de las respuestas al estar mayormente en la opción 1 “totalmente en desacuerdo” nos indica que las personas no reconocen una contraseña segura, o no la contemplan porque es difícil de escribir o de recordar

Figura 9 Análisis Pregunta 8



Elaboración propia mediante Python,

De acuerdo con la distribución de las respuestas, hay una tendencia marcada a no realizar pagos con tarjeta de crédito en las personas encuestadas, solo el 13.9% de las personas encuestadas realizan pagos con tarjeta de crédito.

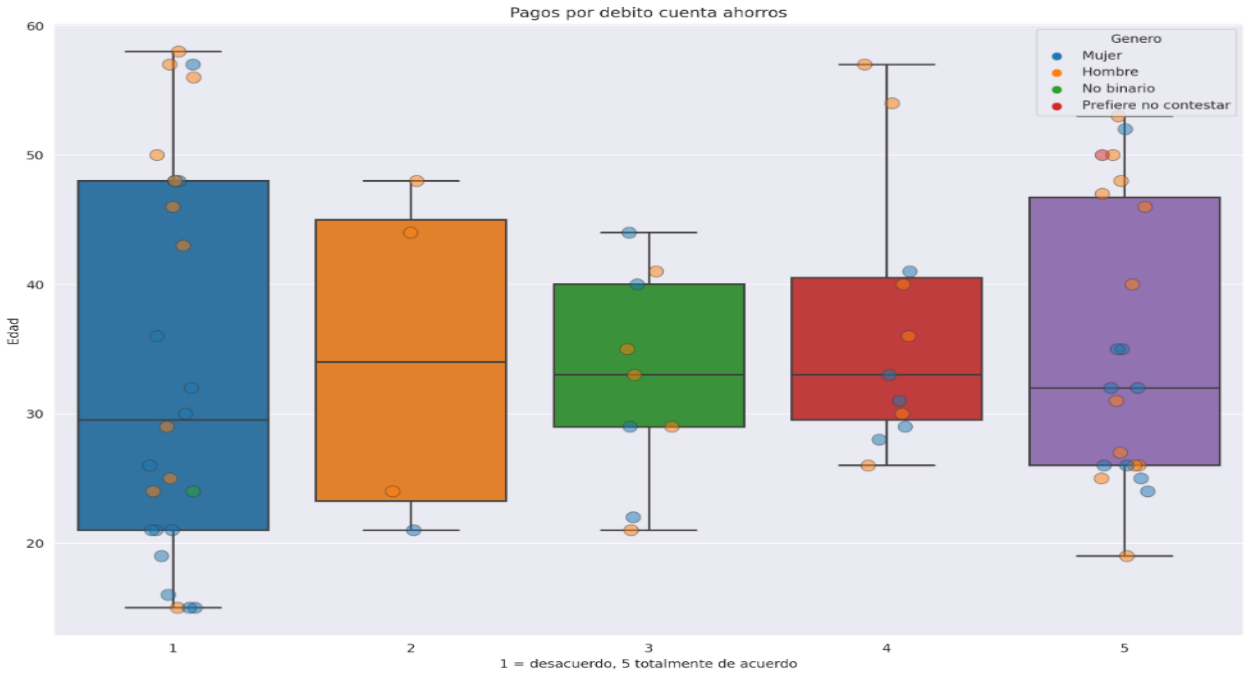
Tabla 10 análisis estadístico pregunta 8

Pagos con tarjeta de crédito	
Media	2,23611111
Error típico	0,18181516
Mediana	1
Moda	1
Desviación estándar	1,54275276
Varianza de la muestra	2,38008607
Rango	4
Mínimo	1
Máximo	5
Cuenta	72

Fuente: elaboración propia mediante Excel

Hay una tendencia marcada de los encuestados a no utilizar la tarjeta de crédito, lo que puede obedecer a que los encuestados no poseen una de estas tarjetas o no es su medio de pago preferido.

Figura 10 análisis pregunta 9



Elaboración propia mediante Python,

En la figura 9 se puede apreciar que la tendencia es más marcada a realizar pagos mediante la tarjeta de débito por medios electrónicos. La concentración de las respuestas se encuentra en las opciones 4 y 5,

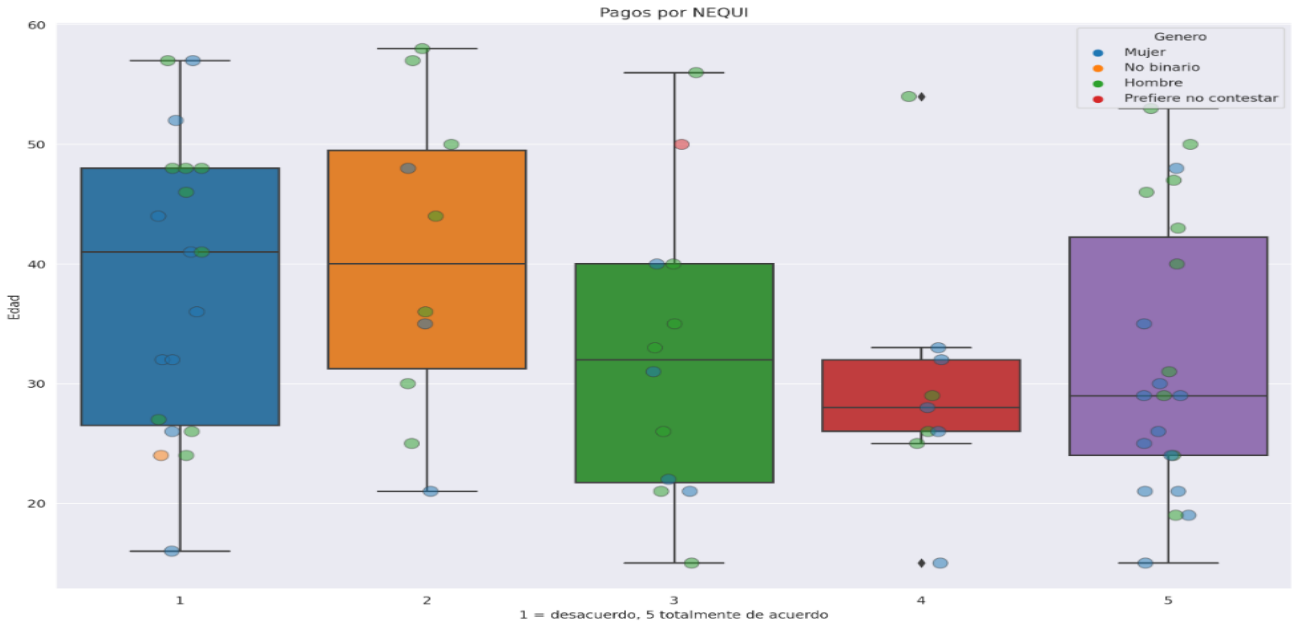
Tabla 11 análisis estadístico Pregunta 9

Pagos por debito cuenta ahorros	
Media	2,98611111
Error típico	0,20122187
Mediana	3
Moda	1
Desviación estándar	1,70742418
Varianza de la muestra	2,91529734
Rango	4
Mínimo	1
Máximo	5
Cuenta	72

Fuente: elaboración propia mediante Excel

De acuerdo con los datos estadísticos de la tabla 11, la tendencia cambia respecto a la tabla 10, aquí la tendencia cambia a las opciones 4 y 5 mayormente

Figura 12 Análisis pregunta 11



Elaboración propia mediante Python,

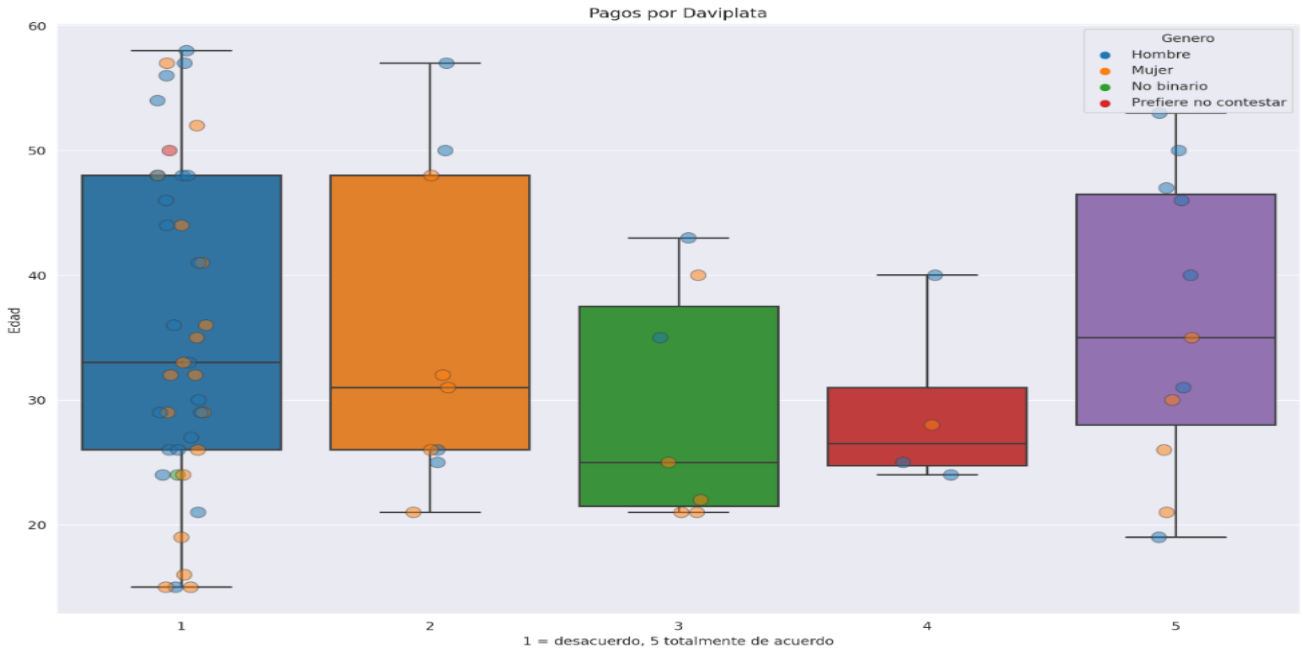
En la figura 12, sobre la pregunta si los encuestado utilizan pagos mediante NEQUI, no hay un patrón o tendencia definidos, la distribución de los datos está en todo el espectro de las opciones de respuesta.

Tabla 11 análisis Pregunta 11

Pagos por NEQUI	
Media	3,06944444
Error típico	0,18902433
Mediana	3
Moda	5
Desviación estándar	1,60392467
Varianza de la muestra	2,57257433
Rango	4
Mínimo	1
Máximo	5
Cuenta	72

Fuente: elaboración propia mediante Excel

Figura13 Análisis Pregunta 12



Elaboración propia mediante Python

En la figura 13, se aprecia una tendencia marcada a no estar de acuerdo no la pregunta, si comparamos con la figura 12, las personas encuestadas tienden a utilizar más Nequi que Daviplata y comparado con la figura 9 Nequi está levemente por encima de los pagos con tarjeta de crédito.

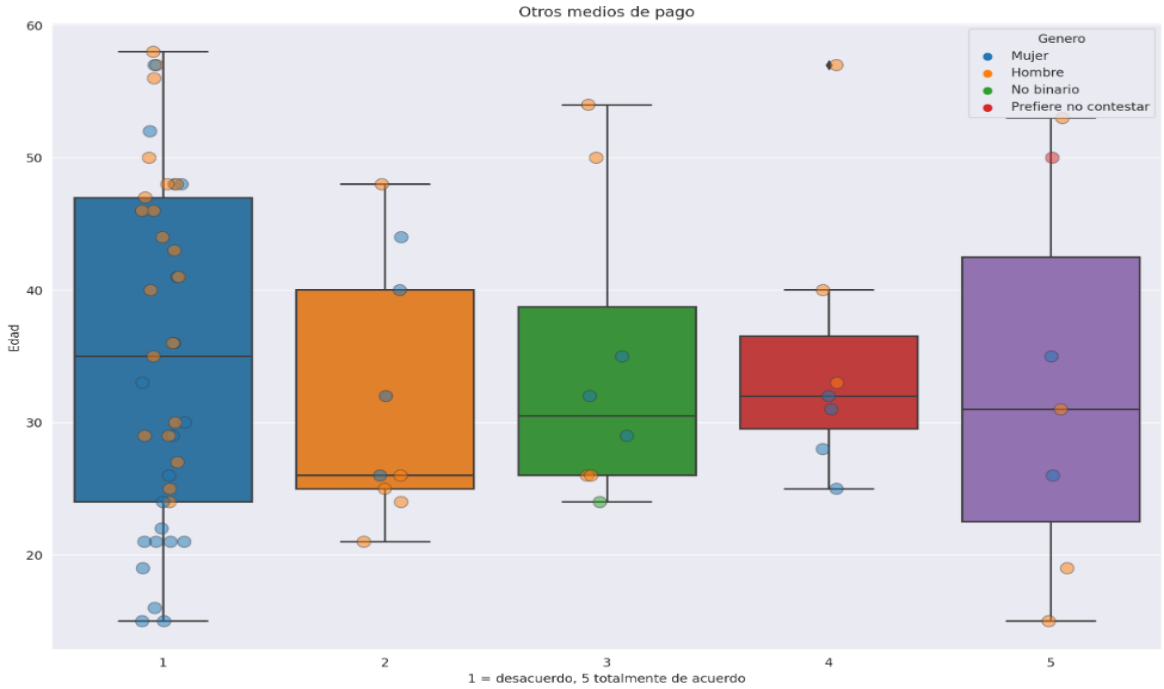
Tabla 12 Análisis estadístico Pregunta 12

Pagos por DAVIPLATA	
Media	2,09722222
Error típico	0,17819268
Mediana	1
Moda	1
Desviación estándar	1,512015
Varianza de la muestra	2,28618936
Rango	4
Mínimo	1
Máximo	5
Cuenta	72

Fuente: elaboración propia mediante Excel

De acuerdo con los datos de la tabla 12, se aprecia que la preferencia de las personas encuestadas es mayor a realizar pagos con Nequi y tarjeta de débito que con Daviplata.

Figura 14 análisis Pregunta 13



Elaboración propia mediante Python,

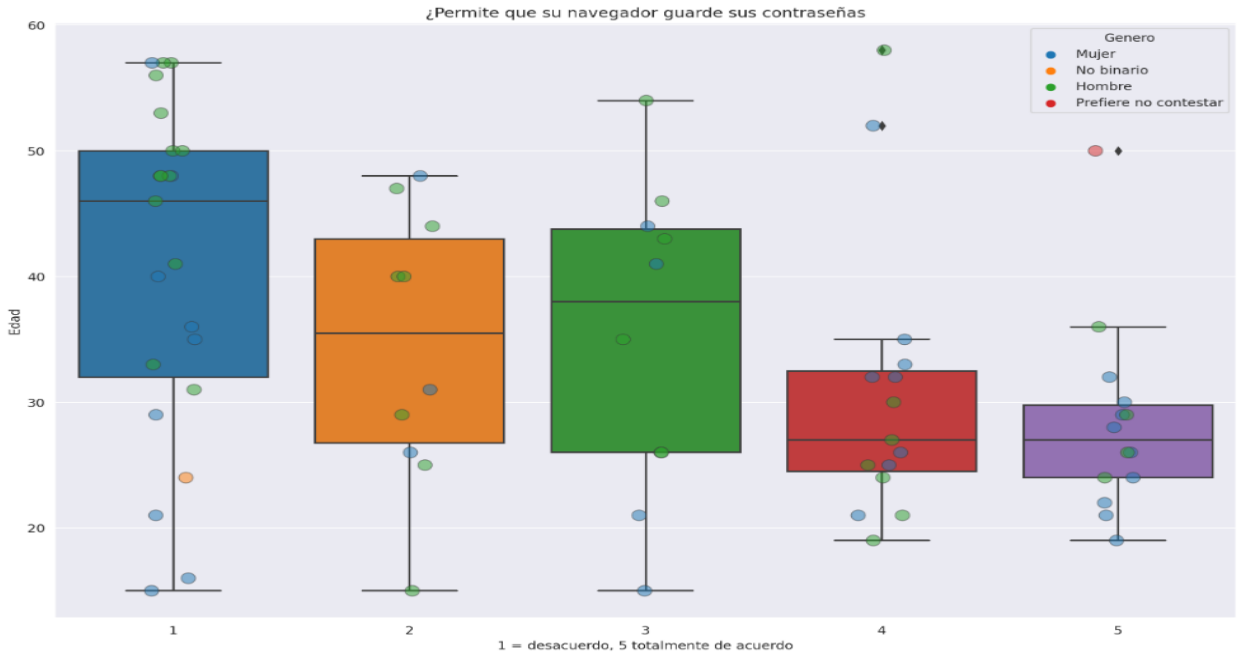
Tabla 13 Análisis Estítico Pregunta 13

Otros	
Media	2,02777778
Error típico	0,16545596
Mediana	1
Moda	1
Desviación estándar	1,40394035
Varianza de la muestra	1,97104851
Rango	4
Mínimo	1
Máximo	5
Cuenta	72

Fuente: elaboración propia mediante Excel

De acuerdo con la tabla 13, las personas encuestadas prefieren realizar los pagos con medios como Nequi y tarjeta de débito, con los datos de las tablas 10 y 11

Figura 15 Análisis Pregunta 14



Elaboración propia mediante Python,

En la figura 15 podemos apreciar que los encuestados, están distribuidos en todo el rango de respuestas, lo cual nos indica que no hay una tendencia o una correlación entre entra variables como la calificación de una pregunta en función de la edad o el género.

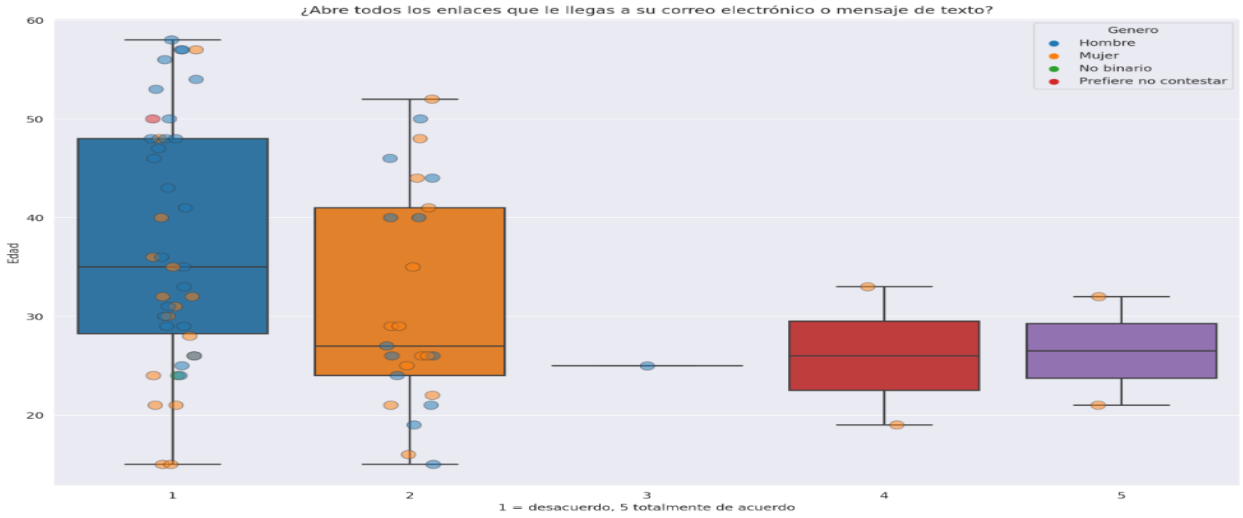
Tabla 14 Análisis estadístico Pregunta 14

¿Permite que su navegador guarde sus contraseñas?	
Media	2,819444444
Error típico	0,182709554
Mediana	3
Moda	1
Desviación estándar	1,550341979
Varianza de la muestra	2,40356025
Coeficiente de asimetría	0,100538937
Rango	4
Mínimo	1
Máximo	5
Cuenta	72

Fuente: elaboración propia mediante Excel

Ahora bien, los datos estadísticos en la tabla 14, podríamos inferir que aproximadamente el 68% de los encuestados es decir una desviación estándar hacia arriba y una desviación estándar hacia debajo de la media, podrían permitir que el navegador guarde sus contraseñas, lo cual es una brecha de seguridad sí son atacados mediante un programa maligno o phishing.

Figura 16 Análisis Pregunta 14



Elaboración propia mediante Python,

En la figura 16. Se describe la pregunta 14 de la encuesta, esta pregunta tiene relación directamente con el phishing, ya que, por enlaces de ofertas, promociones ganancias atractivas o correos o mensajes de texto como "*su cuenta ha sido bloqueada, ingrese al siguiente enlace para desbloquearla*" o mensajes como "*Su tarjeta registra un pago de XX$ ingrese al siguiente enlace para revertir la compra*"

Tabla 15 Análisis estadístico Pregunta 14

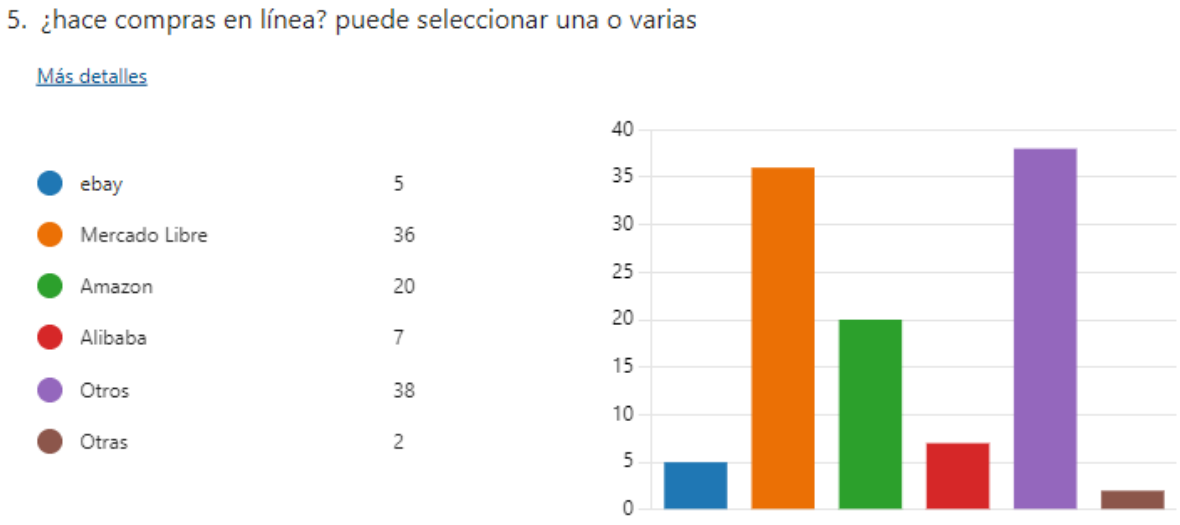
¿Abre todos los enlaces que le llegas a su correo electrónico o mensaje de texto?	
Media	1,569444444
Error típico	0,10433932
Mediana	1
Moda	1
Desviación estándar	0,885348485
Varianza de la muestra	0,783841941
Coeficiente de asimetría	2,225969037
Rango	4
Mínimo	1
Máximo	5
Cuenta	72

Fuente: elaboración propia mediante Excel

De acuerdo con los datos estadísticos, hay una probabilidad muy baja de que respondan o den clic a enlaces sin analizar la procedencia de los supuestos enlaces

Compras en línea

Figura 17 Histograma de preferencias para compras en línea de los encuestado

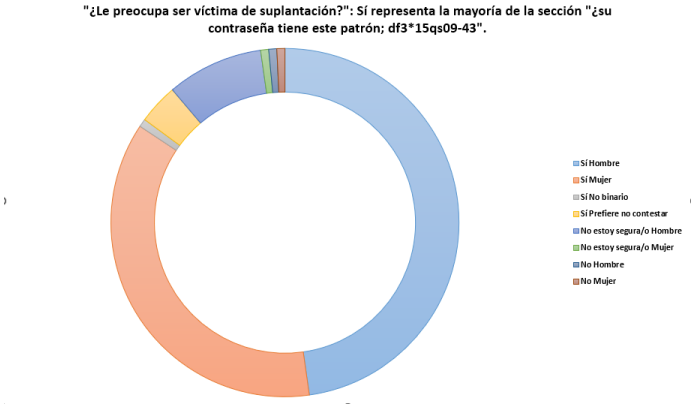


Elaboración propia mediante Excel

En la figura 17, podemos ver las preferencias de los encuestados para realizar las compras en línea, lo que valida que las personas encuestadas, realizan transacciones en línea que necesariamente realizan pagos por medios electrónicos de cualquier tipo.

Correlación de los datos más relevantes

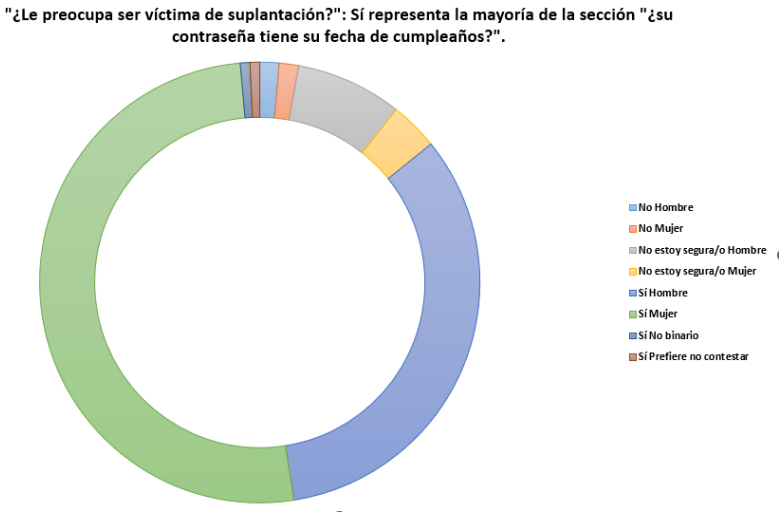
Figura 18 Correlación entre la pregunta si le preocupa ser víctima de suplantación y la pregunta 7



Elaboración propia mediante Excel

En la figura 18, tenemos una correlación y podemos evidenciar que por un lado hay una preocupación de las personas encuestadas ser víctimas de suplantación, pero manejan una contraseña débil.

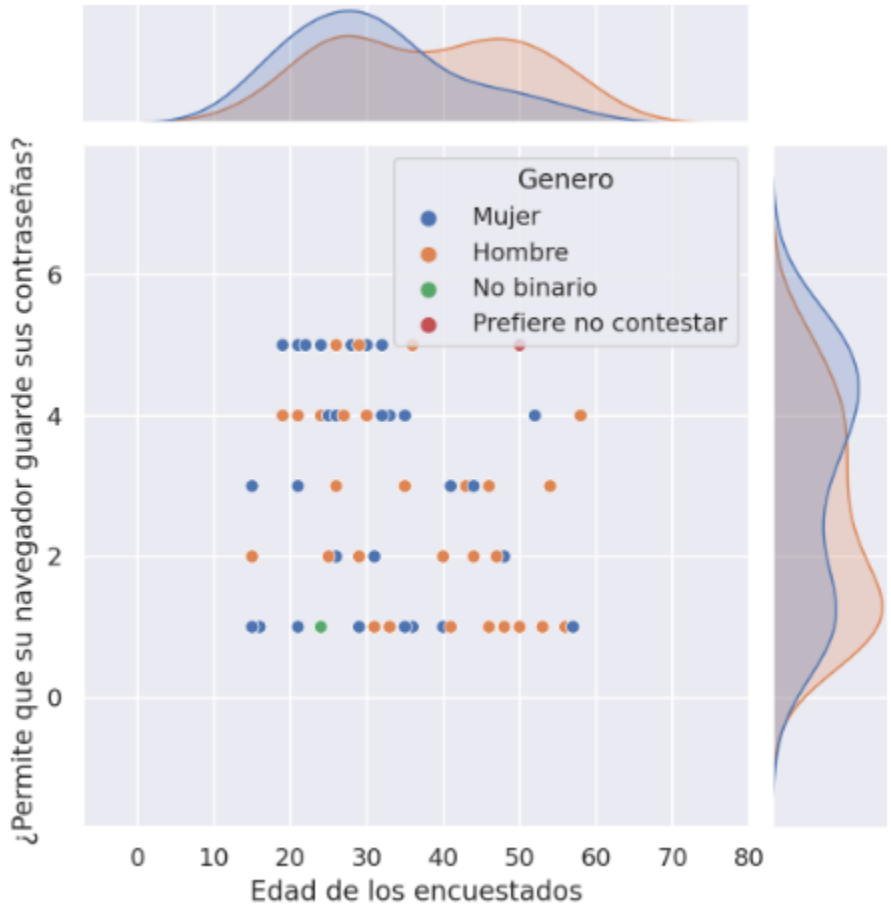
Figura 19 Correlación entre la pregunta le preocupa ser víctima de suplantación y la pregunta 1



Elaboración propia mediante Excel

De acuerdo con los daos de la figura 19, a las personas les preocupa ser víctimas de suplantación, pero tienen una brecha de seguridad en el cifrado de las contraseñas

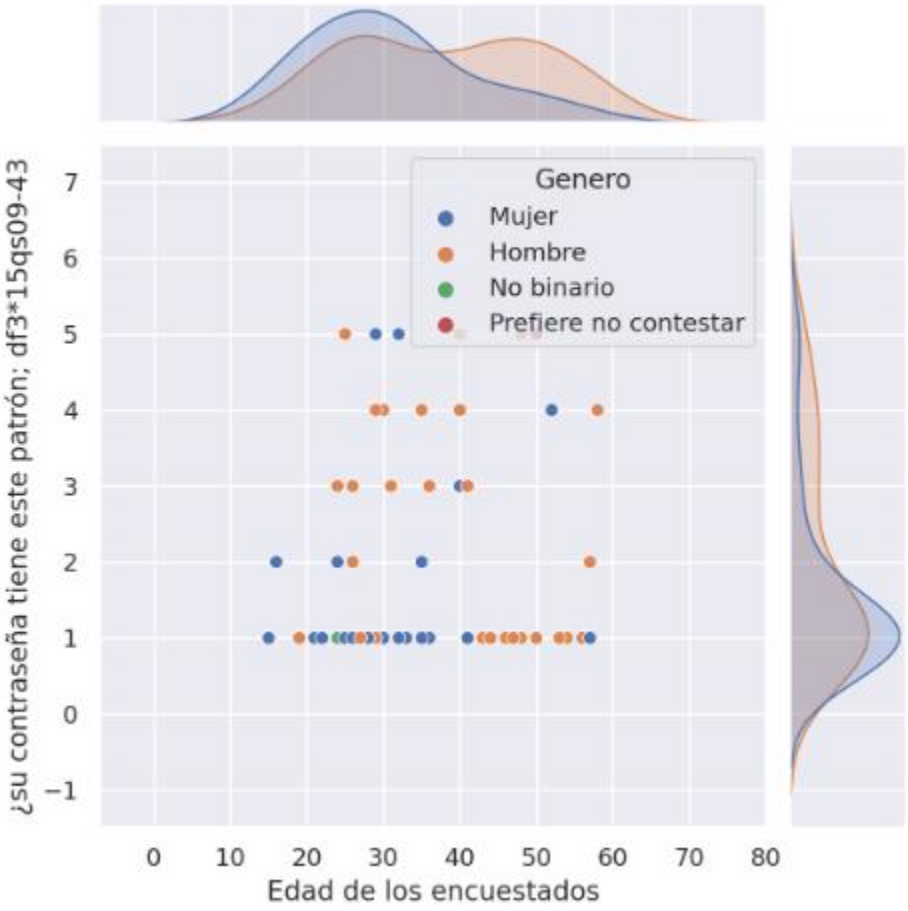
Figura 20 Correlación entre una contraseña débil y la edad de los encuestados



Elaboración propia mediante Python,

En la figura 20. Se gráfica la calificación de una contraseña débil, con la edad de los encuestados, con el objetivo de si hay una correlación lineal entre estas dos varíales.

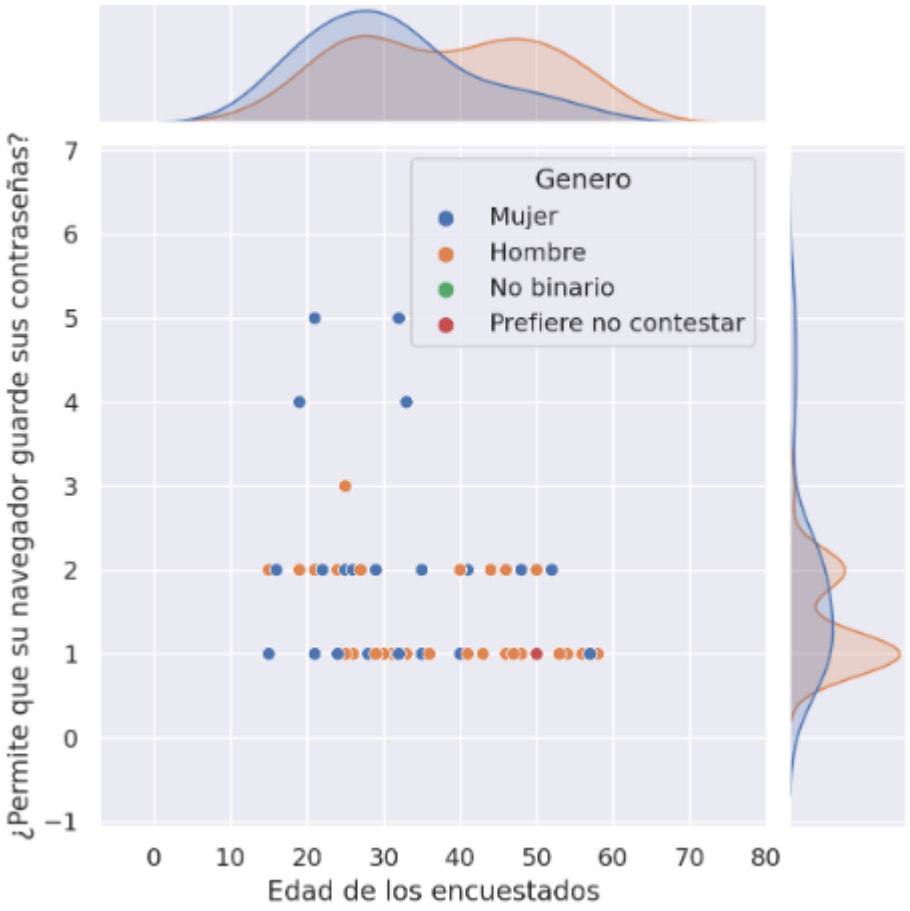
Figura 21 Correlación entre una contraseña fuerte y la edad



Elaboración propia mediante Python

En la figura 21. Se grafica la calificación de una contraseña fuerte y la edad de los encuestados con el objetivo de determinar si hay una correlación lineal entre estas dos varíales

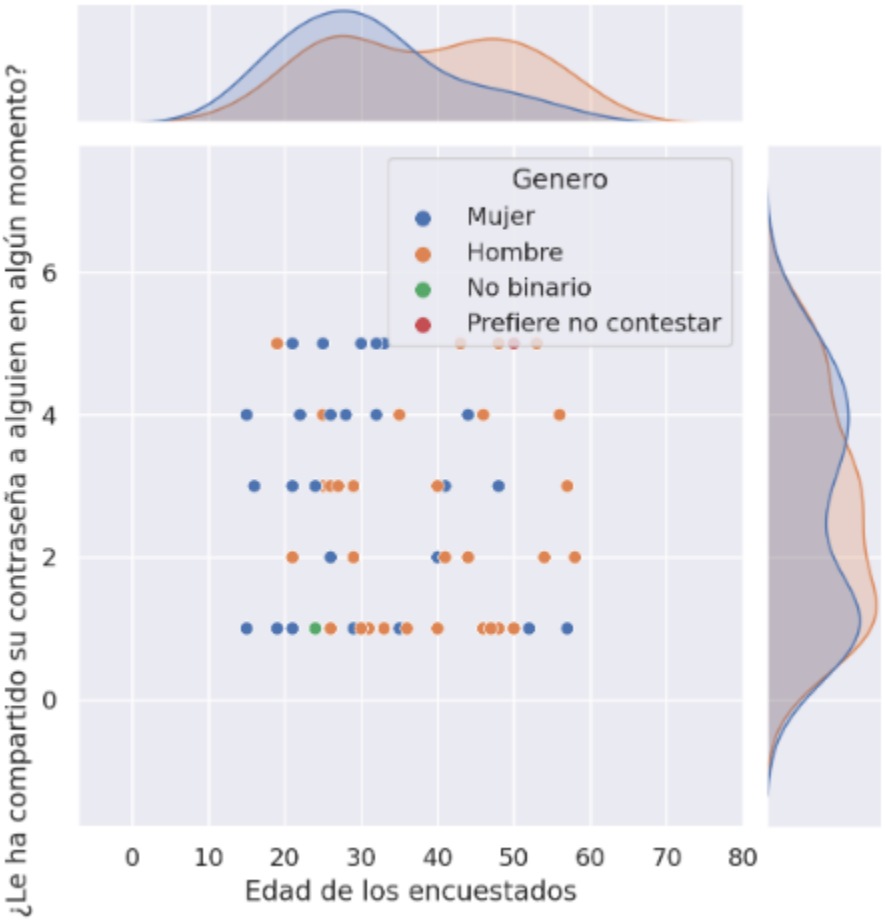
Figura 22 Correlación entre una mala práctica de seguridad y la edad



Elaboración propia mediante Python

En la figura 22 se grafica la calificación de una mala practica de seguridad con la edad de las personas encuestadas, con el objetivo de determinar sí hay correlación entre estas dos variables.

Figura 23 Correlación entre una falla de seguridad y la edad de los encuestados



Elaboración propia mediante Python

En la figura 23 se grafica la calificación de una falla de seguridad con la edad de las personas encuestadas, para determinar si hay una correlación entre estas dos varíales

Discusión de Resultados

A continuación, se exponen los resultados más relevantes de la encuesta y se analizaran los resultados obtenidos de la muestra de 72 personas encuestadas

De acuerdo con los resultados de la encuesta podemos realizar la discusión de los resultados. Para esto nos apoyaremos de la matriz de riesgo de que encontramos en la tabla 1, como parámetro de medición o de valoración, teniendo en cuenta el promedio de las respuestas globales de cada pregunta y se asignara una valoración de baja, media o alta de acuerdo con los resultados de la encuesta

Variables valoradas dentro de la matriz de riesgo según los resultados

Tabla 16 Matriz de riesgo valoración contraseñas

Variables/Riesgo	Alta	Media	Baja
encriptación de claves	Perdida de información Financiera	Resultado (2.05) Posible robo de información personal	Perdida de información publica
Nivel de información compartida en redes sociales	Exposición de información personal	Riesgo de suplantación de identidad resultado 2.43	Posible Spam
Compras o transacciones en línea	Robo de información de medios de pago	Riesgo de suplantación de identidad Resultado 2.43	Falla de entrega de productos
Apertura de links mediante mensajes de texto o e-mails	Virus y programa maligno, que afecte sus equipos de cómputo y/o robo de información	posible estafa o Phishing resultado 2.17	Spam o publicidad no deseada

Fuente: elaboración propia mediante Excel

Tabla 17 tabla de valoración matriz de riesgo

Puntuación	Viabilidad
1	baja
2	media
3	alta

Fuente: fuente (Rodríguez, 2011)

En la tabla 18 encontramos la tabla de valoración propuesta para alimentar la matriz riesgo (tabla 17), con el cual se valoran las calificaciones de la encuesta y si hacer match con los objetivos propuestos en la presente investigación.

Tabla 18 Tabla de comparación de calidad de contraseñas

	Bloque De Contraseñas					
Características en contraseñas	Fechas Nacimientos	Números ID	Es la misma para varias aplicaciones	Es Genéricas	La Comparten	No la Cambia
Media	1,96	1,74	1,74	1,47	2,67	2,71
Mediana	1,00	1,00	1,00	1,00	3,00	3,00
Moda	1,00	1,00	1,00	1,00	1,00	3,00
Desviación estándar	1,48	1,37	1,37	1,09	1,52	1,33
Varianza de la muestra	2,18	1,89	1,89	1,18	2,31	1,76
Rango	4,00	4,00	4,00	4,00	4,00	4,00
Mínimo	1,00	1,00	1,00	1,00	1,00	1,00
Máximo	5,00	5,00	5,00	5,00	5,00	5,00
Cuenta	72,00	72,00	72,00	72,00	72,00	72,00

Fuente: elaboración propia mediante Excel

Como se aprecia en la tabla 9, que es la contraparte de este bloque donde se pone un ejemplo de contraseña segura, con un nivel de encriptación alto la media esta más baja del promedio de la tabla 18. Lo que confirmaría que la calidad de contraseñas es coherente par la calificación en la matriz de riesgo

Tabla 19 Bloque estadísticas medios de pago utilizados por los encuestados

Bloques medios de pago						
Medios de pago	T crédito	T debito	Paypal	Nequi	Daviplata	Otros
Media	2,24	2,99	2,18	3,07	2,10	2,03
Error típico	0,18	0,20	0,18	0,19	0,18	0,17
Mediana	1,00	3,00	1,00	3,00	1,00	1,00
Moda	1,00	1,00	1,00	5,00	1,00	1,00
Desviación estándar	1,54	1,71	1,53	1,60	1,51	1,40
Varianza de la muestra	2,38	2,92	2,35	2,57	2,29	1,97
Coeficiente de asimetría	0,75	-0,05	0,87	-0,05	1,04	1,05
Rango	4,00	4,00	4,00	4,00	4,00	4,00
Mínimo	1,00	1,00	1,00	1,00	1,00	1,00
Máximo	5,00	5,00	5,00	5,00	5,00	5,00
Cuenta	72,00	72,00	72,00	72,00	72,00	72,00

Fuente: elaboración propia mediante Excel

En la tabla 19, se centra en un bloque las preguntas relacionadas con los medios de pago que utilizan las personas encuestadas.

Se aprecia que hay una leve tendencia entre las personas encuestadas a preferir Nequi sobre otros medios de pago

Tabla 20 Bloque estadísticas vulnerabilidad a robo información

Bloque Exposición a robo información			
Item	Inf Personal en redes	Abrir Enlaces	Guarda CS navegador
Media	2,13	1,57	2,82
Error típico	0,10	0,10	0,18
Mediana	2,00	1,00	3,00
Moda	2,00	1,00	1,00
Desviación estándar	0,84	0,89	1,55
Varianza de la muestra	0,70	0,78	2,40
Coeficiente de asimetría	0,35	2,23	0,10
Rango	4,00	4,00	4,00
Mínimo	1,00	1,00	1,00
Máximo	5,00	5,00	5,00
Cuenta	72,00	72,00	72,00

Fuente: elaboración propia mediante Excel

En la tabla 20, encontramos los datos estadísticos de las preguntas relacionadas con la medición de la vulnerabilidad de las personas encuestadas a ser victimas de robo de información por exposición de información personal, por malas prácticas o malos hábitos frente a su información personal.

La encuesta se diseñó para no hacer preguntas con un lenguaje técnico, como vulnerabilidad, brechas se seguridad, malas prácticas de ciber seguridad, en lugar de eso, se pusieron ejemplos de estos parámetros en las preguntas y de allí se clasificaron los tres bloques principales de respuestas

Alineado con el objetivo de Analizar el conocimiento de las personas encuestadas sobre la necesidad de resguardar sus datos personales:

Basado en la matriz de riesgo (tabla 17) la cual se alimentó con los valores de la matriz de puntuación (tabla 18) y las fuguras 21, 22 y 23 podemos inferir que las personas encuestadas tienen un conocimiento medio-bajo frente a los parámetros, prácticas o que son vulnerabilidades de seguridad.

La encuesta se diseño para no hacer preguntas con un lenguaje técnico, como vulnerabilidad, brechas se seguridad, malas practicas de ciber seguridad, en lugar de eso, se pusieron ejemplos de estos parámetros en las preguntas y de allí se clasificaron los tres bloques principales de respuestas.

Alineado con el objetivo de identificar que tan seguros son los medios que utilizan las personas pares proteger sus datos.

Se evidencia que hay un riesgo medio-alto a que las personas tengan se víctima de algún tipo de fraude o suplantación, de acuerdo con la calificación de la matriz de riesgo (tabla 17) en las variables “compras en línea” y “nivel de información que exponen en redes sociales”

Esto podría ser explotado por un ciberdelincuente mediante ingeniería social en el caso que llegara a se objetivo esta practica de crimen, hay que tener en cuenta que los fines de la ingeniería social son únicamente económico, también hay motivaciones de causar daño reputacional, o de fuga o comercialización de los datos sensibles de las personas encuestadas con fines publicitarios o a campañas políticas y de algún otro tipo de perdida de la privacidad.

Dando cumplimiento al objetivo de proponer una metodología de autoevaluación para que una persona identifique su nivel de vulnerabilidad frente a un ciber ataque se propone las siguientes técnicas

Contraseñas seguras:

una contraseña segura es una que tenga mas de 8 caracteres alfanuméricos y además que contenga símbolos especiales, como el ejemplo de la encuesta

(df3*15qs09-43). La desventaja es que no es fácil de recordar sin embargo una técnica es utilizar frases fáciles de recordar como “cumploenenero”, claro, escrita así es una contraseña débil,

Figura 24 Calificación de contraseñas

Fuente de figura 24 (Kaspersky, S.F)

pero si esta frase la escribimos cambiando las vocales por números quedaría así “c5mpl03n3n3r0” esta ya es una contraseña que tiene un nivel de encriptación muy bueno.

Figura 25 Verificación de contraseña segura

Fuente; (Kaspersky, S.F)

Como se puede verificar en la calificación de la contraseña de la figura 25, esta memo-técnica para utilizar una frase fácil de recordar, pero cambiando las vocales por numeros aumenta significantemente la encriptación de la contraseña. En la medida que se adquiera el habito de cifrar las contraseñas será más fácil desarrollar contraseñas cada vez mas complejas

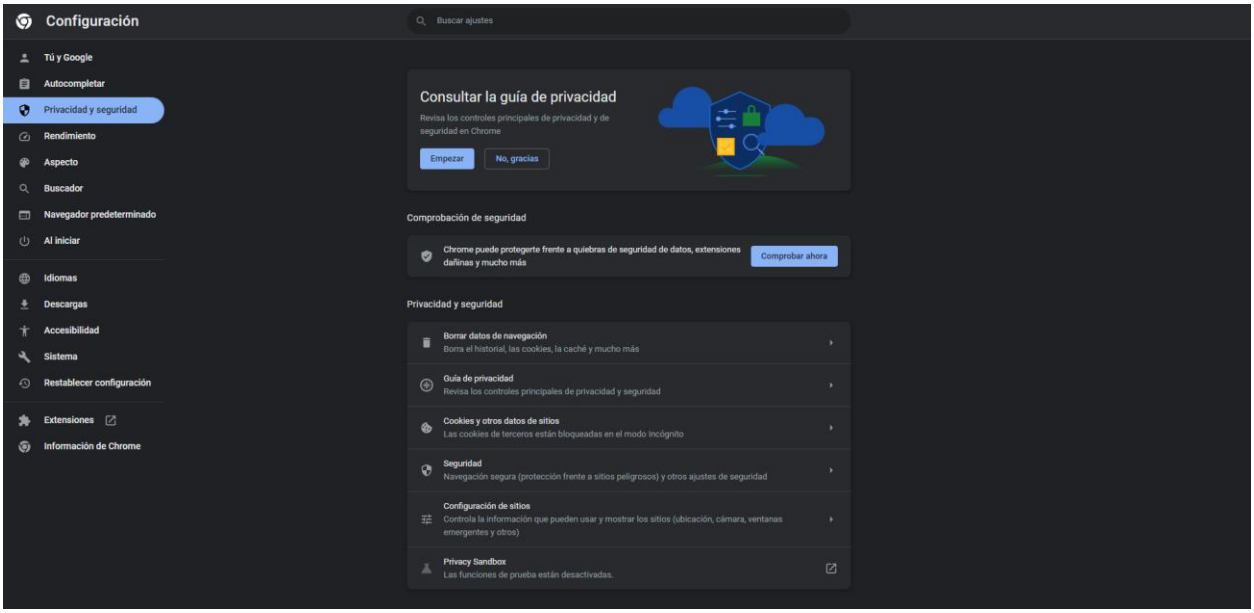
Cambiar periódicamente las claves:

las contraseñas se deben cambiar periódicamente, la recomendación de los expertos es cada mes cambiar las contraseñas para asegurar que solo el titular de la información tiene acceso a la información.

Evitar guardar las contraseñas

en el navegador, el navegador siempre da la opción de guardar las contraseñas y el algoritmo de la página, tiene la capacidad de recordar el sitio web donde se utiliza esta contraseña. Pero esta es una brecha de seguridad, ya que esta información puede ser accedida fácilmente si es victima de Phishing. Cómo verificar si tiene contraseñas guardadas y de que sitios

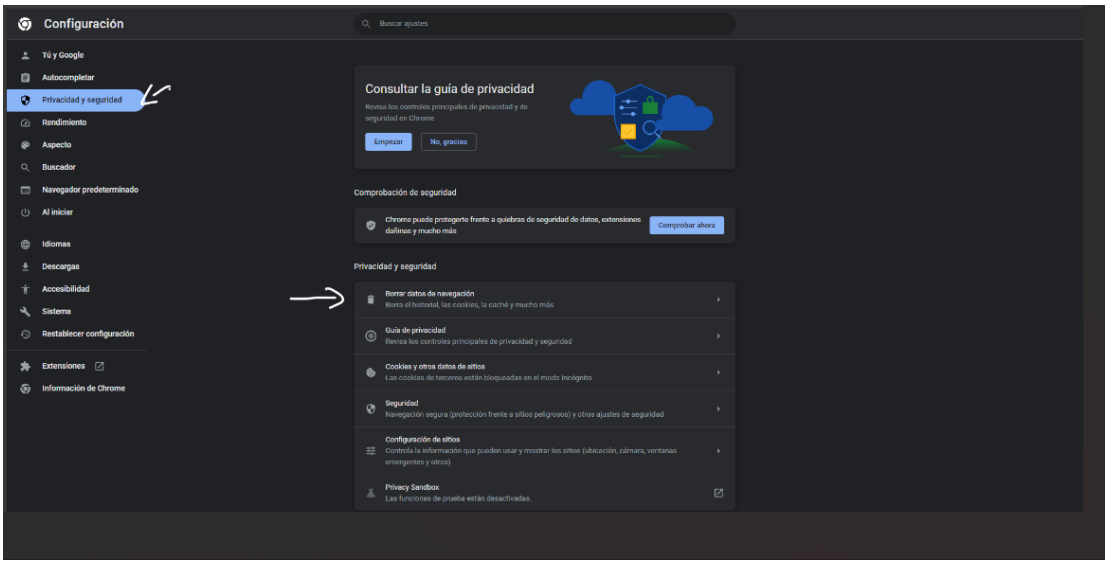
Figura 26 Acceder al historial del navegador mediante ctrl+h se acede al historial



Fuente (Google.com, s.f.)

En la figura 26, se toma como ejemplo el navegador de Google, y se accede al historial de navegación mediante Ctrl+h

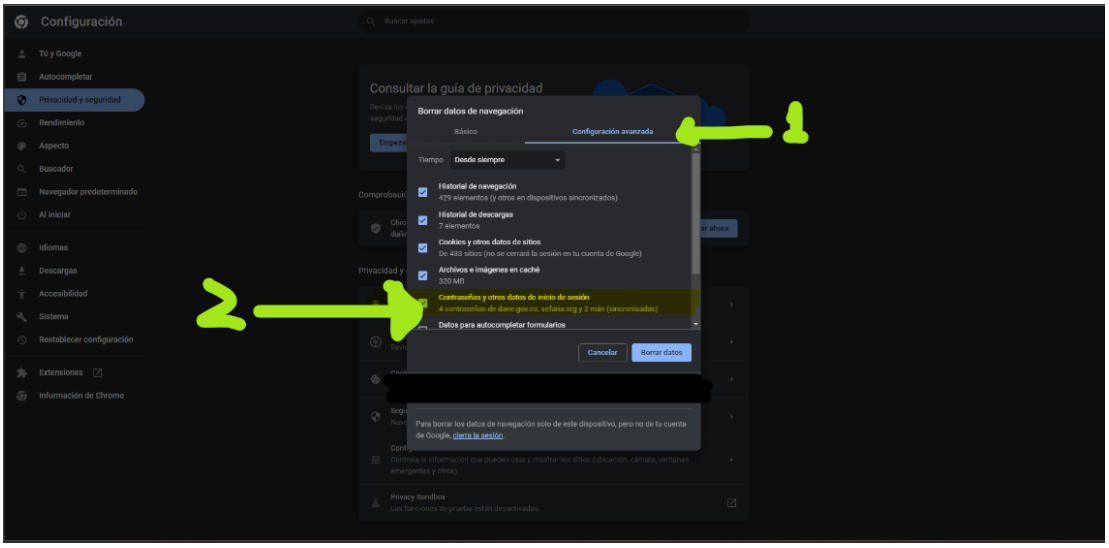
Figura 27 Borrar contraseñas del navegador



Fuente: (Google.com, s.f.)

En la figura 27 se describe como acceder la historial de navegación para verificar si hay contraseñas guardadas que eventualmente pueden ser capturadas mediante Phishing o cualquier programa maligno.

Figura 28 Aqui aparecen las contraseñas guardades



Fuente (Google.com, s.f.)

En la figura 28 encontramos que al seleccionar estas opciones y dar clic en borrar datos se eliminan del navegador las contraseñas guardadas incluso si se guardaron de manera automática, este procedimiento se debe realizar para todos los navegadores que estén instalados en la computadora que utilizamos.

Verificación de enlaces:

De acuerdo con los expertos, se debe evitar a toda costa dar clic en enlaces que ofrezcan premios, ganancias inmediatas, o que ha sido seleccionado para alguna promoción o rebaja.

También desconfiar de mensajes de texto, o al correo electrónico como que su cuenta de ahorros ha sido bloqueada, ingrese al siguiente enlace para desbloquearla.

También puede ser un mensaje como, se ha realizado una compra de xxxx$ con su tarjeta de crédito o débito, si no fue usted, ingrese al siguiente enlace para reversar la compra.

Al ingresar a estos enlaces fraudulentos, lo puede direccionar a una página similar a la de su entidad bancaria y capturar sus datos de acceso a su cuenta y ser víctima de un fraude.

O instalar un programa maligno que toma el control de sus dispositivos móviles y acceder a toda la información que esté en su computadora, como medios de pago, contraseñas, números de tarjeta o toda la información bancaria,

Por otra parte, puede ser victima de secuestro de toda la información que ese en la computadora, mediante la encriptación y luego le exigen pago por entregarle el control nuevamente de su información,

Este ultimo punto es posible, sí se comparte demasiada información en redes sociales, donde algún ciberdelincuente encuentra una persona como objetivo de ingeniería social se iniciar un proceso de perfilación y explotación de las vulnerabilidades.

Cuando inicia la explotación de las vulnerabilidades mediante los mensajes sospechosos, es posible que sea ya fue víctima de ingeniería social o algún perfilamiento para ser atacado.

Conclusiones

La respuesta a la pregunta de la investigación: ¿Están las personas conscientes de la importancia de resguardar sus datos personales en la era digital?,

Teniendo en cuenta las variables y la metodología de cuantificar los datos mediane la matriz de riesgo, se podría inferir que hay una preparación media-baja de las personas encuestadas de la importancia de resguardar los datos personales en esta era digital.

No hay una correlación entre la edad y contraseñas débiles que permita afirmar en esta investigación que, por ejemplo, en nivel de encriptación de las contraseñas está en función de la edad o del género.

Así mismo no hay una correlación entre las malas practicas de seguridad como permitir que el navegador gurde las contraseñas, en función de la edad o del género.

Tomando como base; que todos tenemos derecho a la privacidad, como está plasmado en el capitulo 15 de la constitución política de Colombia y que nadie tiene derecho a violar esta privacidad personal o de la familiar resulta fácil pensar que este derecho es respetado por los demás.

Ahora bien, en el mundo real, en el entorno de ciber ecosistema, hay una creciente ola de violación del derecho a la intimidad, como se relacionó en esta investigación es un fenómeno global que afecta a grandes y medianas empresas con consecuencias que afectan amiles de personas.

Pero también hay un aumento exponencial de ataques a personas del común que son víctimas de suplantación y robo, estafas.

Aquí es donde surgen las preguntas: ¿a quién le corresponde velar por la integridad de la privacidad?

Una respuesta podría ser que, debería sobrevivir el mas apto, es decir que el que tenga mas recursos para enfrentar los peligros y superarlos.

Y esto tiene una lógica de la naturaleza sobreviven los que mejor se adaptan al entorno, y el entorno es que hay peligros de ser suplantados, manipulados mediante la información que cada persona está poniendo a disposición para ser explotada con fines extorsivos.

La ventaja es que aquí la adaptación no está sujeta o no es dependiente de la genética, o de las cualidades que le dé a un individuo la naturaleza, esta ventaja se puede adquirir de forma consciente de la realidad del entorno y de las medidas que cada persona tome para cerrar brechas de seguridad como:

Aumentar la encriptación de claves de acceso

Cambiar cada mes las claves de acceso.

Evitar utilizar una misma contraseña para todas o varias aplicaciones

Evitar anotar las contraseñas en cualquier lugar, sea físico como en un papel o cuaderno o algún archivo en la computadora que alguien pueda acceder a estas claves.

Verificar los mensajes y los sitios web para verificar la autenticidad

Evitar abrir todos los enlaces que llegan al correo electrónico o mensajes de texto para minimizar el riesgo a ser suplantado y victima de secuestro o robo de información,

Estas serían las conclusiones de esta investigación, pero queda mucho por estudiar, aquí en el alcance de esta investigación cubrimos las medidas básicas de conocimiento que debe tener una persona para estar adaptada a esta realidad de la sociedad.

Quedan por abordar temas de ciberseguridad como la infraestructura básica de un hogar para que sea una red familiar segura. Hacer una identificación de riesgos de la red de wifi del hogar, como identificar quien tiene acceso, qué tan vulnerable es un hogar a un ciber ataque.

Síntesis:

La presente investigación se centró en evaluar mediante las herramientas metodológicas ya expuestas sí las personas son conscientes de la importancia de resguardar sus datos personales en esta era digital con la variables ya expuestas y analizadas.

En este contexto actual, y las implicaciones que el adquirir una buenas practicas para resguardar los datos, sobre la base del autocuidado resulta esencial abrir nuevas oportunidades para realizar nuevas investigaciones adicionales que podrían ser las siguientes:

1) La influencia de la educación en la conciencia de la seguridad de los datos: investigar cómo la educación formal y la capacitación en seguridad de datos, afectan la conciencia de las personas sobre la importancia de proteger sus datos personales. Sobre esta base, se podría realizar un estudio comparativo entre personas que han recibido educación especifica en seguridad digital y aquellas que no han la han recibido y analizar si hay una correlación entre el conocimiento y la adopción de buenas practicas en ciberseguridad.
2) Factores psicológicos y de comportamiento en la protección de los dados personales: investigar cómo los factores psicológicos y de comportamiento influyen en las decisiones de las personas para proteger o exponer su datos

personales por ejemplo en redes sociales, sobre la base de la percepción del riesgo y la confianza que hay en redes sociales y plataformas digitales y así investigar sí hay motivadores subyacentes que impulsan a las personas a adoptar o no, una actitud de autocuidado de los datos personales.

3) Efectividad de las políticas y regulaciones de protección de datos: evaluar la efectividad de las políticas y regulaciones existentes para la protección de datos personales, ejemplo; una línea de investigación podría ser cómo las organizaciones adoptan y se apegan a la norma de protección de los datos (1581 de 2012) y en virtud de esta norma que tanto conocen las personas naturales los derechos que busca proteger esta norma antes de aceptar o firmar el tratamiento de datos personales.

Es así como se puede cerrar esta investigación inicial destacando la necesidad de la conciencia en las buenas prácticas de seguridad de los datos personales en esta era digital.

Al abordar las áreas mencionadas en este trabajo podemos desarrollar una compresión más completa de cómo las personas interactúan con la protección de sus datos lo que permite adoptar medidas básicas de autocuidado frente a los peligros y asumir o no los riesgos con herramientas básicas pero efectivas.

Referencias

Ahmed Aleroud, L. Z. (2017). Entornos, técnicas y contramedidas de phishing: una encuesta. *Informática y Seguridad*, 160-196. doi:https://doi.org/10.1016/j.cose.2017.04.006

Bailón, T. A. (13 de Ocubre de 2021). *El mercado del seguro: impacto de las nuevas tecnologías en el sector asegurador.* Recuperado el 20 de Febrero de 2023, de https://uvadoc.uva.es/bitstream/handle/10324/53259/TFG-E-1378.pdf?sequence=1&isAllowed=y

Borghello, C. (13 de abril de 2019). *El arma infalible, la ingeneiria Social*. Obtenido de Technical & Educational Manager de ESET para Latinoamérica: https://d1wqtxts1xzle7.cloudfront.net/55136701/Arma_Infalible_-_Ingenieria_Social-libre.pdf?1511889264=&response-content-disposition=inline%3B+filename%3DEl_arma_infalible_la_Ingenieria_Social.pdf&Expires=1682864960&Signature=TXmYZr~bWXONel3jO5r~CGvf9eAOk

Borghello, C., & Temperini, M. (2012). *Suplantación de Identidad Digital como delito informático en Argentina.* La Plata: Simposio Argentino de Informática y Derecho .

Castro Jaramillo, Á. M. (2016). *Derecho a la intimidad en las redes sociales de internet en Colombia.* (U. l. Colombia, Ed.) Cali, Colombia. doi:10.14718/NovumJus.2016.10.1.5

Castro, M. I. (2018). *INTRODUCCIÓN A LA SEGURIDAD INFORMÁTICA Y EL ANÁLISIS DE VULNERABILIDADES.* Alicante: Área de Innovación y Desarrollo,S.L.

Cristian Borghello, T. M. (2012). Suplantación de Identidad Digital como delito informático en Argentina. *Simposio Argentino de Informática y Derecho (SID 2012)(XLI JAIIO, La Plata, 27 al 31 de agosto de 2012)*.

Díaz, A. F. (Noviembre de 2019). *SUPLANTACIÒN DE IDENTIDAD DIGITAL UNA REALIDAD ECONÒMICA EN COLOMBIA.* Bogota: UNIVERSIDAD LIBRE FACULTAD DE CIENCIAS ECONÓMICAS, ADMINISTRATIVAS Y CONTABLES INSTITUTO DE POSGRADOS. Obtenido de https://hdl.handle.net/10901/22284

Dubout, F. (2020). *Prevenir el fraude en tiempos dificiles.* NG2 Business Park. Nottingham, NG801ZZ: The sir John Peace Building, Experian Way.

El Informador.mx. (13 de enero de 2023). *Detectan fraude en ofertas laborales a través de celular*. Obtenido de www,informador.mx: https://www.informador.mx/Fraudes-Detectan-ofertas-laborales-falsas-a-traves-de-celular-l202301130001.html

Ferguson, P. &. (Abril de 1998). *What is a VPN?* Non Citie: Non Editorial .

Forbes. (20 de Diciembre de 2022). *Ransomware en Colombia seguirá causando disrupciones: la necesidad de tomar medidas urgentes*. Obtenido de forbes.co: https://forbes.co/2022/12/20/tecnologia/ransomware-en-colombia-seguira-causando-disrupciones-la-necesidad-de-tomar-medidas-urgentes

Google. (01 de abril de 2023). *www.colab.research.google.com/*. Obtenido de Te damos la bienvenida a Colaboratory: https://colab.research.google.com/

Google.com. (s.f.). *Navegador de goole Historia de navegacion ctrl+h*.

Grande, C. E. (2015). Ingeniería Social: El Ataque Silencioso. *REVISTA TECNOLÓGICA N˚ 8*, 38-45.

ICONTEC. (18 de Febrero de 2022). *Norma ISO 27001 de 2013 Seguridad de la Informacion*. Obtenido de www.icontec.org: https://www.icontec.org/eval_conformidad/certificacion-iso-27001-sistemas-de-gestion-de-seguridad-de-la-informacion-2/

Isaak, J., & Hanna, M. J. (agosto de 2018). User Data Privacy: Facebook, Cambridge Analytics, and Privacy Protection. *THE POLICY CORNER*.

Kaspersky. (S.F). *Kaspersky password checker* . Obtenido de https://password.kaspersky.com/es/

Lauren, S. G.-P. (2011). Defeating pharming attack at the client-side. *5th International Conference on Network and System Security*, 33-40. doi:10.1109/ICNSS.2011.6059957 .

Limon Vidal, L. L. (2016). Suplantación de identidad y su uso en las redes sociales. *Ecos Sociales*, 214-218.

Mendo, Á. (2014). *DELITOS Y REDES SOCIALES: MECANISMOS FORMALIZADOS DE LUCHA Y DELITOS MÁS HABITUALES. EL CASO DE LA SUPLANTACIÓN DE IDENTIDAD.* III Fórum de Expertos y Jóvenes Investigadores en Derecho y nuevas tecnologías (FODERTICS)...

Montero, M. I. (2013). Criptografía y psicología de la contraseña: generando una contraseña fuerte para diferentes servicios. *Apuntes ciencia & sociedad*. doi:https://doi.org/10.18259/acs.2013008

Ornelas, J. L. (2020). CONVIVENCIA: LA VÍA PARA GENERAR DOMINIOS DE LIBERTAD Y LAS AMENAZAS A SU AUTOPOIESIS EN LA ERA DIGITAL. *Revista Contribuciones a las Ciencias Sociales,*. Obtenido de www.eumed.net/rev/cccss/2020/03/convivencia-era-digital.html

Owalda, A. (2 de agosto de 2021). *Estafas en Amazon: conozca los modelos de fraude más comunes*. Obtenido de www.welivesecurity.com: https://www.welivesecurity.com/la-es/2021/08/05/estafas-amazon-conozca-modelos-fraude-mas-comunes/

Pandas ORG. (24 de abril de 2023). *Pandas documentation*. Obtenido de www.pandas.pydata.org : https://pandas.pydata.org/docs/

Python . (30 de Abril de 2023). *www.python.org/*. Obtenido de Sitio oficial Python : https://www.python.org

Rangel, M. R. (2020). Desafíos nacionales frente a la ciberseguridad en el escenario global: un análisis para Colombia. *Rev. Crim. / Volumen 62 - Número 2*, 199-217.

Rehman, I. u. (2019). Facebook-Cambridge Analytica data harvesting: What you need to know. *Library Philosophy and Practice (e-journal). 2497.* Obtenido de https://digitalcommons.unl.edu/libphilprac?utm_source=digitalcommons.unl.edu%2Flibphilprac%2F2497&utm_medium=PDF&utm_campaign=PDFCoverPages

Rodríguez, C. P. (2011). ¿CÓMO CONSTRUIR UNA MATRIZ DE RIESGO OPERATIVO? *Ciencias Económicas 29-No. 1*, 630-635.

seaborn pydata org. (30 de Abril de 2023). *www.seaborn.pydata.org*. Obtenido de seaborn: statistical data visualization: https://seaborn.pydata.org/index.html

Security Standards Council. (17 de Febero de 2023). *Norma PCI DSS*. Obtenido de www.pcisecuritystandards.org: https://www.pcisecuritystandards.org/minisite/es-es/

Suarez, J. L. (2020). *Seguridad Informática y Ciberseguridad.* Bogotá: Universidad Piloto de Colombia.

Temperini, B. C. (2012). *Suplantación de Identidad Digital como delito informático en Argentina.* La Plata: Simposio Argentino de Informática y Derecho.

Triola, M. f. (2004). *Estadistica Novena Edición.* Mexico: Pearson Edicación.

Usma Espinel, F. (2016). El consentimiento en los contratos en línea B2C y su protección bajo la ley colombiana. *Cuadernos De La Maestría En Derecho, (5), 287–330.* Obtenido de https://revistas.usergioarboleda.edu.co/index.php/Cuadernos/article/view/997