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

Francisco Federico Murillo Villareal

Fmurillo9096@universidadean.edu.co

Resumen

La era digital ha traído como resultado la mejora en aspectos de la vida cotidiana como; la comunicación, la agilidad con la que las personas acceden a bienes y servicios mediante medios electrónicos, así como tramites que antes se debían realizar de forma presencial en una oficina llevar papeles, hacer fila en una entidad pública o privada por mencionar solo algunas.

Esta facilidad de acceder a necesidades trajo una reducción de tiempo en el acceso a servicios, tramites, así como acortar distancias mediante las comunicaciones, antes de la era digital enviar una comunicación escrita dependiendo de la distancia podía tardar semanas ahora las personas se conectan a un clic de distancia.

Sin embargo, esta era digital también trajo consigo nuevas formas de ataques, de crimen por razones económicas o ideológicas y aunque a nivel de empresas, gobierno hay estándares y reglas de seguridad las personas del común como usted que esta leyendo esto puede haber una alta probabilidad que sea victima de uno de estos ataques. Este trabajo intenta averiguar que tanto son conscientes las personas como usted de resguardar los datos y dar herramientas básicas para aumentar la seguridad de sus datos.

Introducción

Sobre la base que en esta era hay un conjunto variado de personas de varias edades niveles socioeconómicos y diferentes tipos de formación es interesante analizar si hay una diferencia marcada en los diferentes sectores de la sociedad frente a la seguridad de los datos que es el eje central en el que gira esta investigación.

¿por qué los datos son fundamentales? Porque a medida que los datos de las personas estén expuestos a personas mal intencionadas se aumenta la probabilidad que alguien sea víctima de algún tipo de ciber ataque en este entorno digital o ciber ecosistema (Bailón, 2021).

Ahora bien, si alguien se pregunta eso solo pasa en otros países en otras sociedades lejos de aquí y solo se escucha en las noticias la verdad es que pasa más cerca de los que se piensa como el caso de EPM

o Keralty que fueron víctimas de un ciber ataque aquí en Colombia afectando a miles y miles de usuarios (Forbes, 2022) y (ManageEngine, 2023)

Y tal vez usted que está leyendo esto, se pregunte, ¿y eso que tiene que ver conmigo?, eso solo pasa a grandes empresas. La respuesta es que hay miles de personas afectadas a nivel mundial por ciber delincuentes (Torres M, 2019) y claro Colombia no es la excepción.

Marco de referencia

Para tener un contexto claro de la importancia del objeto de esta investigación abordaremos si todo lo referente a ciber seguridad es algo trivial o tiene alguna relevancia para alguien u otras personas se han tomado el trabajo de investigar y escribir sobre la importancia de resguardar los datos personales como un activo o algo que tiene mucho valor, y hay un nuevo término "ingeniería social" (Borghello, 2019).

Entonces aquí encontramos dos variables, una que es la información de las personas que son susceptibles de comercialización como el caso de los datos de millones de personas que fueron comercializados con fines de manipulación política de acuerdo con el trabajo de (Isaak & Hanna, 2018).

La otra variable es desde las empresas que deben manejar los datos de las personas para brindar servicios el modelo de Busines to Consumers que no es otra cosa que empresas que conectan a las necesidades de las personas con los servicios que ofrece una entidad mediante centros de atención telefónica (Call Centeres) de acuerdo con el trabajo de (Usma Espinel, 2016).

En el primer caso, la identidad de las personas es vulnerada si ningún tipo de legislación clara y en el segundo ejemplo soy hay un marco regulatorio que las empresas que se dedican a este sector de la economía deben seguir para poder funcionar.

El punto en común en estos dos escenarios anteriores es que los datos de las personas son uno de los activos de mas alto valor para las organizaciones.

Desde el punto de vista de (Castro Jaramillo, 2016) el concepto de la intimidad ha sido trasformado debido a las redes sociales debido a que en este ciber ecosistema este es uno de los focos más débiles para que los datos sensibles de las personas sean expuestos o puedan ser víctimas de ingeniería social con fines delictivos.

En el marco de referencia expuesto anteriormente este trabajo se enfoca en investigar que tan vulnerables son las personas a un ciber ataque sobre las siguientes variables o puntos críticos en los que se basan los ciber delincuentes para suplantar personas, realizar transacciones bancarias o compras como si las realizara la persona titular causando una afectación económica.

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.

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.

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. Rangos de edad de los entrevistados

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

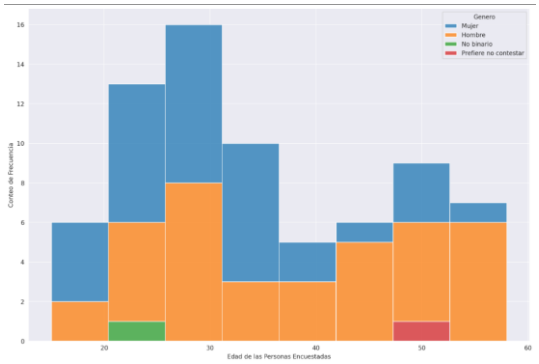
La encuesta se realizó a 72 personas, que contestaron la encuesta de forma libre y espontanea mediante la difusión de la encuesta, compartiendo el enlace mediante grupos de WhatsApp, Facebook.

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

Figura 1 Análisis de Frecuencia Edad y Genero Personas Encuestadas



Elaboración propia mediante Python

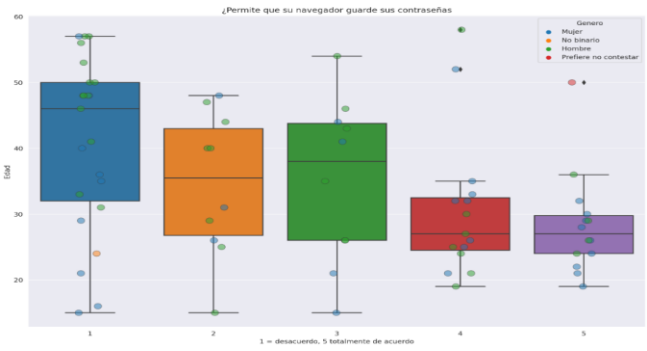
En la figura 1, encontramos una descripción demográfica de las personas que contestaron la encuesta de donde se extraen los datos de las variables. Donde se aprecia que la muestra está distribuida de forma equivalente entre hombres y mujeres

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.

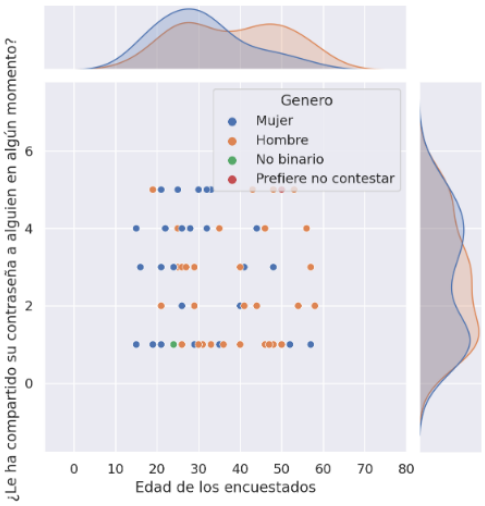
Figura 2 Modelo de tratamiento de cada pregunta para su valoración estadística



Elaboración propia mediante Python

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

Figura 3 Ejemplo de medir correlación entre preguntas y la edad de los encuestados



Elaboración propia mediante Python

Como se aprecia en la figura 3. No hay correlación en una pregunta en función de la edad de los encuestados que permita relacionar la edad con alguna brecha de seguridad.

Variables valoradas dentro de la matriz de riesgo según los resultados

Tabla 1 Matriz de calificación de los resultados

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 2 Matriz de puntuación

Puntuación	Viabilidad
1	baja
2	media
3	alta

Fuente: fuente (Rodríguez, 2011)

En la tabla 2 encontramos la tabla de valoración propuesta para alimentar la matriz riesgo tabla 1, con el cual se valoran las calificaciones de la encuesta y si hacer match con los objetivos propuestos en la presente investigación.

Tabla 3 Resultados estadístico bloque de preguntas sobre contraseñas de los encuestados

	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 3, 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 2. Lo que confirmaría que la calidad de contraseñas es coherente par la calificación en la matriz de riesgo

Tabla 4 Resultados estadístico bloque de preguntas sobre medios que pago de 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 4, 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 5 Resultados estadísticos de exposición a robo de información de los encuestados

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

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 prácticas 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 capítulo 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 a miles 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 más apto, es decir que el que tenga más recursos para enfrentar los peligros y superarlos.

Y esto tiene la lógica de la naturaleza donde sobreviven los que mejor se adaptan al entorno, y el entorno 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 víctima 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.

Agradecimientos

Agradecimientos al Profesor Luis Armando Cobo por el acompañamiento durante todo el trabajo de investigación, el direccionamiento y las aclaraciones suyas fueron esenciales para realizar este interesante trabajo y pasar de verlo como una materia más a un instrumento de investigación útil para la vida profesional.

Así mismo agradezco a las personas que se tomaron el tiempo de responder la encuesta ya que sin los datos recolectados este trabajo no hubiese sido posible.

Bibliografía

Bailón, T. A. (13 de Ocubre de 2021). 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

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

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

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

ManageEngine. (13 de Enero de 2023). *Ataque de ransomware a Keralty: ¿acto cibercriminal o desafío a la seguridad de las compañías?* Obtenido de logs.manageengine.com/espanol/2023/01/13/ataque-ransomware-keralty-sanitas-colsanitas-html.html#:~:text=El%20ataque%20de%20ransomware%20afectó,y%20Colsanitas%2C%20del%20grupo%20Keralty.

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

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

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

Torres M, A. (2019). *SUPLANTACIÒN DE IDENTIDAD DIGITAL UNA REALIDAD ECONÒMICA EN COLOMBIA.* Bogota: UNIVERSIDAD LIBRE, FACULTAD DE CIENCIAS ECONÓMICAS, ADMINISTRATIVAS Y CONTABLES.

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