TRABAJO DE GRADO

ATAQUE CONTROLADO DE INGENIERIA SOCIAL USANDO CODIGOS QR

HERNAN DARIO CARVAJAL

JOHN ALEXANDER CASTELLANOS

UNIVERSIDAD CATÓLICA DE COLOMBIA

FACULTAD DE INGENIERÍA

PROGRAMA DE ESPECIALIZACIÓN EN SEGURIDAD DE LA INFORMACIÓN

BOGOTÁ D.C 2019

creative commons

Atribución-NoComercial 2.5 Colombia (CC BY-NC 2.5)

La presente obra está bajo una licencia:
Atribución-NoComercial 2.5 Colombia (CC BY-NC 2.5)
Para leer el texto completo de la licencia, visita:
http://creativecommons.org/licenses/by-nc/2.5/co/

Usted es libre de:

Compartir - copiar, distribuir, ejecutar y comunicar públicamente la obra

hacer obras derivadas

Bajo las condiciones siguientes:

Atribución — Debe reconocer los créditos de la obra de la manera especificada por el autor o el licenciante (pero no de una manera que sugiera que tiene su apoyo o que apoyan el uso que hace de su obra).

No Comercial — No puede utilizar esta obra para fines comerciales.

TRABAJO DE GRADO

ATAQUE CONTROLADO DE INGENIERIA SOCIAL USANDO CODIGOS QR

DIRIGIDO POR:

ING RAUL BARENO GUTIERREZ

UNIVERSIDAD CATÓLICA DE COLOMBIA

FACULTAD DE INGENIERÍA

PROGRAMA DE ESPECIALIZACIÓN EN SEGURIDAD DE LA INFORMACIÓN

BOGOTÁ D.C 2019

Nota de Aceptación

_____
_____
_____
_____
_____
_____
_____

Firma del Presidente del Jurado

_____

Firma del Jurado

_____

Firma del Director

Fecha:

Bogotá, D.C., 2019

TABLA DE CONTENIDO

Pág.

INDICE DE TABLAS

INDICE DE IMÁGENES

- Fase II – (Ataque Controlado): Respecto a los alumnos de informática social, del total de volantes repartidos, el 42.9% fueron escaneados y diligenciaron la información que se los solicito.
- Fase II – (Ataque Controlado): Del total de volantes repartidos en los dos cursos, el 62.5% de los alumnos escanearon el código y diligenciaron la información que se los solicito.

Después del estudio de datos estadísticos Se seleccionó el curso que más fue impactado por el ataque y se realizó un feedback donde se les indico como se planeó el ataque, y como estos cayeron en él, se hicieron las respectivas recomendaciones y se diligenció un formato donde se evidencia la participación de dicho grupo.

La motivación de la investigación es medir estadísticamente las amenazas y vulnerabilidades de los códigos Qr, los códigos están presentes en ataques phishing en el mundo e identificar formas de mejorar la seguridad de la información, además de analizar los comportamientos de usuarios en el manejo de sus teléfonos inteligentes cuando visiten sitios web. Finalmente realiza contraste de los resultados del ataque controlado de ingeniería social además de las respectivas recomendaciones de prevención y mejores prácticas.

Palabras clave: Análisis; Escaneo; Ataque; QR; Phishing

ABSTRAC

This research project focuses on analyzing the different techniques that can be carried out social engineering attacks, the vulnerability and risks that arise in the use of qr codes, its operation is studied, therefore it proceeds to perform controlled social engineering attack using QR codes, in progress of the systems engineering program of the Catholic University of Colombia. The factor identified in the investigation, when reading the Qr codes, the source is not verified and there is no knowledge of its reliability, and falling into inappropriate hands as computer criminals can benefit and materialize the risks, access the user data, in this way the social engineering attack mode arises due to the vulnerability of the qr codes through phishing.

Given the selected sample of two systems engineering courses such as convergent network design and social engineering of the systems engineering program of the Catholic University of Colombia, 62.5% more than half fell under the form of social engineering attack through Phishing, all presented the initial survey of information security knowledge and all presumed to know about the subject in their responses but on the contrary in the attack were victims. According to the above, statistical data on the materialization of the attack is analyzed, these are some of the relevant data of the investigation.

• Phase I - (Survey): within the trend regarding the basic knowledge of students regarding the topic of information security and protection of personal data, the answers are at an Excellent level.
• Phase II - (Controlled Attack): It was evident that the students of network design and convergent services of the total number of leaflets distributed 100% were scanned and filled in the information requested.

• Phase II - (Controlled Attack): Regarding the students of social informatics, of the total number of leaflets distributed, 42.9% were scanned and filled in the information requested.
• Phase II - (Controlled Attack): Of the total of flyers distributed in the two courses, 62.5% of the students scanned the code and filled in the information requested.
After the study of statistical data, the course that was most impacted by the attack was selected and feedback was made where they were told how the attack was planned, and how they fell into it, the respective recommendations were made and a format where the participation of said group is evidenced.

The motivation of the investigation is to statistically measure the threats and vulnerabilities of the Qr codes, the codes are present in phishing attacks in the world and identify ways to improve the security of the information, in addition to analyzing the behaviors of users in the management of their Smartphones when visiting websites. Finally, it contrasts the results of the controlled social engineering attack in addition to the respective prevention recommendations and best practices.

Keywords: Analysis, Scan; Attack; QR; Phishing

1 INTRODUCCIÓN

La seguridad de la información se establece a partir de tres pilares fundamentales los cuales son disponibilidad, integridad y confidencialidad, estos cobran importancia en el manejo de datos personales, así como en las organizaciones, sin embargo, existen muchas amenazas que atentan contra esos pilares, entre ellos los factores de exposición a los diferentes métodos de ingeniería social.

Sin embargo, el manejo y cuidado de la información tiene que fortalecerse con la implementación de buenas prácticas de seguridad, para mitigar los riesgos a los que se expone la información al estar conectado a internet. La ingeniería social es similar al hacking, el cual es conocido por ser una intrusión abusiva a un sistema informático, para realizar un ataque de ingeniería social no se requiere de interacción con una máquina, por el contrario, hace uso de técnicas de engaño psicológico a personal que tenga acceso a la información, para finalmente

obtenerla con fines maliciosos.

"El primero en usar el término "Ingeniería Social" en el ámbito de la seguridad informática fue el reconocido hacker Kevin Mitnick, quien sostiene que la ingeniería social se refiere a la aplicación de técnicas, métodos informáticos que utilizan los hackers para engañar a un usuario e ingresar a los sistemas informáticos de una compañía, obtiene información sensible y confidencial, logrando de forma insospechada la captura de datos." [1]

La implementación de algoritmos, políticas de seguridad, firewalls conllevan a esfuerzos de análisis y complejidad, por lo que los atacantes les resulta efectivo esquivar los esquemas de seguridad con métodos de ingeniería social. Los ataques seducen a los usuarios a ingresar a páginas web no seguras, utilizando métodos de lectura de códigos QR y captura de datos.

En el presente documento se plantea un ejercicio académico utilizando técnica de phishing para realizar ingeniería social; a partir del uso de un código QR se pretende realizar la captura de información a una población específica, con el fin de demostrar los niveles de seguridad de los códigos y saber lo vulnerable que son las personas a la lectura de ellos.

Una vez obtenidos los resultados del ataque se espera lograr la sensibilización de la población participante para que de esta forma se verifique cierta información antes de realizar un escaneo y ello los lleve a realizar mejores prácticas que fomenten la seguridad de la información en sus diferentes ámbitos sociales.

2 DESCRIPCIÓN GENERAL

Es necesario conocer el funcionamiento de la ingeniería social; esta apunta a persuadir el factor humano en la estructura organizacional, considerada para muchos como la parte más débil del sistema.

Actualmente, la información es uno de los recursos más valiosos para las organizaciones, proteger adecuadamente los datos es de vital importancia, ya que pondría en riesgo el funcionamiento y rentabilidad del negocio. Por esta razón, las instituciones de gobierno, educativas y financieras, buscan la manera de implementar controles de seguridad para proteger su información como firewalls, políticas de seguridad, cámaras de vigilancia, sensores de proximidad, restricción de puertos de enlace.

Dado que la mente humana almacena información sensible, es un reto para las organizaciones asegurar la información que posee cada individuo al interior de la compañía, por esta razón, se concentran muchos esfuerzos en hacer campañas de sensibilización para el manejo adecuado de dicha información.

Siempre existe un riesgo humano presente en la ingeniería social. Si los ataques logran cumplir su objetivo, utilizando distintos métodos como engaño, suplantación, persuasión o llamada telefónica, y evadiendo candados físicos o lógicos que se crean para la protección de un activo, pueden apoderarse por medio de un individuo y dar acceso a los sistemas de información.

2.1 LÍNEA DE INVESTIGACIÓN

Investigación de Software inteligente y convergencia tecnológica

2.2 PLANTEAMIENTO DEL PROBLEMA

La tecnología avanza a grandes pasos y cada invención puede ser utilizada de diferentes maneras, por esa razón, se necesita una comprensión de las nuevas modalidades de comunicación que satisfacen determinadas exigencias y requerimientos, igualmente, el funcionamiento a grandes velocidades de conectividad y rendimiento de red.

Es necesario el uso de la tecnología en la vida diaria y es evidente la necesidad de conectividad constante, generando un aumento en el consumo de servicios virtuales tales como: productos y servicios web, publicidad en línea y campañas de mercadeo con vallas publicitarias.

Debido a lo anterior, es necesario analizar la influencia del consumismo y la navegación sin control en internet. Muchas personas utilizan diariamente vínculos web de manera indiscriminada. La presente investigación pretende dar a conocer una modalidad de interacción con códigos QR. Estos códigos operan al hacer lectura en un dispositivo móvil, obteniendo una rápida respuesta y finalmente direccionando a una URL. El problema radica en que las aplicaciones que emplean la función de leer un código QR no tienen oportunidad de inspeccionar la procedencia de la URL antes de visitarla.

Hay muchas aplicaciones y servicios web conocidos que fueron vulnerables a este ataques de código QR hasta la fecha, Aquí hay algunos ejemplos que incluyen, entre otros: WhatsApp, WeChat, Line, Weibo, QQ Instant Messaging, QQ Mail (Personal y Empresa Corporativa), Yandex Mail según los reportes investigados.

Normalmente, al realizar lectura de los códigos QR, no se verifica la fuente y no se tiene conocimiento de su confiabilidad. Los delincuentes informáticos pueden sacar provecho de este descuido, escanear los códigos representa un riesgo cuando no se realiza la verificación de su origen, además, puede ser una gran fuente de información y ayudar a un atacante a encontrar un vía para filtrarse internamente en los servicios de las organizaciones o acceder a los datos de los usuarios.

"QRLJACKING responde a código de hacking como vector de ataque de ingeniería social capaz de secuestro de una sesión que afecta todas la aplicaciones y páginas web con la función de iniciar sesión con códigos QR como una forma segura de iniciar y verificar enlaces web, lo que resulta en un secuestro y sustracción de información" [2]

De esta manera, surge una nueva modalidad de ataque de ingeniería social, a través de la vulnerabilidad de los códigos QR. Los atacantes presentan ventaja al tener el factor sorpresa, esto facilita el robo de la información y el daño a la reputación.

2.2.1 Antecedentes del problema

Existen diferentes tipos de amenazas de ciberseguridad y diversas modalidades de operación, se debe tener en cuenta que es uno de los eslabones de la ingeniería, por medio de la interacción social, el cual aprovecha la vulnerabilidad que presentan los códigos QR.

El código QR (o código de respuesta rápida) es un código de barras de matriz que puede ser leído por un dispositivo con imágenes de la cámara y luego procesado para leer sus datos. Fue desarrollado inicialmente para la industria automotriz en Japón, pero ahora está siendo utilizado por muchas compañías. El código QR fue inventado en 1994 por Denso Wave. Hoy en día, los códigos QR se utilizan para mostrar texto a los usuarios, para guardar una información de contacto de vCard en el teléfono inteligente del usuario, para abrir una URL de sitio web [3]

Según un estudio realizado en la Universidad Carnegie Mellon en Pittsburgh Pennsylvania especializada en estudios tecnológicos y de ciberseguridad, La navegación en internet permite que los usuarios tengan mayor posibilidad de escanear datos sin necesidad de realizar una autenticación [4]

Uno de los ataques de código QR más conocidos, se registró en el ámbito internacional al gigante de los dispositivos móviles APPLE a lo largo del año 2017, su sistema operativo fue víctima de ataques y vulnerabilidades impensables, el lector integrado de códigos QR, que por defecto accionaba la cámara de IOS, en el fallo se evidencio, los usuarios estaban siendo dirigidos a sitios web maliciosos sin su conocimiento [5]

2.2.2 Pregunta de investigación

¿Podrá ser peligroso escanear cualquier código QR en la universidad católica de Colombia?

2.2.3 Variables del problema

- Se realiza la medición de datos proporcionados por el ataque de ingeniería social por medio de códigos QR
- Nivel de seguridad de los códigos QR
- Confiabilidad en el número de personas que realizaran el experimento de ataque controlado con códigos QR.
- Medir las amenazas y vulnerabilidad de los códigos QR

2.3 JUSTIFICACIÓN

Según los estudios Carnegie Mellon University Pittsburgh los códigos (QR) se están generalizando rápidamente en los entornos urbanos de todo el mundo. Los códigos QR se utilizan para representar datos, como una dirección web, en una forma sencilla que puede ser fácilmente escaneado y analizado por dispositivos móviles de consumo. [6]

Sin embargo, esta tecnología anima a los usuarios móviles a escanear datos no autenticados de carteles, vallas publicitarias, calcomanías, y más, proporcionando un nuevo vector de ataque. Los atacantes pueden atraer usuarios para escanear los códigos y luego visitar sitios web maliciosos, instalar programas o cualquier otra acción en el dispositivo móvil.

De acuerdo con lo antepuesto, se identifica que las aplicaciones que emplean la función de leer un código QR no tienen la función de inspeccionar la fuente de la URL antes de visitarla.

El plan y motivo de la investigación es medir las amenazas y vulnerabilidad de códigos QR, los códigos presentan un vector de ataque de phishing e identificar formas de mejora para la seguridad de la información respecto a la interacción del código QR.

El interés de analizar comportamientos de los usuarios de teléfonos inteligentes cuando hacen lectura de un código QR, en los laboratorios de informática de la universidad Católica de Colombia, la consecuencia es la visita al sitio web desde el código QR. Al realizar el ataque controlado el experimento se podrá comprobar, la facilidad con la que se puede crear y distribuir un código QR y hacerlo atractivo para dirigir a las personas a un sitio web por medio de la técnica del phishing.

2.4 OBJETIVOS

2.4.1 Objetivo general

Realizar un ataque controlado de ingeniera social usando códigos QR, en un curso del programa de ingeniería de sistemas de la Universidad Católica de Colombia

2.4.2 Objetivos específicos

- Analizar las distintas técnicas con las que se pueden realizar ataques de ingeniería social, sus características y vectores.
- Implementar el ataque controlado usando la técnica de phishing para hacer ingeniería social usando como vector códigos QR.
- Contrastar los resultados del ataque controlado contra la evaluación y encuesta, además las respectivas recomendaciones de prevención y alertas oportunas

1.5.2.3 . Alcances

Implementar un phishing suplantando la página de inicio de la Universidad Católica de Colombia, en curso del programa de Ingeniería de Sistemas, los estudiantes acceden a ella escaneando un código QR que se entrega previamente impreso en un volante, la información que se entrega motiva por medio de ingeniería social que realicen voluntariamente y digiten libremente la información requerida, además sujetas de acuerdo con la ley 1581 del 2012 de protección de datos personales. De acuerdo con lo anterior, se lleva a cabo la realización del ataque de forma controlada en diferentes fases:

Evaluación (Formulario), por instrucción del docente de dicho curso con el fin de cuantificar el conocimiento en el tema de los estudiantes.

- Implementación del phishing y captura de datos a través de la ingeniería social.
- Encuesta de post-ataque.
- Contraste de resultados obtenidos por el ataque

1.6 CRONOGRAMA

Se describen las actividades a realizar durante el proyecto como se muestra a continuación en el cronograma.

Imagen 1. Cronograma de actividades 1

Modo de tarea	EDT	Nombre de tarea	Duración	Comienzo	Fin	Predecesoras	Nombres de los recursos
	1	**Inicio De Proyecto**	**1 día**	**mié 20/03/19**	**mié 20/03/19**		
	1.1	Solicitud VoBo de la Universidad Católica	41 días	sáb 06/04/19	vie 31/05/19		
	1.1.1	Asignacion tutor	1 día?	mié 27/03/19	mié 27/03/19		
	1.1.2	Envio de correo electronico con la solicitud	1 día	sáb 06/04/19	sáb 06/04/19		Lider de Proyecto
	1.1.3	Envio Boseto	1 día	lun 13/05/19	lun 13/05/19		
	1.2	Documentacion y Planeacion de Anteproyecto	48 días	mié 27/03/19	vie 31/05/19		
	1.2.1	Definir Objetivo General y Especificos	6 días	sáb 30/03/19	vie 05/04/19		
	1.2.2	Marco referencial	4 días	vie 05/04/19	mié 10/04/19		
	1.2.2.1	Levantamiento de informacion sobre ataques de ingenieria social en Colombia	1 día	vie 05/04/19	vie 05/04/19		Lider de Proyecto
	1.2.2.2	Verificacion de estadisticas de ataques de ingenieria social en colombia	1 día	sáb 06/04/19	sáb 06/04/19		Lider de Proyecto
	1.2.2.3	Investigacion sobre poblacion vulnerable en Colombia	1 día	lun 08/04/19	lun 08/04/19		Lider de Proyecto
	1.2.2.4	Verificacion de legislacion Nacional e Internacional	1 día	mar 09/04/19	mar 09/04/19		Lider de Proyecto
	1.2.2.5	Estudio Tecnico de ataques de ingenieria social con codigos QR	1 día	mié 10/04/19	mié 10/04/19		Lider de Proyecto, Lider Tecnico
	1.2.3	Definicion Marco Teorico	2 días	jue 11/04/19	vie 12/04/19		Lider de Proyecto
	1.2.4	Elección de población a atacar	2 días	sáb 13/04/19	lun 15/04/19		Lider de Proyecto
	1.2.5	Planteamiento Del Problema	3 días	lun 15/04/19	mié 17/04/19		
	1.2.6	Presupuesto	3 días	jue 18/04/19	lun 22/04/19		
	1.2.7	Pregunta de investigación	3 días	dom 21/04/19	mar 23/04/19		
	1.2.8	Alcance	4 días	mié 24/04/19	sáb 27/04/19		
	1.2.9	Metodologia	7 días	dom 28/04/19	sáb 04/05/19		
	1.2.10	Identificacion de Herramientas a Utilizar	4 días	sáb 04/05/19	mié 08/05/19		
	1.2.11	Limitaciones	3 días	jue 09/05/19	dom 12/05/19		
	1.2.12	Definicion de estrtategia de comunicación	5 días	lun 13/05/19	vie 17/05/19		
	1.2.13	Correcciones documento	10 días	sáb 18/05/19	jue 30/05/19		
	1.2.14	Sustentacion de Anteproyecto	1 día	sáb 15/06/19	sáb 15/06/19		
	2	**Diseño y implementacion del Proyecto**	**33 días**	**lun 02/09/19**	**mié 16/10/19**		
	2.1	Rediseño del proyecto	11 días	lun 02/09/19	dom 15/09/19		
	2.1.1	Definir nuevo titulo y Objetivos	6 días	lun 02/09/19	lun 09/09/19		
	2.1.2	Ajustes al documento	5 días	mar 10/09/19	dom 15/09/19		
	2.2	Diseño y implementacion de Codigo QRs	5 días	lun 16/09/19	vie 20/09/19		
	2.2.1	Investigacion y definicion de herramienta para codigos QR	3 días	lun 16/09/19	mié 18/09/19		Lider Tecnico
	1.2.4	Elección de población a atacar	2 días	sáb 13/04/19	lun 15/04/19		Lider de Proyecto
	1.2.5	Planteamiento Del Problema	3 días	lun 15/04/19	mié 17/04/19		
	1.2.6	Presupuesto	3 días	jue 18/04/19	lun 22/04/19		
	1.2.7	Pregunta de investigación	3 días	dom 21/04/19	mar 23/04/19		
	1.2.8	Alcance	4 días	mié 24/04/19	sáb 27/04/19		
	1.2.9	Metodologia	7 días	dom 28/04/19	sáb 04/05/19		
	1.2.10	Identificacion de Herramientas a Utilizar	4 días	sáb 04/05/19	mié 08/05/19		
	1.2.11	Limitaciones	3 días	jue 09/05/19	dom 12/05/19		
	1.2.12	Definicion de estrtategia de comunicación	5 días	lun 13/05/19	vie 17/05/19		
	1.2.13	Correcciones documento	10 días	sáb 18/05/19	jue 30/05/19		
	1.2.14	Sustentacion de Anteproyecto	1 día	sáb 15/06/19	sáb 15/06/19		
	2	**Diseño y implementacion del Proyecto**	**33 días**	**lun 02/09/19**	**mié 16/10/19**		
	2.1	Rediseño del proyecto	11 días	lun 02/09/19	dom 15/09/19		
	2.1.1	Definir nuevo titulo y Objetivos	6 días	lun 02/09/19	lun 09/09/19		
	2.1.2	Ajustes al documento	5 días	mar 10/09/19	dom 15/09/19		
	2.2	Diseño y implementacion de Codigo QRs	5 días	lun 16/09/19	vie 20/09/19		
	2.2.1	Investigacion y definicion de herramienta para codigos QR	3 días	lun 16/09/19	mié 18/09/19		Lider Tecnico

Fuente: Autores

En la imagen 1 se identifica el inicio del proyecto con su respectiva planeación y documentación con los ítems a desarrollar de comienzo a fin en cada etapa, además del diseño, ejecución y control con sus respectivos ítem de seguimiento para los entregables finales.

1.7 PRESUPUESTO

Para la preparación y presentación del presupuesto se deben tener en cuenta las siguientes indicaciones:

Tabla 1.Presupuesto global de la propuesta por fuentes de financiación

RUBROS	VALOR UNITARIO	VALOR TOTAL
PERSONAL	38.750.000	80.500.000
ESTACION DE TRABAJO	968750	1.937.500
SOFTWARE	0	0
MATERIALES	300.000	300.000
HOSTING	0	0
TOTAL	**40.018.750**	**82.737.500**

Fuente: Formato utilizado por Colciencias

Tabla 2.Descripción de los gastos de personal

INVESTIGADOR / EXPERTO/ AUXILIAR	FORMACIÓN ACADÉMICA	FUNCIÓN DENTRO DEL PROYECTO	DEDICACIÓN Horas/semana	VALOR
Ingeniero 1	Especialista	Líder Técnico	1240	38.750.000
Ingeniero 2	Especialista	Gerente Proyecto	1240	38.750.000
Ingeniero 3	Especialista en Desarrollo	Desarrollador Web	100	3.000.000
TOTAL				**80.500.000**

Fuente: Formato utilizado por Colciencias

Tabla 3. Descripción y cuantificación de los equipos de uso propio (en miles de $)

Tabla 3.Descripción y cuantificación de los equipos de uso propio

EQUIPO	VALOR TOTAL
ESTACION DE TRABAJO	968750
ESTACION DE TRABAJO	968750
TOTAL	**1.937.500**

Fuente: Formato utilizado por Colciencias

Tabla 4.Materiales y suministros

MATERIALES[1]	JUSTIFICACIÓN	VALOR TOTAL
Resma de papel	Documentación	60000
Carteleras	Herramienta de ataque en el proyecto	120000
Lapiceros	Documentación	20000
Volantes Código QR	Para las encuestas y ataque controlado	100.000
TOTAL		**300.000**

Fuente: Formato utilizado por Colciencias

[1] https://www.colciencias.gov.co/sites/default/files/upload/convocatoria/anexo3_3.pdf

2 MARCOS DE REFERENCIA

2.5 MARCO CONCEPTUAL

Los códigos QR se originan a partir de la matriz de los códigos de barras, y estos se están generalizando rápidamente por todo mundo Estos códigos se utilizan para representar datos y direccionar a una página web de una manera rápida, puede ser fácilmente escaneado y utilizado por dispositivos móviles alrededor del mundo. Estos son populares en las cadenas de ventas comerciales debido a su versatilidad.

"Códigos QR fueron creados en 1994 por Denso Wave, subsidiaria japonesa en el Grupo Toyota. El uso de esta tecnología es ahora libre. El Código QR no es el único código de barras de dos dimensiones en el mercado, otro ejemplo es el código de matriz de datos. En el 2010, Códigos QR comenzaron a expandirse en los EE.UU. y luego en Europa, donde pueden verse notablemente en los anuncios." [7]

Los códigos QR, fueron creados inicialmente para registrar los repuestos de la fabricación de partes de vehículos. La aparición y popularización de dispositivos móviles contribuyó a que se expandieron por el mundo. [8]

Sin embargo los atacantes atraen a los usuarios para escanear los códigos qr bajo pretextos, induciéndolos a visitar sitios web maliciosos, con el fin de capturar información del dispositivo móvil e iniciar un ataque en la modalidad de phishing, se evidencia en este trabajo de investigación aplicada. [9]

2.1 ESTADO DEL ARTE

2.2.0 Ataque de ingeniería social

Se realiza ataque de ingeniería social de manera controlada, explotando la seguridad orientada a el factor humano, mediante el uso de técnicas en este caso de Phishing, por medio de engaños obtendremos la información se captura por medio de la actividad de identificación de la red y datos suministrados con consentimiento. [10]

2.2.0.1. HISTORIA DE LA INGENIERÍA SOCIAL

El uso de la expresión se inició en 1894 con un ensayo del empresario y filántropo holandés J.C. Van Marken, difundido en Francia por Émile Cheysson (uno de los integrantes del Musée Social), pero recibió su mayor impulso en EE.UU. a través del libro "Social Engineering" del reformista social W.H. Tolman, conocido en aquella época por "ayudar a los pobres". La idea central es que no había en las empresas una función social (algo así como los departamentos de recursos humanos de hoy), por lo que el ingeniero social tenía una función de mediador para resolver los conflictos como intermediador racional entre el capital y el trabajo. En esta acepción, el ingeniero social debía contar con habilidades sociales, en contraste con el uso posterior del término, basado en la metáfora de la máquina que se convierte en el núcleo del concepto peyorativo actual. Se sugiere que el origen del término está en el concepto filantrópico de los pensadores liberales de la segunda mitad del siglo XIX como los "intermediarios racionales" entre el capital y el trabajo. Para las décadas 30 y 40 del siglo XX el término había caído en desuso. [11]

2.2.1 Tipos de ataque de ingeniería social

2.2.2. Carnada

Los humanos somos curiosos, lo cual es fundamental en estas situaciones. El cibercriminal puede dejar un dispositivo, como una memoria USB, infectado con software malicioso a la vista en un espacio público. Alguien recoge ese dispositivo y lo conecta a su equipo para ver qué contiene.

En ese momento, el software malicioso se introduce en el equipo. [12]

2.2.3. Phishing

Es el fraude informático mediante correo electrónico, comúnmente denominado phishing, es un proceso fraudulento de la rama de la ingeniería social cuyo objetivo es adquirir información sensible como nombres de usuario, claves o datos de cuentas o tarjetas de crédito, a través de una comunicación electrónica, fingiendo ser una entidad de confianza, tal como un banco o una entidad gubernamental. El término phishing proviene de la palabra en inglés "fishing" (pesca) y hace alusión al acto de "pescar" usuarios mediante "anzuelos" (trampas) cada vez más sofisticados para obtener contraseñas e información financiera [13]

Esta táctica depende de que los usuarios tomen decisiones basadas en el miedo, en lugar de pensar por un momento en la situación. A través de correos electrónicos simulan provenir de una figura de autoridad, ejemplo alguien de mayor jerarquía en la empresa que solicita su nombre de usuario y contraseña para poder acceder a un sistema. Las personas suelen cumplir con lo solicitado si proviene de un compañero de trabajo, en particular si tiene mayor jerarquía administrativa.

2.2.4 Hacking de correo electrónico y envío de spam a contactos

Actualmente se denomina Spam o "correo basura" a todo tipo de comunicación no solicitada, realizada por vía electrónica. De este modo se entiende por Spam cualquier mensaje no solicitado y que normalmente tiene el fin de ofertar, comercializar o tratar de despertar el interés respecto de un producto, servicio o empresa. Aunque se puede hacer por distintas vías, la más utilizada entre el público en general es mediante el correo electrónico. Esta conducta es particularmente grave cuando se realiza en forma masiva. [14]

Es por lo que cibercriminales buscan las direcciones de correo electrónico y las contraseñas, una vez que obtienen esas credenciales, pueden apoderarse de la cuenta y enviar spam a todos los contactos de la libreta de direcciones del usuario. El objetivo principal es difundir software

malicioso, engañar a las personas para obtener sus datos personales.

2.5.5. Pretexto

Un pretexto es una historia elaborada que inventa el cibercriminal con el fin de crear una situación en la cual atrapar a sus víctimas, generalmente con una historia trágica. Estos tipos de situaciones apelan a la tendencia de las personas a ayudar a quienes lo necesitan (compasión). El atacante se hace pasar por otra en una llamada telefónica. [15]

2.5.8 Vishing

De todos estos métodos, el vishing es el que involucra mayor interacción humana. El criminal llama al empleado de una empresa y se hace pasar por una persona de confianza o por un representante de su banco o de otra empresa con la cual tiene negocios. Luego, intenta obtener información del objetivo haciéndose pasar por un compañero que perdió su contraseña (y le pide al empleado la suya) o haciéndole una serie de preguntas para verificar su identidad. [16]

2.5.9. Hunting

El hunting es la versión corta de estos ataques. Normalmente, los cibercriminales usan el phishing, la carnada y el hacking de correo electrónico con el propósito de extraer tantos datos como pueda de la víctima con la menor interacción posible. [17]

2.5.9.1 Farming

Es una estafa de larga duración, en la cual los cibercriminales buscan establecer una relación con el objetivo. Normalmente, observan los perfiles de redes sociales del objetivo e intentan construir una relación con él basada en la información que recopilan durante la investigación. Este tipo de ataque también depende del pretexto, ya que el atacante intenta engañar a la víctima por tanto tiempo como puede para obtener todos los datos que sean posibles. [18]La ingeniería social está en todos lados, en línea y sin conexión. El gran éxito que tiene se debe al único componente

involucrado en el que no se puede instalar software de seguridad: el ser humano. La mejor defensa contra estos tipos de ataques es informarse y conocer las señales de alerta.

2.5.9.2 Ataques de ingeniería social

Los ataques de ingeniería social tienen un rápido crecimiento en los dispositivos móviles y computadoras, se encuentra la información sensible y de importancia almacenada. Por lo anterior crece la demanda de ataques en este tipo de equipos y por consecuencia aplicaciones maliciosas que pueden espiar o robar la información y acceder [19]

2.5.9.3. Ataques de ingeniería social y susceptibilidad de códigos qr en ataques de phishing en dispositivos móviles

Según los estudios carnegie mellón university Pittsburgh los códigos (QR) se están generalizando rápidamente en los entornos urbanos de todo el mundo. Los códigos qr se utilizan para representar datos, como una dirección web, en una forma compacta que puede ser fácilmente Escaneado y analizado por dispositivos móviles de consumo. [20]

Sin embargo, esta tecnología anima a los usuarios móviles a escanear datos no autenticados de carteles, vallas publicitarias, calcomanías, y más, proporcionando un nuevo vector de ataque para los atacantes. Por posicionar códigos QR bajo pretextos, los atacantes pueden atraer usuarios para escanear los códigos y luego visitar sitios web maliciosos, instalar programas o cualquier otra acción en los dispositivos móviles

Tabla 5.Aplicaciones de IOS y Android, visitan automáticamente Url con códigos QR

Rank	Application	Vendor	Auto Visit
1	Barcode Scanner	Versolab	no
2	ShopSavvy (Barcode and QR Scanner)	ShopSavvy, Inc.	yes
3	RedLaser Barcode and QR Scanner	eBay, Inc.	no
4	ScanLife Barcode and QR Reader	Scanbuy, Inc.	yes
5	AT&T Code Scanner	AT&T Inc	no
6	pic2shop - Barcode Scanner	Vision Smarts	no
7	Bakodo - Barcode Scanner	Dedoware, Inc	no
8	NeoReader - QR reader	NeoMedia Technologies, Inc	yes
9	i-nigma QR Code scanner	3GVision	yes
10	MOBILETAG - Barcode Scanner	Mobile Tag	yes

(a) iOS Applications

Rank	Application	Vendor	Auto Visit
1	Barcode Scanner	ZXing	no
2	ShopSavvy Barcode Scanner	ShopSavvy, Inc.	yes
3	QuickMark Barcode Scanner	SimpleAct, Inc.	no
4	RedLaser Barcode and QR Reader	eBay Mobile	no
5	ScanLife Barcode and QR Reader	Scanbuy, Inc.	yes
6	Barcode scanner	george android	no
7	i-nigma Barcode Scanner	3G Vision	yes
8	AT&T Code Scanner	AT&T Service, Inc.	no
9	ixMAT Barcode Scanner	ixellence.com	no
10	BARCODE SCANNER	Jet Ho	no

(b) Android Applications

Fuente: Seguridad en dispositivos móviles tomado de: http://repositorio.unap.edu.pe/handle/UNAP/7047

De acuerdo con Tabla 5 se puede identificar que las aplicaciones que emplean la función de leer un código QR no tienen en lo absoluto la oportunidad de inspeccionar la procedencia de la URL antes de visitarla.

A continuación, ejemplos de ataques de ingeniería social con códigos QR:

Imagen 2. Personalización de códigos qr

Fuente: Articulo seguridad en dispositivos http://repositorio.unap.edu.pe/handle/UNAP/7047

Este ataque comprende como se muestra en la imagen 2 la utilización de una herramienta poderosa llamada Kali Linux cuyo fin con el ataque es exponer la ingeniería social para captar la información. Para empezar, abrimos Kali Linux y en la consola se escribe: setoolkit

Imagen 3. Kali linux

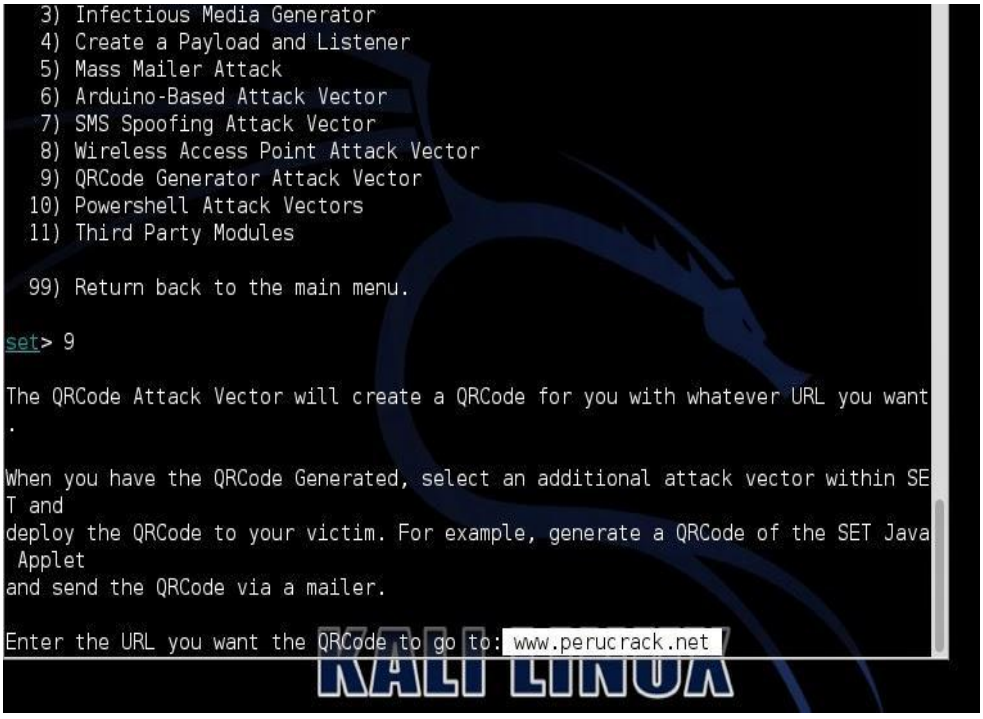
Fuente: https://hackingpills.blogspot.com/2018/03/hack

Como se muestra en la Imagen 3, Aparece el menú de opciones de esta potente e intuitiva herramienta. [21]
Luego se hace clic en la siguiente opción:

Opcion 1) Social-Engineering Attacks
Opcion 9) QR code generator Attack vector

Este arreglo informático nos proporciona la ruta que queremos atacar y dirigir al escanear el código QR en el dispositivo.

Imagen 4. Implementación KALI LINUX [16]



Fuente: https://hackingpills.blogspot.com/2018/03/hack

Se mueve imagen a código QR

Se enlaza al código QR Imagen 4 algún sitio malicioso para móviles, alguna aplicación apk con el fin de obtener datos e infectar a la víctima ya todo depende de la ingeniería social. [22]

cp/root/.set/reports/qrcode_attack,pnp/root/Desktop

2.5.9.3 Estadísticas

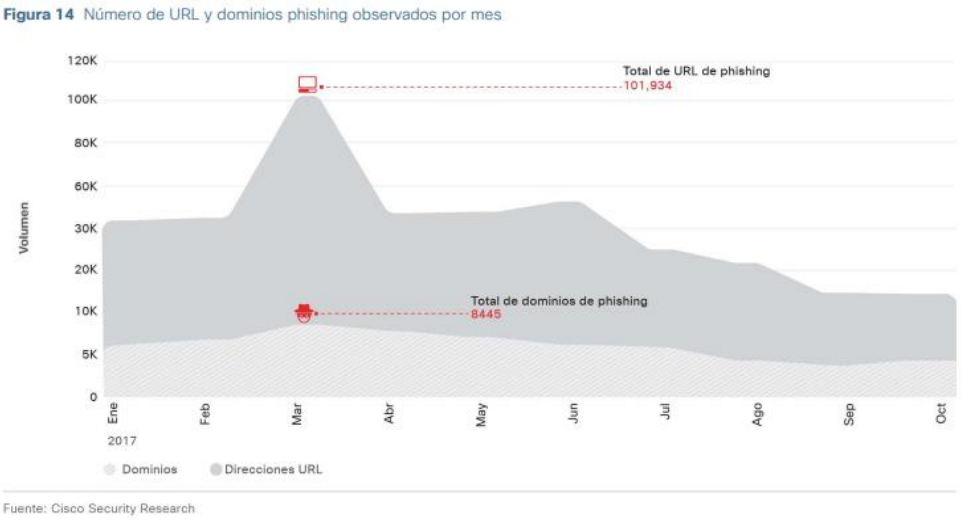
2.5.9.4. Internacional aplicación de ingeniería social

La ingeniería social presenta diferentes plataformas para el lanzamiento de ataques ya sea de correo electrónico o phishing y spear phishing son tácticas para apoderarse y apropiarse de la información, robar credenciales de los usuarios por medio de engaños, información sensible y de

mucha importancia. Muchos de estos ataques, se evidencian en coreos electrónicos, URL y dominios redirigidos con la modalidad de phishing y spear phishing de hoy, aprovechando las brechas y aplicando la ingeniería social.

A continuación, se muestra las estadísticas de la investigación de ataque de ingeniería social de la marca CISCO empresa estadounidense enfocada en el desarrollo y fabricación de hardware de redes y equipos de telecomunicaciones por diferentes países del mundo.

Imagen 5. Número de URL y dominios de ob



Fuente: latam. Kaspersky laboratorio

“Los investigadores de amenazas de Cisco examinaron datos de fuentes que investigan correos electrónicos potencialmente "phishing" enviados por usuarios a través de inteligencia contra amenazas de phishing basada en la comunidad. La imagen 5 muestra el número de URL de phishing y dominios de phishing observados durante el período de enero a octubre de 2017.” [23]En la imagen 5 se pueden observar picos en marzo y junio, esto se puede atribuir a dos campañas diferentes. El primero parecía dirigirse a los usuarios de un importante proveedor de servicios de telecomunicaciones. La campaña:

- Involucró 59,651 URL que contenían subdominios bajo information [dot]org.

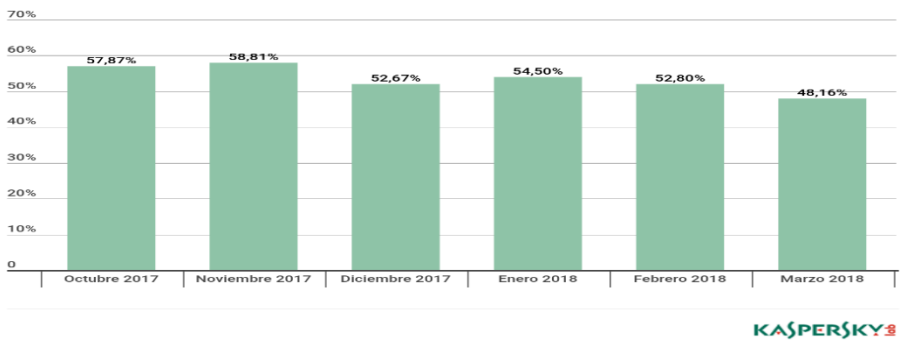
- Tenía subdominios que contenían secuencias al azar consistentes de 50-62 letras.

Cada longitud de subdominio (50-62) contenía aproximadamente 3500 URL, lo que permitió el uso programático de los subdominios.

2.5.9.6. Porcentaje de spam de tráfico a nivel internacional y el mundo

Como se evidencia en la imagen 6 parte inferior, en el primer trimestre de 2018 la mayor parte del spam (54,50%) se registró en enero. El promedio de spam en el tráfico postal mundial fue del 51,82%, que es de 4,63 p.p. por debajo del promedio del último trimestre de 2017 [24]

Imagen 6. Porcentaje de spam en el tráfico en 2018



Fuente: Kaspersky [9].

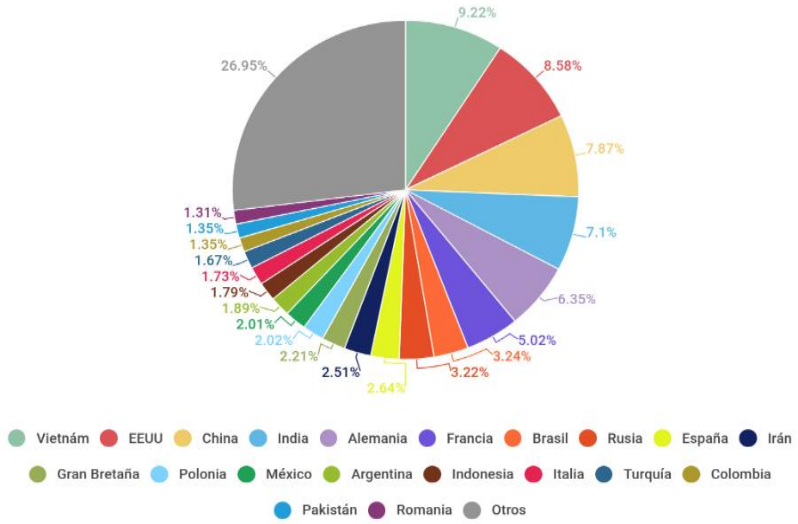
Según los resultados mostrados en la imagen 6. El primer trimestre de 2018, Vietnam (9,22%) se convirtió en el líder entre los países fuente de spam. En el segundo lugar por la cantidad de spam saliente, con una diferencia de sólo 0,64 p.p. están los Estados Unidos (8,55%). China, que con frecuencia lidera la estadística, bajó al tercer lugar (7,87%), y en la cuarta y quinta posición tenemos a India (7,10%) y Alemania (6,35%) respectivamente. Irán cierra la lista de los diez primeros países (2,51%) [9].

2.5.9.7. Países fuentes de spam y phishing

En esta imagen 7 que se muestra el análisis del primer trimestre de 2018 respecto las

afectaciones de correos maliciosos y phishing en diferentes países que usan correo electrónico y páginas web en las compañías y organizaciones

Imagen 7. Países fuentes de spam en el mundo, primer semestre de 2018



Fuente: Kaspersky [9].

En la Imagen 7 fuente estadística de Kaspersky, abordó los datos de secuencia de 21 de los países que presentan más incidentes y materializaciones de

2.5.9.8 . Estadísticas de engaño y phishing

En el primer trimestre de 2018, el sistema Antiphishing neutralizó 90.245.060 intentos de remitir al usuario a páginas de phishing. El porcentaje de usuarios únicos atacados fue del 9,6% del número total de usuarios de productos de Kaspersky Lab en el mundo.

2.5.9.9 . Geografía de los ataques de phishing en Latinoamérica y Europa

En el primer trimestre de 2018, Brasil, con el 19,07% (-1,72 p.p.) se convirtió en el país con mayor porcentaje de usuarios atacados por los phishers

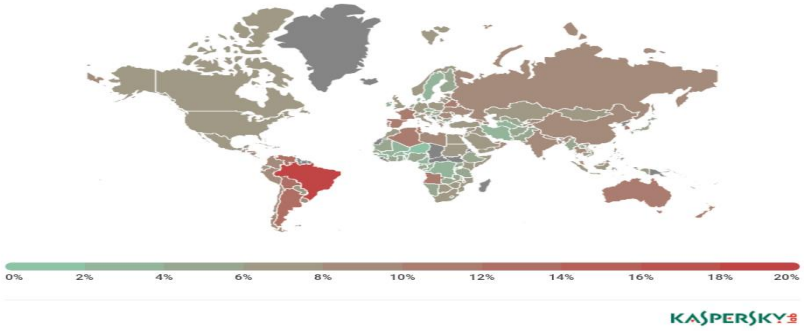
Tabla 6.Tabla de Geografía de los ataque phishing, primer semestre 2018 [9].

PAIS	**%**
Brasil	19,07
Argentina	13,30
Venezuela	12,90
Albania	12,56
Bolivia	12,32
Reunión	11,88
Bielorrusia	11,62
Georgia	11,56
Francia	11,40
Portugal	11,26

Fuente: https://securelist.lat/spam-and-phishing-in-q1-2018/86992/

En la tabla 6 se evidencia los porcentajes de spam y de phishing en diferentes paises que lideran con la mayor cantidad de ataques de ingenieria social segun los reportes de securelist deminova en conjunto con la marca de antivirus kaspersky.

Imagen 8. Tabla de geografía de los ataques de phishing primer semestre de 2018 [9].



Fuente: Fuente: T. S. y. M. V. N. Demidova, SECURELIST spam y phishing

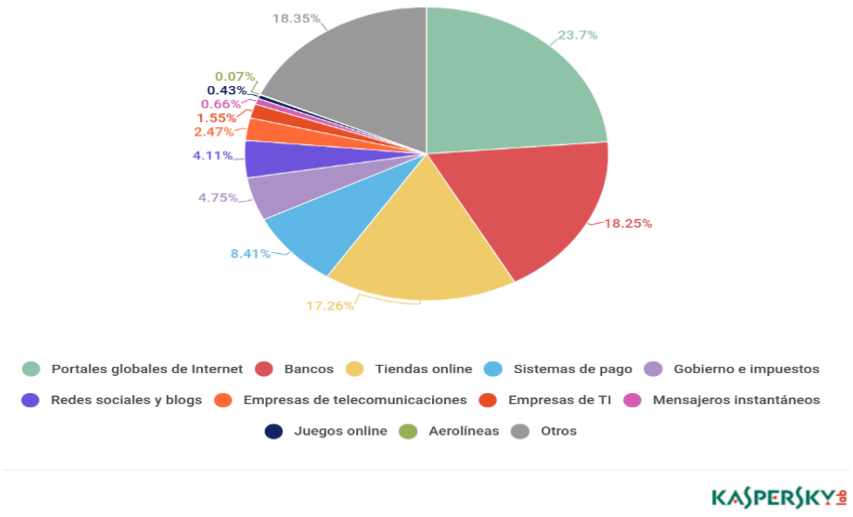
En la tabla 6 y la imagen 8 se presenta en el segundo lugar se ubicó Argentina (13,30%), y el tercer lugar fue ocupado por Venezuela (12,90%). En el cuarto y quinto lugar están Albania (12,56%) y Bolivia (12,32%) respectivamente.

2.5.9.9.1. Organizaciones atacadas por engaño o phishing

2.5.9.9.1 Phishers

La estadística de las categorías de las organizaciones atacadas por los phishers se basa en las detecciones de nuestro anti phishing en los equipos de los usuarios. Este componente detecta páginas con contenido phishing, que el usuario intentó visitar al seguir enlaces presentes en mensajes electrónicos o en Internet.

Imagen 9. Distribución de categoría de las organizaciones cuyos usuarios fueron afectados por phishing en el 2018



Fuente: T. S. y. M. V. N. Demidova, SECURELIST spam y phishing[9]

Carece de importancia de qué forma se haga el paso: sea como resultado de pulsar un enlace en un mensaje phishing como se muestra en la imagen 9, en un mensaje de una red social o debido a las acciones de un programa malicioso. Cuando el sistema de defensa reacciona, el usuario ve en el navegador un banner que le advierte sobre la posible amenaza. En el primer trimestre de 2018, la categoría, portales globales de Internet" volvió a ocupar el primer lugar y acaparó el 23,7% (-2,56 p.p.).

2.5.9.9.2 Ingeniería social en Colombia

Este informe de contextualización del centro policial del cibercrimen en Colombia dirigida por el Teniente Coronel Alex Uriel Duran Sants catalogando los principales flancos de tipos de ataques informáticos y evidencias investigadas en el ámbito Nacional , como fuente de implementación y modelo referencial de la Europol iocta 2018 agencia Europea de Cooperación policial de ciberdelincuencia. [19].

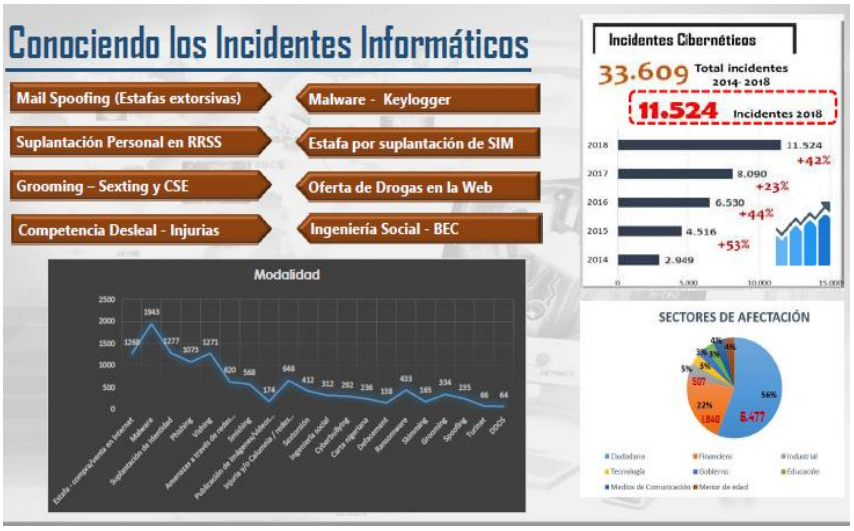
Imagen.10 Principales amenazas Colombia

Fuente: European Cybercrime Centro, Contexto de Cibercrimen en Colombia [25]

En Colombia se reconocen diferentes modos de operación de ataques de ciberseguridad enlazadas a análisis de Malware, se identifican las siguientes amenazas según lo observamos en esta imagen 10 Se puede conocer principales amenazas que recurren en el territorio nacional.

- Ramsonware
- Los ataques DDoS sector privado y publico
- Abuso infantil en la Web
- Fraude en medio de Pago
- Incremento de uso de criptomonedas
- Criptojacking
- Ingeniería Social
- Dark Web

Imagen 11. Incidentes informáticos en Colombia



Fuente: Centro Cibernético Policial,, 2017

Según el reporte de acuerdo con la imagen 11 en el 2017, el cibercriminal reportó un incremento 28.30% respecto al año anterior, consolidándose como uno de los principales retos en materia de lucha contra la criminalidad y cibercrimen en el mundo; los delitos informáticos han puesto en serios problemas a la parte física y virtual de diferentes entidades y organizaciones como lo muestra la figura 10 y mencionando los resultados [20].

Datos obtenidos fueron los siguientes:

- Estafa compra en internet 1200 reportes
- Malware 1943 reportes
- Suplantación de identidad 1277 reportes
- Phishing 1073 reportes
- Ransomware 433 reportes
- Ingeniería Social 312 reportes
- Skimming 165 reportes
- Turinet 66 reportes
- DDOS 64 reportes

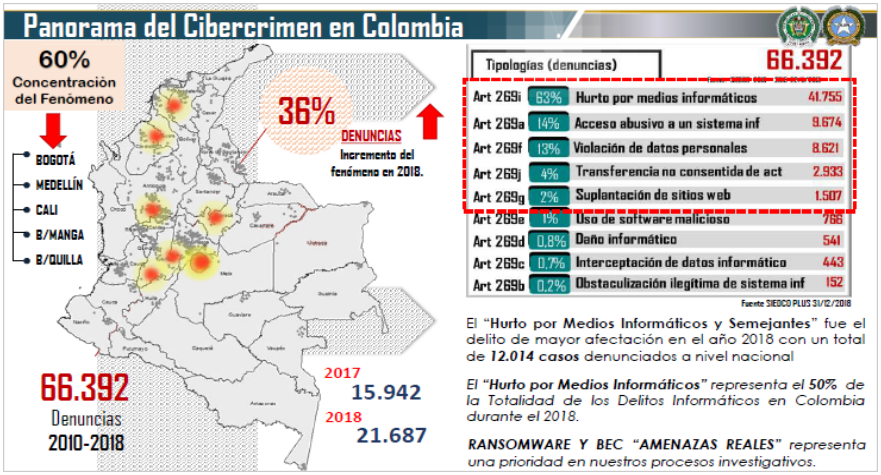
La venta de datos personales, la oferta inusitada de malware, la comercialización de productos ilegales como armas, estupefacientes, bienes hurtados, documentos fraudulentos, entre otros, se han visto favorecidos por el afianzamiento de las criptomonedas como medio de pago predilecto para el crimen, aunado al anonimato que ofrece la Internet profunda y las rentas criminales derivadas del auge de estas conductas [20].

"Ciberataques sofisticados de afectación global impactaron infraestructuras digitales críticas en el mundo, en Colombia 446 empresas reportaron haber sido víctimas"

2.5.5.9.3. Vishing de ingeniería social

Tráfico de datos financieros personales. Modalidad de estafa en la que los ciberdelincuentes aplican técnicas de ingeniería social vía telefónica, con el fin de tener acceso a información personal y financiera de sus víctimas para así lucrarse económicamente. Durante la vigencia se han recibido 1055 casos de phishing por cifras cercanas a los $2.132.000.000,00.

Imagen 12. Panorama de denuncias cibercriminal en Colombia



Fuente: Reporte Anual cibercriminal Policía nacional 2017-2018 [20]

En el histórico panorama de cibercriminal en Colombia se muestra en la imagen 12 las fechas comprendidas del 2010 hasta el 2018, se evidencio una cifra de hurto informático de 41.755, Acceso abusivo a un sistema Informático 9.674, Violación a datos personales de 8.621,

transferencias no consentidas de activos 2.933, suplantación de sitios web 1.507 son los datos más considerables para la concentración de los ataques. Con un total de 66.392 denuncias de ciberataques localizados en las ciudades de Bogotá, Medellín, Cali, Bucaramanga, Barranquilla se evidencia este fenómeno.

2.5.5.9.4. SML que es como funciona

En esta investigación se relaciona el marcado de confirmaciones SAML, por sus siglas son credenciales de seguridad sean compartidas por múltiples computadoras a través de una red, la autenticación determina como quieren ser y poder aceptar el tratamiento de datos, y la autorización determina si los usuarios tienen derecho acceder a los sistemas y contenido, SAML se utiliza para codificar la información y ayudar a los procesos de seguridad. [26]

3 METODOLOGÍA

Fase 1: Desarrollo

- En esta fase se realiza el diseño del ataque de vulnerabilidad de código QR
- Se genera el código QR en la herramienta gratuita QR code generator
- Se crea formulario en google form de Seguridad de la información enlazada a código QR
- Se diseña volante el cual es el medio de captura de los datos de quien haga la lectura del código QR, se almacena luego en suite de google form.
- Suplantación de página web de la universidad católica de Colombia para ataque controlado de ingeniería social.

Fase2: Implementación

- Se creó los códigos QR para fase 1 encuesta de seguridad de la información, fase 2 ataque controlado de ingeniería social, fase 3 evaluaciones de conocimientos después el ataque.
- Se realizó el phishing de la página oficial de la universidad católica de Colombia por medio de la herramienta Httrack Website Copie, y almacenada en código Html en ficheros exportables.
- Se realizó pruebas locales con la herramienta Xampp-control, contenido virtual de Apache, MySQL, con la suplantación del sitio web y dirigido a la captura de datos en google form.
- Monitoreo en tiempo real del número de escaneos de los códigos QR y versión de dispositivos
- Publicación del ataque en la web en el hosting 000webhost File, hosting web de hospedaje gratuito con cpanel, php, mySlq, desarrollo de botón tipo carnada y gif.
- Implementación de volantes publicitarios con el phishing del ataque controlado de ingeniería social para la captura de datos.
- Análisis de resultados de las encuestas y ataque controlado
- Se realiza retroalimentación y etapa de concientización de las mejores prácticas de identificación de sitios maliciosos, metodologías de seguridad de la información, a los cursos más afectados.
- **Fase 3: Documentación**

- Documentación de resultados de los datos obtenidos (Estadísticas y análisis)

- Artículo científico IEEE

3.5 INSTRUMENTOS O HERRAMIENTAS UTILIZADAS

Imagen 13. Captura de código Qr

Fuente: R. Menendez, «Comunidad Peru crack,» Hacker master

Para este ejercicio se requieren una serie de herramientas que se describe a continuación, teniendo en cuenta que parte de este ejercicio académico, es que a través de dispositivos móviles la población elegida escanee el código QR (Quick Response) como se muestra en la imagen 13 que estará impresos en unos volantes que se ubican en los laboratorios de sistemas de la sede el claustro y de aulas de clase de la Universidad Católica de Colombia.

Una vez realizada dicha acción se redijere automáticamente a una página web donde inicialmente acepta el tratamiento de datos, ley 1581:2012 y pasan a un formulario donde diligenciaran cierta información que será almacenada en una base de datos, paralelamente la página lee los datos del dispositivo (IP, MAC, Versión SO, Navegador y su respectiva versión), sin causar sospecha alguna de la persona que está navegando, esta información también se almacena en formulario de google form [27]

3.5.1. HERRAMIENTAS

- Generador código QR (Quick Response), herramienta QR code generator y proceso para el ejercicio académico

- Google form herramienta para encuestas y datos estadísticos
- Estación de trabajo para pruebas locales xampp controles v3 permite instalar el entorno MyLQL ,apache y Php para proyectos web.
- Servidor Host gratuito para almacenar la página web, hosting 000webhost File

3.5.2. POBLACIÓN Y MUESTRA

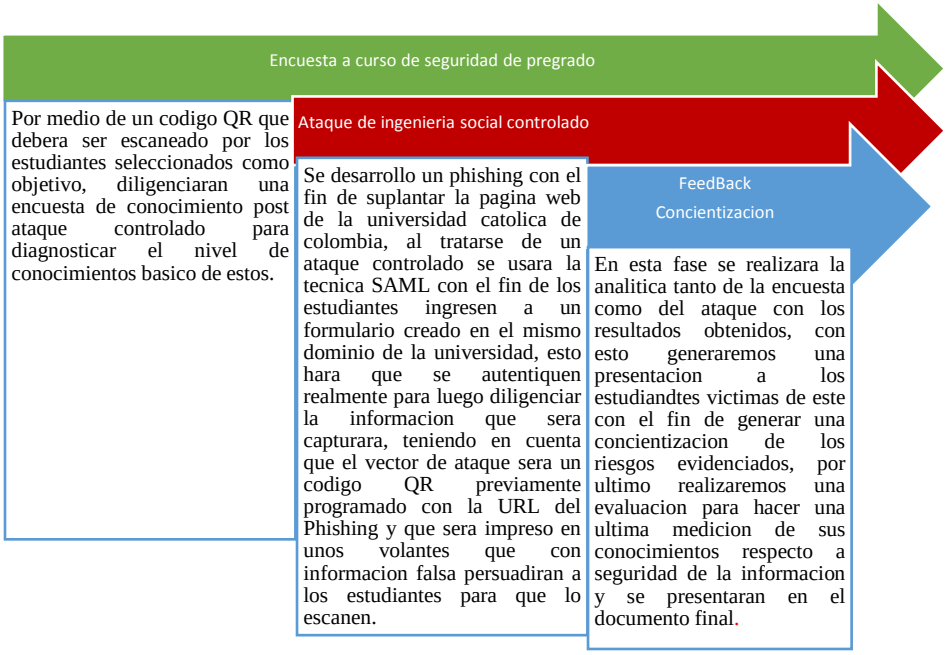
Para este ejercicio académico se seleccionó los siguientes cursos de ingeniería de sistemas como diseño de redes y servicios, informática social de sede el claustro de la Universidad Católica de Colombia claramente de cursos de pregrado. El público seleccionado cuenta con los medios según cifras del ministerio de las tic indican que el 77 % de los estudiantes de las universidades de Colombia tienen acceso a internet a través de sus dispositivos móviles, se puede garantizar que el público elegido en su mayoría contara con un dispositivo móvil y acceso a internet para poder llevar acabo el ejercicio académico. [25]. La selección de esta población se debió a temas de cumplimiento ya que en el país actualmente rige la ley 1581 protección de datos personales y 1273 delitos informáticos (véase en el ANEXOS 1), teniendo en cuenta el ejercicio busca hacerlo en un ambiente controlado y autorizado.

3.6 REALIZACIÓN Y METODOLOGÍA DE ATAQUE CONTROLADO

Se presenta el desarrollo de la intervención de la metodológica realizada; la implementación del ataque controlado de ingeniería social por medio de phishing en la universidad católica de Colombia, a continuación, se presenta y explica de manera detallada como se realizó cada una de las fases de la implementación: Planeación, diseño, codificación y programación y respectivas pruebas.

3.7 PLANEACIÓN PARA LA EJECUCIÓN POR FASES DEL PROYECTO

Imagen 14. Planeación por fases de ejecución

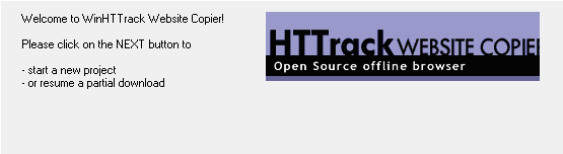


Fuente: propia

3.8 DISEÑO DEL PHISHING Y REALIZACIÓN

Httrack es un efectivo navegador gratuito (GPL,software libre) que permite realizar la descarga de un sitio de la web de internet a un directorio local ,creando directorios ,obtenidos en html , y una imagen de los archivos del servidor original en la computadora una pagina completa reflejada. [28]

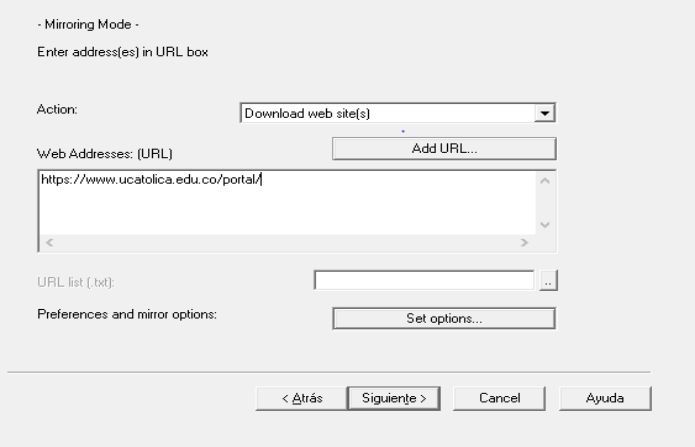
Imagen 15 .HTTrack clonado de páginas web



Fuente: https://www.httrack.com/

Como se observa en la imagen 15 a continuación httrack realiza una copia el sitio web con la dirección de la url, en este caso de el sitio oficial de la universidad catolica de colombia y se procede a descargar la plataforma enforma de ficheros. [28]

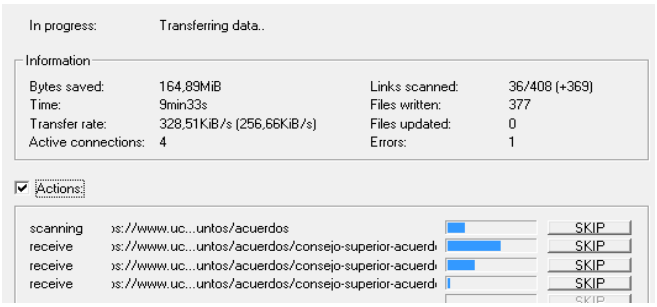
Imagen 16. Proceso de escaneo y copia de sitio web



Fuente: https://www.httrack.com/

La herramieta da comienzo y luegar a el escaner en todo el portal web hasta capturar finalmente el codigo html, imágenes y emula el dominio , realiza un espejo para poderlo proyectar de forma local o en un servidor .

Imagen 17. Escaneo y guardar ficheros Http

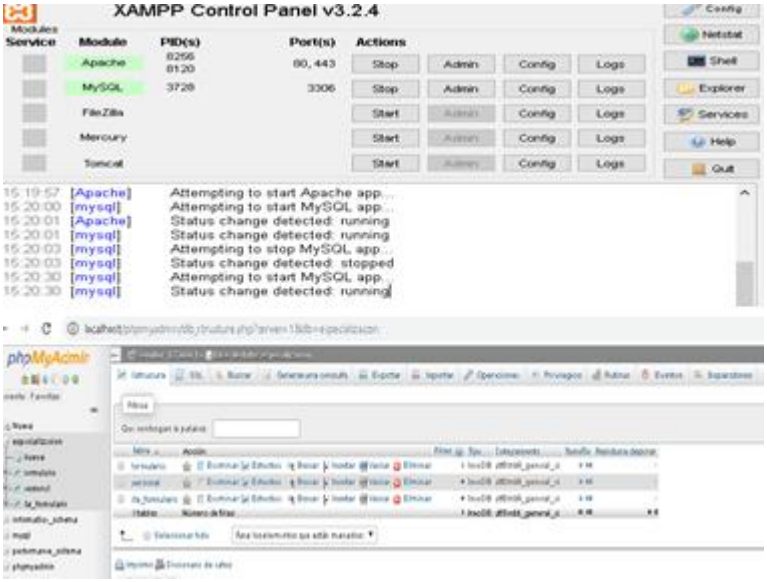


Fuente: https://www.httrack.com/

A continuación, como se muestra en la imagen 17 se evidencia la clonación y escaneo de la página web de la universidad católica de Colombia que finalmente serán alojados en ficheros de datos Http.

Pruebas Locales: Despues de sustraer la información y clonar la pagina web oficial de la universidad catolica de colombia se procede a trabajar con la herramientica xampp controles v3 es una herramienta practica que permite instalar el entorno MyLQL ,apache y Php para empezar proyectos web o considerar una aplicación localmente . [29]

Imagen 18. Servidor local XAPP control



Fuente: https://www.apachefriends.org/es/index.html

En la imagen18 se observa la carga apache y MySQL localmente para probar la publicación de la página web clonada que será el phishing del ataque controlado modo de pruebas, se crea los campos y la volumetría de datos para la captura de datos relacionados con el ejercicio académico y guardado en el servidor local, los datos se capturan finalmente en google form.

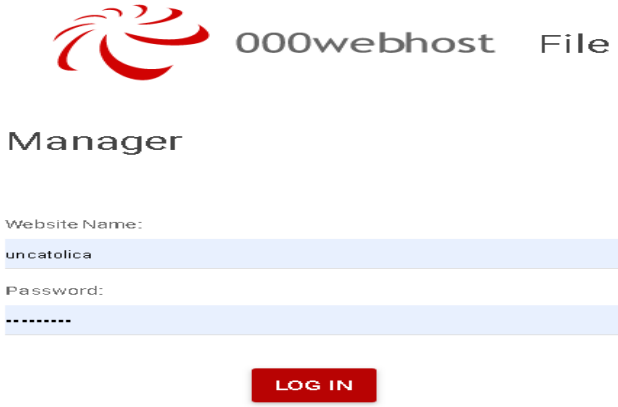
Imagen 19. Resultado de suplantación de página web universidad católica de Colombia, en servidor local

Fuente: Autores

Como se muestra en esta imagen 19 se refleja la página de la universidad católica de Colombia clonada en el servidor local de pruebas, se desarrolló un botón de participar aquí que dirige a un formulario de google form para inscripción de datos de la víctima, además de la aceptación de política de tratamiento de datos ley 1581 y decreto 1377.

Puesta en Producción: Después de realizar las pruebas correspondientes en el servidor local, se procede a realizar la publicación en el hosting 000webhost File, hosting web de hospedaje gratuito con cpanel, php, mySlq para publicaciones en la web.

Imagen 20. Servidor web 000webhost file



Fuente: Autores

Luego de realizar la suplantación de la página web con la herramienta tecnológica Httrack ,se realiza una creación de cuenta en 00webhost , es un servidor web de manera gratuita como se

muestra a continuación en la imagen 20,se realiza un wordpress sitio de html y posibilidades de funcionamiento fluido .

Imagen 21. Publicación de archivos en hosting

Fuente: Autores

En la imagen 21 se muestra el cargue de los archivos en el site public_html para la publicación de la página web con los resultados requeridos del phishing con el siguiente link: https://uncatolica.000webhostapp.com/ , como resultado la interfaz de la universidad católica de Colombia que a simple vista se ve auténtica. En la siguiente imagen observa el resultado:

Imagen 22. Suplantación de página web con phishing

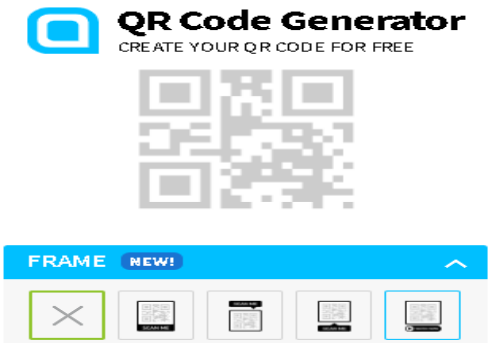
Fuente: Autores

En la imagen 22 se observa la implementación de la página web en la modalidad de phishing, con los gráficos y logos de la universidad y el botón de persuadir las víctimas, y participar por una beca que posteriormente se realiza la captura de datos y análisis de resultados .

3.9 DISEÑO DE CÓDIGO QR

La aplicación qr code generator online se utiliza para la construcción de códigos QR programando la URL de cada uno de los 3 frentes dispuestos en google form.

Imagen 23. Código QR captura formulario



Fuente: Autores

Con la herramienta code generator como se muestra en la imagen 23, se puede crear, personalizar y analizar los códigos qr el servicio es online y gratuito por cierto tiempo, también se tiene la opción de analizar resultados estadísticos de lo escaneado de la creación.

3.10 ENCUESTA A OBJETIVO

Se realiza la programación del código qr con la URL de la encuesta de diagnóstico que contiene preguntas de conocimientos básicos en seguridad de la información alojada en formato de google form.

Imagen 24. Código QR, encuesta de seguridad de la información

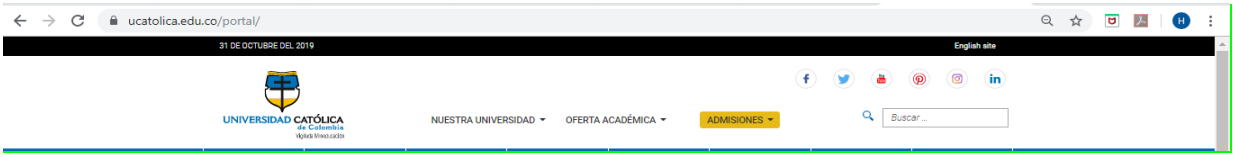
Fuente: Autores

Esta imagen 24 se muestra el código QR que se debe escanear para acceder a la encuesta de forma rápida y sencilla.

3.11 ATAQUE CONTROLADO

Se crea un phising simulando la página de la universidad católica de Colombia: Página original https://www.ucatolica.edu.co/portal/

Imagen 25. Página web universidad Catolica de Colombia original

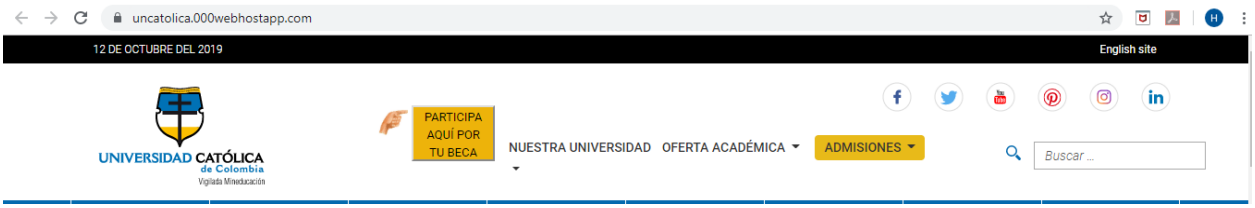


Fuente: https://www.ucatolica.edu.co/portal/

En la imagen 25 se observa la página web institucional de la universidad católica de Colombia original, luego se puede identificar las diferencias respecto a la página web phishing que se observa a continuación.

- Phishing https://uncatolica.000webhostapp.com/

Imagen 26. Página web Phishing



Fuente: Autores

En paralelo se diseñan e imprimen unos volantes alusivos imagen 27 a la universidad católica de Colombia, persuadiendo a los alumnos a que escaneen el código qr impreso allí para participar por becas en el exterior.

Imagen 27. Volantes alusivos para persuadir escanear el código Qr

Fuente: Autores

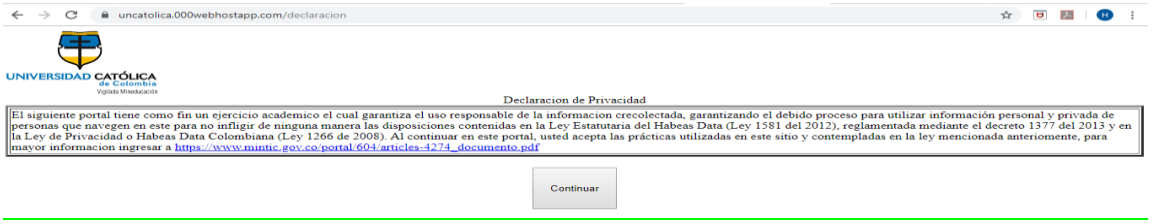
En la imagen 27 Una vez escaneen el código llegan al sitio suplantado en ingresan al botón “PARTICIPA AQUI POR TU BECA” es dirigido a una captura de datos básicos que se encuentra alojada en suite google forms con dominio de la universidad católica de Colombia.

Imagen 28. Phishing de página web y botón persuasivo

Fuente: Autores.

Al hacer clic en el botón amarillo como se ve en la imagen 28 este redirige a otra url donde se indica las implicaciones del marco legal ley 1581 del 2012 de protección de datos personales y que acepten el tratamiento de estos para realizar el ataque controlado y materialización.

Imagen 29. Aceptación de ley de protección de datos 1581 2012



Fuente: Autores

Una vez hacen clic en el botón continuar como se muestra en la imagen 29 , los redirige a un formulario donde se controla el ataque usando la técnica Security SAML (Assertion Markup Language), dando aún más confianza al objetivo para cumplir la finalidad del ataque y asegurando que a este sitio solo ingresen alumnos de la universidad católica de Colombia, se aclara que cuando los alumnos se autentican, están ingresando al dominio real de la universidad ya que el formulario se creó en este, por ende se garantiza que dicha información no es capturadas, solo se obtendrá la data que diligencien en el formulario mencionado.

Imagen 30. Participación en el formulario de datos de phishing

Fuente: Autores

En la imagen 30 se muestra el formulario que los estudiantes tienen que diligenciar, para posteriormente guardar solo las respuestas de las preguntas, luego se procede a analizar los datos que arrojaron las estadísticas.

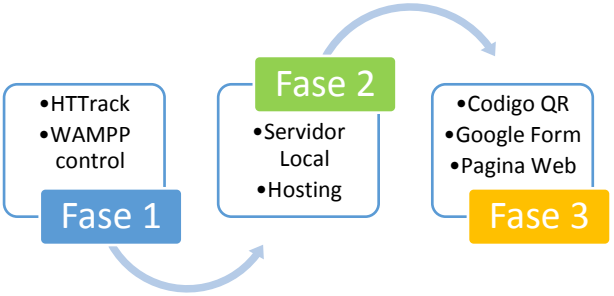
3.12 EVALUACIÓN Y CONCIENTIZACIÓN

Al curso que más se afectó con el ataque de ingeniería social se realiza un feedback de lo sucedido desde la primera fase hasta la finalización del ataque, dando una recomendación para mejorar sus conocimientos y aplicaciones de mejores prácticas de seguridad de la información.

3.13 CODIFICACIÓN Y PROGRAMACIÓN

En la realización de la presente investigación se tuvo encuenta el desarrollo de una pagina web , la constitucion de un servidor local de pruebas, la utilización de un clonador de pagina web y la puesta en producción en un hosting .

Imagen 31. Fases de la realización de ataque de ingeniería social por medio de códigos Qr



Fuente: Autores

Deacuerdo a el diagrama de procesos como se muestra en la imagen 31 se explica cada una de las herramientas utilizadas para el ataque controlado de ingenieria social a unos cursos del programa de ingenieria de sistemas de la universidad catolica de colombia :

4.81 Resultados Encuesta de Seguridad de la información

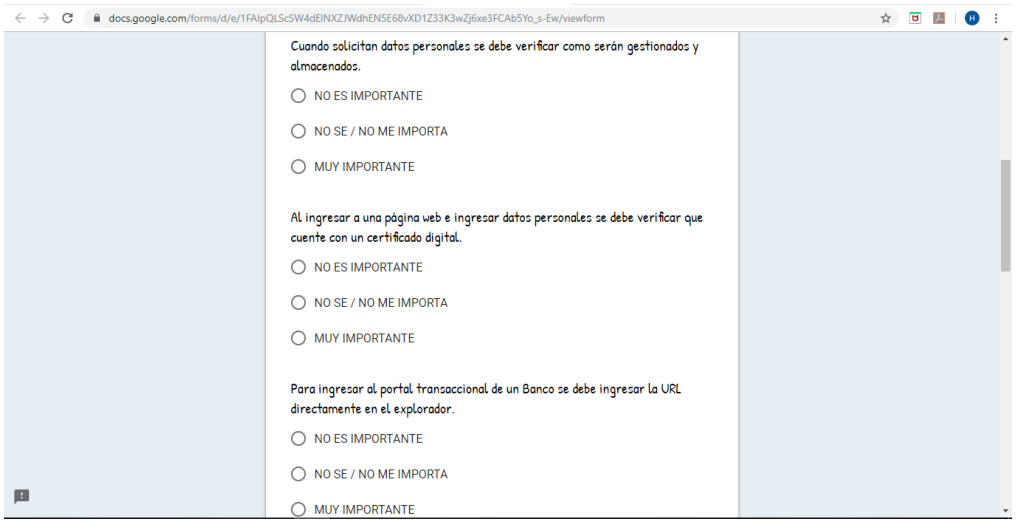
Se elaboró una encuestas a través de Google Forms en el dominio de la Universidad Católica de Colombia con el fin de cuantificar el conocimiento del objetivo (alumnos de Informática Social y Diseño de redes y servicios convergentes) en aspectos básicos de seguridad de la información, previo al ataque controlado se ingeniería social. Se puede verificar el contenido de la encuesta en el (Anexo 4). A continuación, se revela las preguntas realizadas y los resultados.

Imagen 32. Encuesta de seguridad de la información

Fuente: Autores

De acuerdo con la imagen 32 esta se establece la pregunta diagnóstica de vital importancia para la investigación si es transcendental la verificación del origen de los correos.

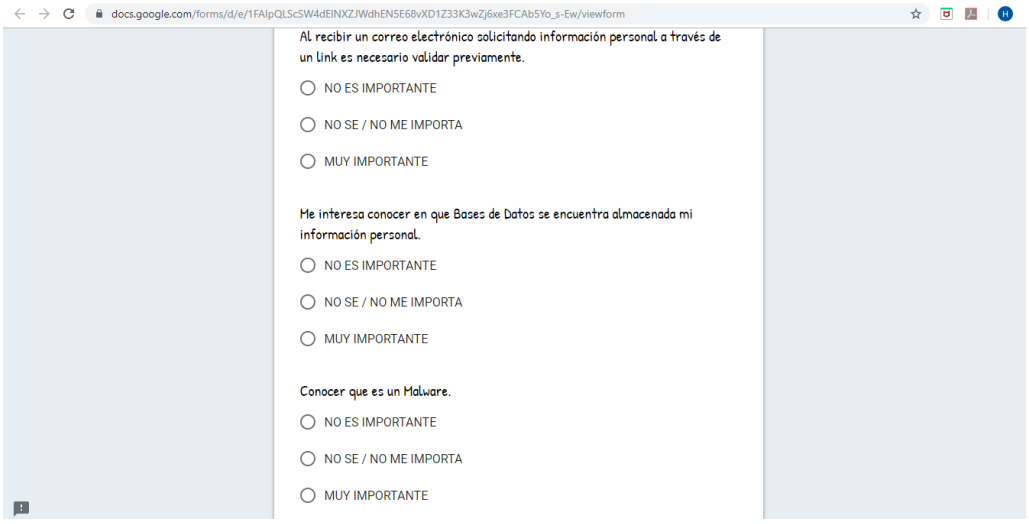
Imagen 33. Encuesta de seguridad de la información pregunta



Fuente: Autores

Estas preguntas son orientadas con el fin de conocer la verificación de los datos y su almacenamiento, conocimiento en verificación de certificado digital como se observa en la imagen 33, y conocimientos en hacer ingresos a portales transaccionales.

Imagen 34. Encuesta de seguridad de la información preguntas

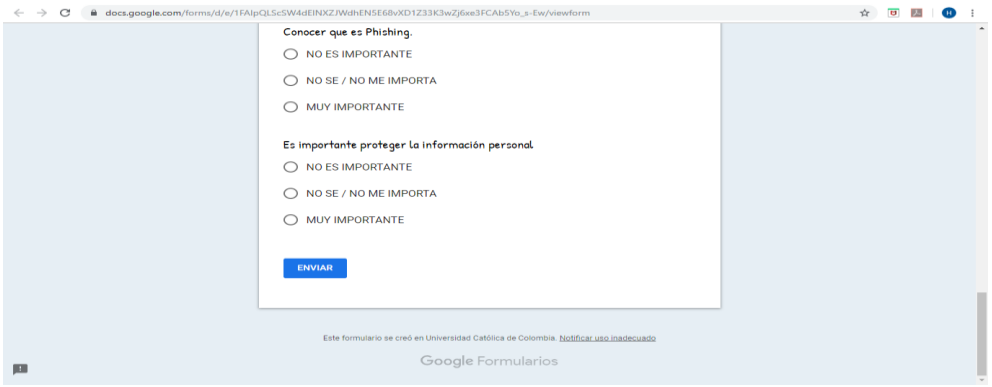


Fuente: Autores

Las preguntas miden el grado manejo de información y políticas de tratamiento de datos según la

ley 1851 como se observa en la imagen 34, enfocando el análisis de la validación y fuentes de almacenamiento de la información.

Imagen 35. Encuesta de seguridad de la información preguntas



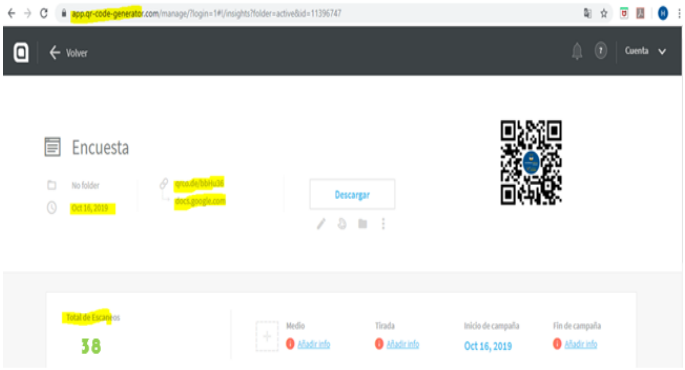
Fuente: Autores

De acuerdo con la figura imagen 35 se enfoca a las preguntas que impactan directamente la investigación de ataque controlado de ingeniería social por medio de phishing como vector de ataque aplicando ingeniería social, además de la vital importancia del tratamiento de datos personales.

4.82 Monitoreo de Códigos QR

Los códigos QR tienen gran funcionalidad para registro de respuesta rápida y dirección a páginas web pero también su base de programación permite monitorear resultados en tiempo real como se muestra a continuación.

Imagen 36. Resultados de encuesta de código Qr



Fuente: Autores

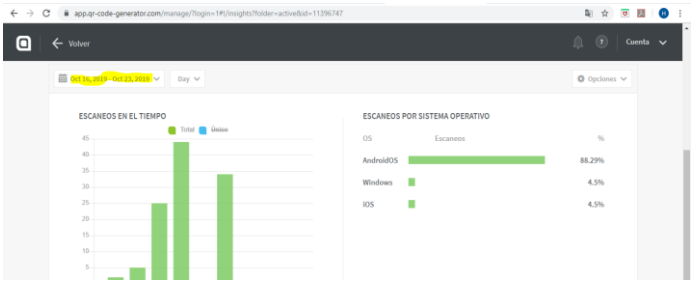
En la imagen 36 se observa los resultados del escaneo del código qr con sus respectivas fechas de inicio y fin de las capturas y de campaña del proyecto. Para el total de escaneos como se muestra en la tabla 7, (38) el 89.5% de los estudiantes diligenciaron el formulario con los siguientes resultados.

Tabla 7. Total de escaneos 1

Escaneos	38	
Formularios Diligenciaos	34	89.5%

Fuente: Autores

Imagen 37. Respuestas de la plataforma de código qr



Fuente: Autores

En la imagen 37 se evidencia la encuesta realizada, teniendo en cuenta como resultado lo siguiente. Desde la siguiente URL se puede hacer seguimiento de la fecha de creación del código QR, el número de escaneos por día, escaneos totales y sistema operativo de los dispositivos que han escaneado el código, teniendo el siguiente resultado.

Imagen 38. Respuestas de la plataforma en google form

Fuente: Autores

Se obtienen de dos fuentes, la herramienta Online QR y de Google Forms con los siguientes resultados, como se observa en la imagen 38.

Tabla 8. Resultados de Escaneos QR 1

Curso	Total Alumnos	Total de Escaneos	Respondieron Encuesta
Informática Social	25	25	21
Diseño de redes y servicios convergentes	13	13	13

Fuente: Autores

Como se observa en la tabla 8 se identifican los cursos que fueron parte del ataque controlado de ingeniería social por vector de ataque de códigos qr mediante la modalidad de phishing de 25 alumnos que escanearon el código en informática social 21 personas llegaron a realizar todo el ejercicio hasta responder la encuesta y de diseño de redes si un total de alumnos de 13 y absolutamente todos llegaron a la totalidad de la actividad hasta responder la encuesta .

Los resultados son los siguientes:

Imagen 39. Encuesta de seguridad de la información

Fuente: Autores

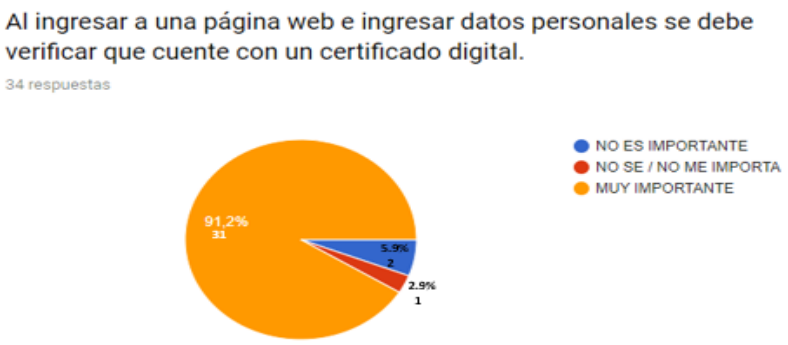
Se evidencia en la imagen 39 los resultados que el 97.1% verifican el origen de los correos y solo un 2.9 % no sabe y le importa entendiendo que es aislada la respuesta.

Imagen 40. Resultados encuesta 1

Fuente: Autores

Es importante saber cómo se gestionan y almacenan los datos personales y el 94.1% está de acuerdo con la pregunta y solo un 5.9 % está en desacuerdo como se observa en la imagen 40, no contemplan la posibilidad de que el robo de datos presenta un riesgo para las personas y entidades corporativas.

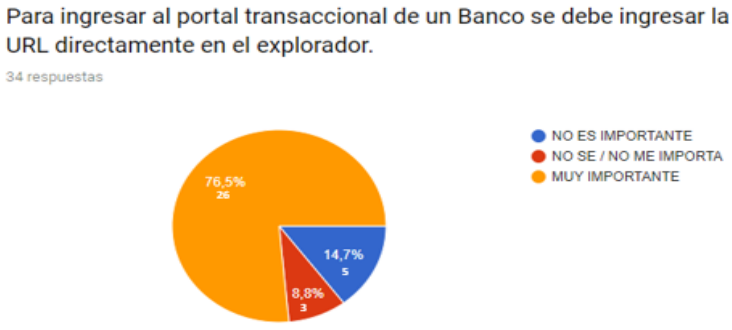
Imagen 41. Información certificado digital



Fuente: Autores

El certificado digital es el documento que hace posible la identificación de las personas en internet y presenta seguridad a la hora de trámites administrativos a través de portales web, los resultados como se observa en la imagen 41, obtenidos 91.2 % manifiesta que es muy importante y solo el 5.9 % afirma que no es importante 2.9 % no sabe y no le importa saber.

Imagen 42. Encuesta pregunta de portal transaccional



Fuente: Autores

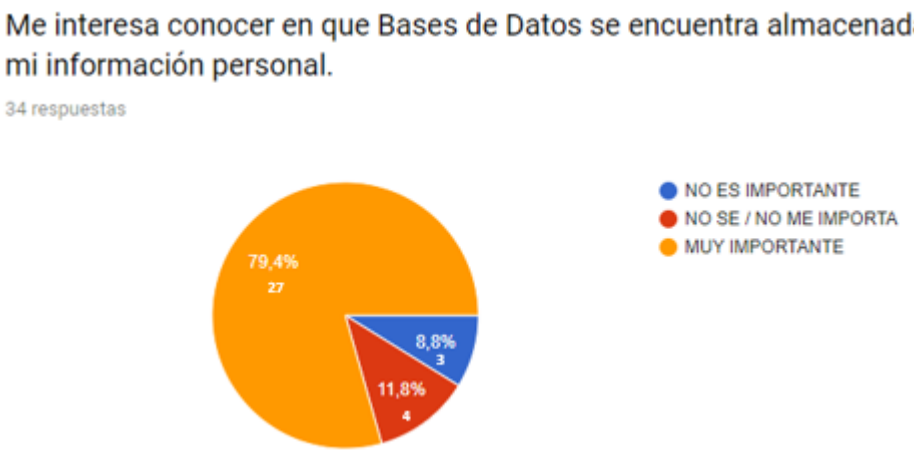
En la imagen 42 el resultado impacta directamente en nuestra investigación porque el 76.5% identifica e ingresa directamente la URL en el explorador para hacer transacciones bancarias y el 14.7% considera que no es importante y pone en riesgo datos personales y posibilidad de ser hurtadas sus cuentas bancarias por medio del phishing y aún más preocupante el 8.8% no le importa en lo más mínimo.

Imagen 43. Encuesta validación de link

Fuente: Autores

En esta pregunta imagen 43 se evidencia que es muy importante la verificación del link en un correo electrónico recibido con un 97.1% y solo el 2.9 % no considera importante.

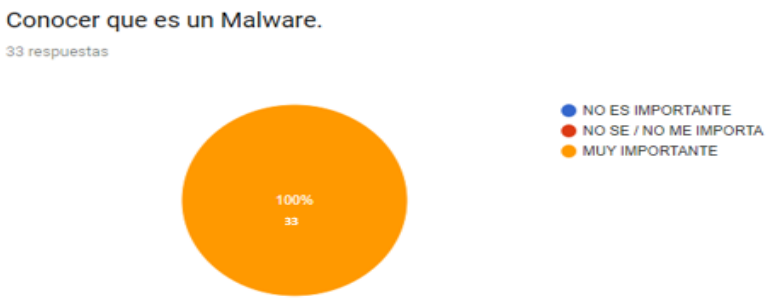
Imagen 44. Encuesta de seguridad base de datos



Fuente: Autores

En esta pregunta como se muestra en la imagen 44 los resultados fueron 79.4 % muy importante saber en qué base de datos es almacenada la información, no importa un 11.8% y un 8.8% que hace pensar que pueden mejorar en estos aspectos.

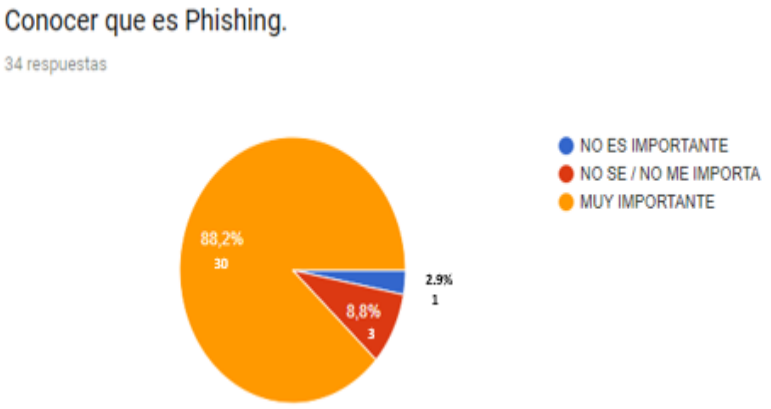
Imagen 45. Encuesta, información de malware



Fuente: Autores

En esta respuesta el 100% afirma conocer que es un malware como se muestra la imagen 45 es muy bueno para fines de seguridad de la información.

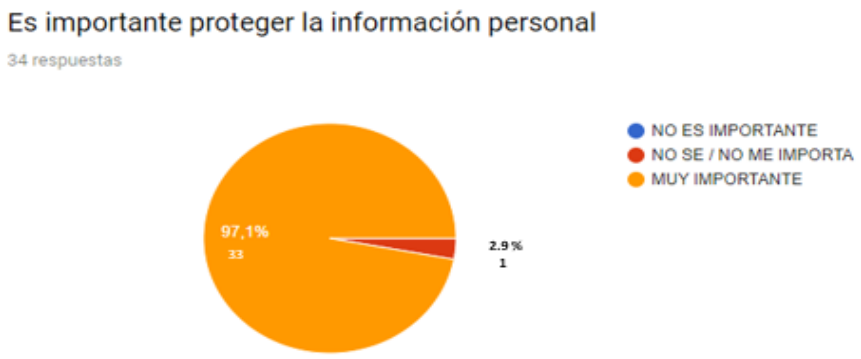
Imagen 46. Encuesta de seguridad de información Phishing



Fuente: Autores

Esta respuesta es fundamental para el estudio e investigación como se muestra en la imagen 46, para contrastar con el ataque controlado de ingeniería social un 88.2 % considera muy importante saber de la técnica de suplantación, un 8.8% considera que no es importante, y finalmente un 2.9 % considera que no es importante.

Imagen 47. Encuesta proteger información personal



Fuente: Autores

Se puede evidenciar en la imagen 47 el nivel de conocimiento básico y de concientización sobre la seguridad de los datos personales y seguridad de la información está en un nivel bueno, estos resultados se contrasta con el ataque controlado de ingeniería social.

Tabla .9 Tendencia de datos 1

Tendencia %
Excelente (90-100)
Buena (70-89)
regular (50-69)
Mala (0-49)

Fuente: Autores

En la tabla 9 se observa las calificaciones y rangos de clasificación para las respuestas de la encuesta, por consiguiente es el punto de partida para el análisis de la información recolectada.

Tabla 10. Respuestas y porcentajes 1

Porcentaje positivo	Porcentaje	Tendencia
respuesta 1	97.10%	Excelente
respuesta 2	94.10%	Excelente
respuesta 3	91.20%	Excelente
respuesta 4	76.50%	Buena
respuesta 5	97.10%	Excelente
respuesta 6	79.40%	Buena
respuesta 7	100%	Excelente
respuesta 8	88.20%	Buena
respuesta 9	97.10%	Excelente

Fuente: Autores

Se evidencio en la tabla 10 el nivel de conocimiento de los alumnos encuestados respecto a seguridad de la información está en un nivel Excelente de acuerdo con la siguiente tendencia, estos resultados se contrasta con el ataque controlado de ingeniería social.

3.14 Ataque controlado y resultados

Se desarrolló un ataque controlado de ingeniería social usando un código qr, impreso en un volante, como vector de este, con el comentario "CONVOCATORIA A ESTUDIANTES DE INGENIERIA PARA APLICAR A BECAS EN EL EXTERIOR" que redirige a los estudiantes a un phishing que simula el home de la página web de la universidad católica de Colombia, persuadiéndolos hacer clic en un botón que dice "PARTICIPE AQUÍ POR SU BECA" este los redirige a un link donde se les indica acerca de la ley 1581 del 2012 de protección de datos personales y el tratamiento de estos; Una vez aceptan las condiciones, se redirigen a un formulario creado en el dominio de la universidad católica de Colombia teniendo en cuenta la técnica de SAML ya que se trata de un ataque controlado, allí diligenciaron su datos completando el objetivo final.

Imagen 48. Volante alusivo o carnada

Fuente: Autores

De acuerdo con la imagen 48 se observa el volante que se diseñó para hacer efectivo el phishing con su respectivo código QR como vector de ataque, además de la labor de ingeniería social y persuasión

Imagen.49 Suplantación de página web con Phishing

Fuente: Autores

La imagen 50 nos muestra el resultado de la suplantación de la página web y se un botón tipo carnada que dice ‘PARTICIPA AQUÍ POR TU BECA’ luego se es dirigido a identificar y aceptar el tratamiento de datos personales ley 1581 del 2012.

Imagen 50. Captura de datos en google forms

Fuente: Autores

Como se puede evidenciar en la imagen 50, la información que se solicitó no fue muy intrusiva ya que solo se pretende demostrar que las personas que diligencian el formulario lo diligencia en su totalidad sin importar que tipo de información se solicita.

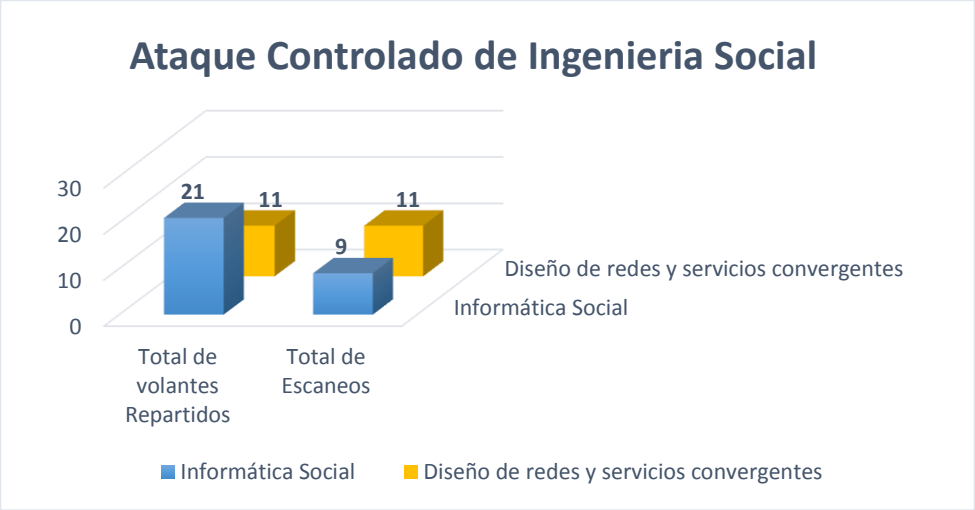
Resultados: El ataque se lanzó sobre los alumnos de los cursos mencionados en el alcance del proyecto:

- Informática Social
- Diseño de redes y servicios convergentes

Es importante tener en cuenta que son estudiantes que actualmente cursan de sexto a decimo semestres, y los resultados de la una encuesta respecto conocimientos en seguridad de la información que se realizó previamente.

Se entregaron un total de 34 volantes, 21 en el curso de Informática Social y 11 en el de Diseño de redes y servicios convergentes, obteniendo los siguientes resultados.

Imagen 51. Grafica Ataque controlado QR 1

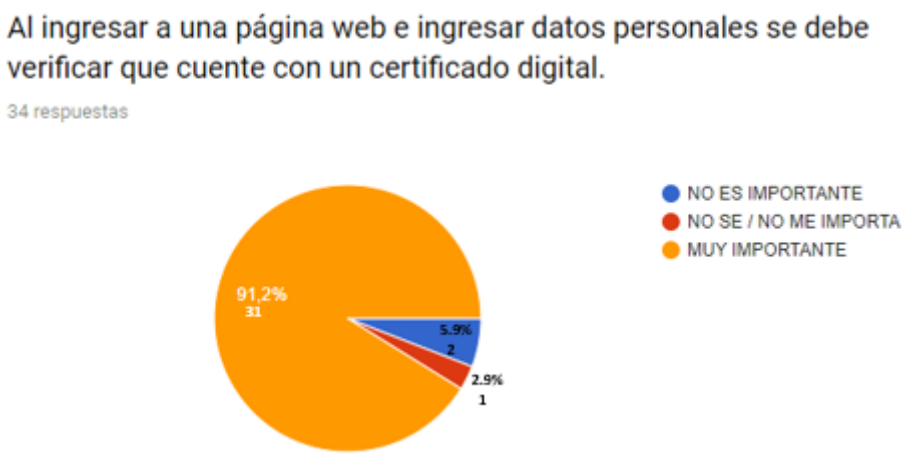


Fuente: Autores

Teniendo en cuenta estos resultados y contrastándolos con los resultados de la encuesta (preguntas puntuales) se llega a las siguientes conclusiones.

Se evidencio que en el curso de diseño de redes y servicios convergentes del total de volantes repartidos el 100% fueron escaneados y diligenciaron la información que se los solicito, respecto al curso de informática social del total de volantes repartidos el 42.9% fueron escaneados y diligenciaron la información que se solicitó, por ende del total de volantes repartidos en los dos cursos el 62.5% de los alumnos escanearon el código y diligenciaron la información que se los solicito, por ende se llega a las siguientes resultados :

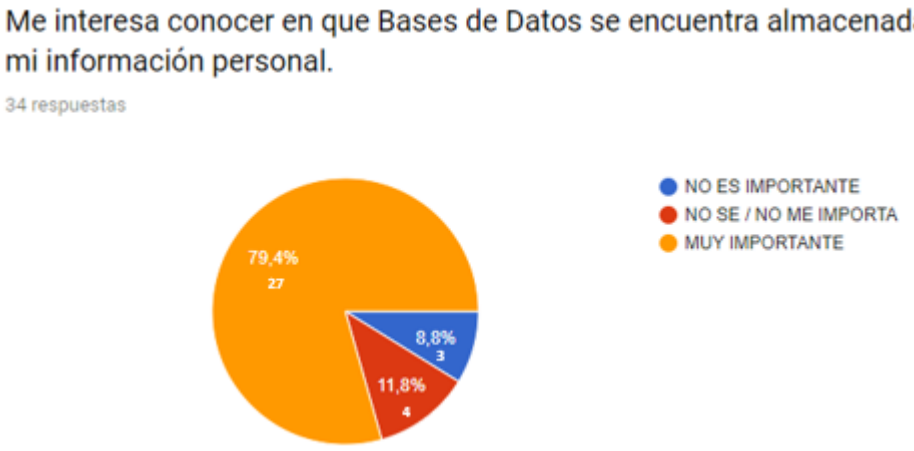
Imagen 52. Datos personales y certificad digital



Fuente: Autores

El 92% de los encuestados indicaron que es importante validar los certificados digitales como se muestra en la imagen 52 de análisis de las páginas web, pero como se evidencia en el ataque el 62.5% no lo tuvieron en cuenta.

Imagen 53. Interés en información en BD

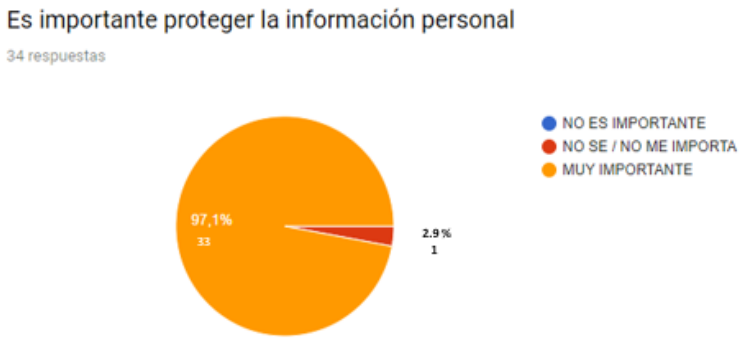


Fuente: Autores

En la imagen 53 se evidencia que 79.4% encuestados indicaron que les interesa saber en dónde

se encuentran almacenada toda la información y datos personales, pero el análisis se enfoca que en el ataque controlado se reportó la incidencia 62% no tuvieron en cuenta este tema.

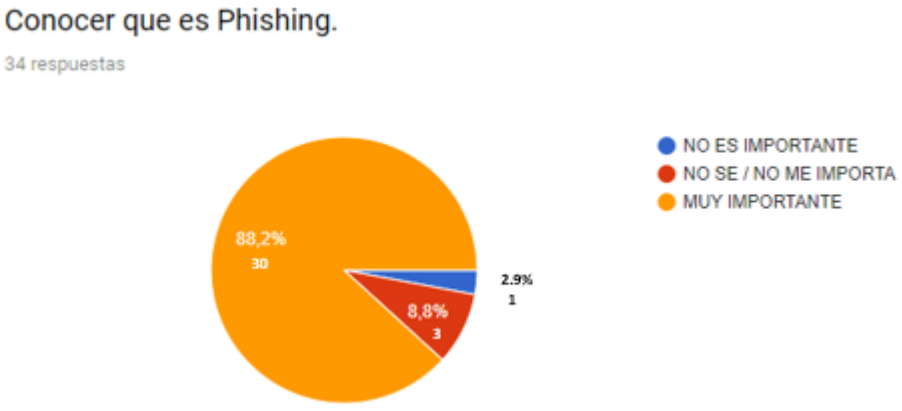
Imagen 54. Interés información personal



Fuente: Autores

Como se observa en la imagen 54 el 97.1% de los encuestados indicaron que es importante proteger su información personal, pero como se evidencia en el ataque el 62.5% no lo tuvieron en cuenta.

Imagen 55. Resultados de conocimientos de Phishing



Fuente: Autores

Como se observa en la imagen 55 el 88.2% de los encuestados indicaron que es importante conocer que es un phishing, pero como se evidencia en el ataque el 62.5% cayeron en este.

El análisis de las distintas técnica actuales y de acuerdo a su características no basamos en una de ellas, usando un código QR como vector de este, con unos resultados donde podemos destacar que se realizó en 3 fases descritas de la siguiente manera:

- Fase I – (Encuesta): Se escaneo el código que redirigía a la encuesta en 38 ocasiones donde 34 alumnos contestaron la encuesta, un porcentaje del 89.5% de la población elegida como objetivo del ataque.
- Fase I – (Encuesta): del curso de Informática Social, 25 alumnos escanearon el código qr y 21 diligenciaron la encuesta para un total de 84% de la población de este curso.
- Fase I – (Encuesta): del curso de Diseño de redes y servicios convergentes, 13 alumnos escanearon el código qr y 13 diligenciaron la encuesta para un total de 100% de la población de este curso.
- Fase I – (Encuesta): dentro de la tendencia respecto al conocimiento básico de los alumnos referentes al tema de seguridad de la información y protección de los datos personales, las respuestas está en un nivel Excelente.
- Fase II – (Ataque Controlado): Se repartió un total de 34 volantes, 21 en el curso de Informática Social y 11 en el de Diseño de redes y servicios convergentes.
- Fase II – (Ataque Controlado): Se evidencio que los alumnos de diseño de redes y servicios convergentes del total de volantes repartidos el 100% fueron escaneados y diligenciaron la información que se los solicito.
- Fase II – (Ataque Controlado): Respecto a los alumnos de informática social, del total de volantes repartidos, el 42.9% fueron escaneados y diligenciaron la información que se los solicito.
- Fase II – (Ataque Controlado): Del total de volantes repartidos en los dos cursos, el 62.5% de los alumnos escanearon el código y diligenciaron la información que se los solicito.

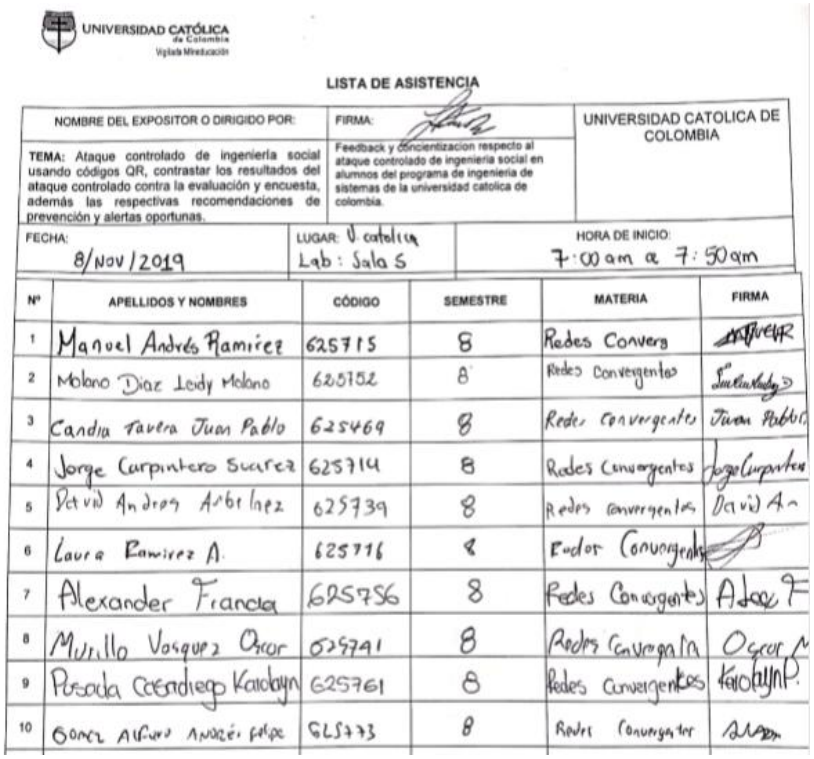
Respecto al contraste con los resultados obtenidos en la Fase I se concluye lo siguiente:

- Fase I vs Fase II: El 92% de los encuestados indicaron que es importante validar los certificados digitales, pero como se evidencia en el ataque el 62.5% no lo tuvieron en cuenta.
- Fase I vs Fase II: El 79.4% de los encuestados indicaron que les interesa saber en qué base de datos se encuentran almacenada su información personales, en el análisis del ataque controlado el 62% no tuvieron en cuenta dicho tema.
- Fase I vs Fase II: El 97.1% de los encuestados indicaron que es importante proteger su información personal, pero como se evidencia en el ataque el 62.5% no lo tuvieron en cuenta.
- Fase I vs Fase II: El 97.1% de los encuestados indicaron que es importante proteger su información personal, pero como se evidencia en el ataque el 62.5% no lo tuvieron en cuenta.

3.15 Concientización

En esta Fase II feedback y Concientización; Se seleccionó el curso que más fue impactado por el ataque y se realizó un feedback donde se les indico como se planeó el ataque, y como estos cayeron en él, se hicieron las respectivas recomendaciones y se diligenció un formato donde se evidencia la participación de dicho grupo.

Imagen 56 . Lista de charla de concientización y mejores practicas



UNIVERSIDAD CATÓLICA de Colombia
Vigilada Mineducación

LISTA DE ASISTENCIA

NOMBRE DEL EXPOSITOR O DIRIGIDO POR:	FIRMA:	UNIVERSIDAD CATOLICA DE COLOMBIA
TEMA: Ataque controlado de ingeniería social usando códigos QR, contrastar los resultados del ataque controlado contra la evaluación y encuesta, además las respectivas recomendaciones de prevención y alertas oportunas.	Feedback y concientizacion respecto al ataque controlado de ingeniería social en alumnos del programa de ingeniería de sistemas de la universidad catolica de colombia.	
FECHA: 8/NOV/2019	LUGAR: U. catolica Lab: Sala S	HORA DE INICIO: 7:00 am a 7:50 am

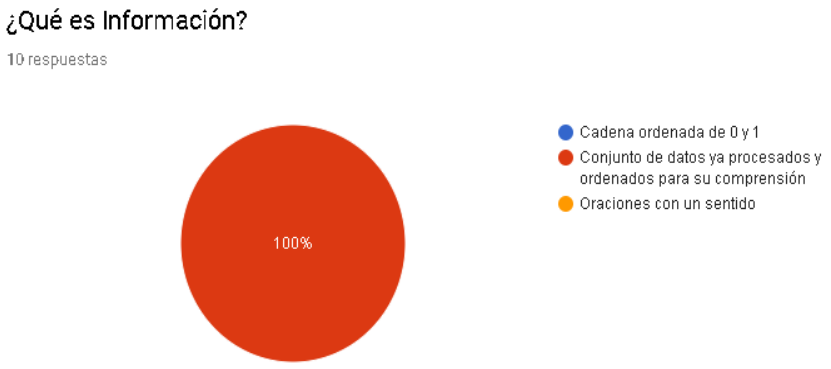
Nº	APELLIDOS Y NOMBRES	CÓDIGO	SEMESTRE	MATERIA	FIRMA
1	Manuel Andrés Ramirez	625715	8	Redes Converg	
2	Molano Diaz Leidy Molano	625152	8	Redes Convergentes	
3	Candia Tavera Juan Pablo	625469	8	Redes Convergentes	
4	Jorge Carpintero Suarez	625714	8	Redes Convergentes	
5	Pervid Andres Arbelaez	625739	8	Redes Convergentes	
6	Laura Ramirez A.	625716	8	Redes Convergentes	
7	Alexander Franco	625756	8	Redes Convergentes	
8	Murillo Vasquez Oscar	625741	8	Redes Convergentes	
9	Posada Cesadiego Karolayn	625761	8	Redes Convergentes	
10	Gomez Alfaro Angel Felipe	625773	8	Redes Convergentes	

Fuente: Autores

De acuerdo a la imagen 56 se evidencia la participación del curso más afectado en el ataque de ingeniería social , realizando la retroalimentación de la forma como fueron víctimas de phishing por medio de códigos qr y como pueden mitigar los riesgos a los que se está expuesto en la web.

3.16 Resultados de encuesta de concientización

Imagen 57. Que es información



Fuente. Autores

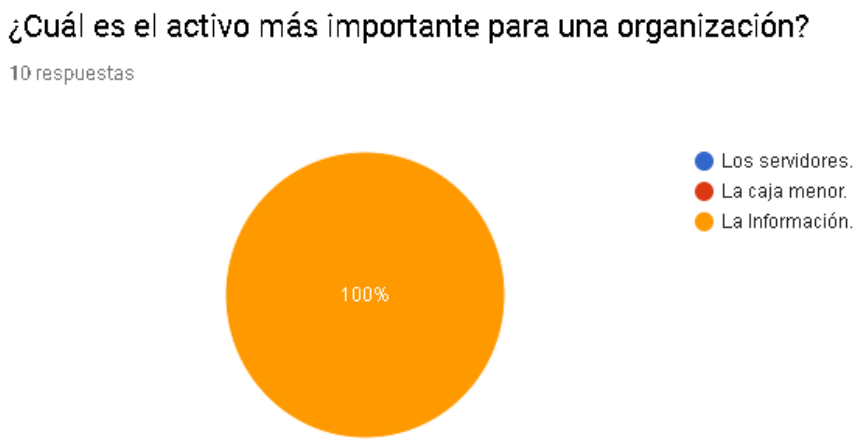
En la imagen 57 se evidencia que después de hacer la retroalimentación en el curso de redes convergentes el 100% conoce y sabe los conceptos de información.

Imagen 58. Pilares de la seguridad de la información

Fuente : Autores

Es un avance importante en la educación, los principios y pilares fundamentales de la seguridad de la información como se muestra en la imagen 58 respondieron correctamente el 100%.

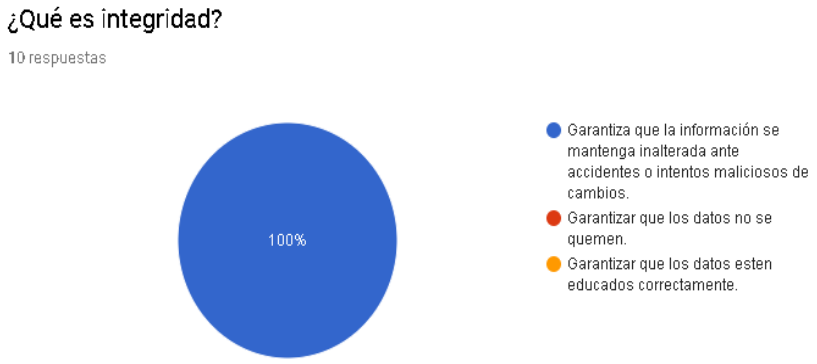
Imagen 59. El activo más importante de la organización



Fuente. Autores

En la imagen 59 se observa como identifican claramente el valor y activo más importante de la organización, actualmente se hacen inversiones económicas para la implementación de sistemas para proteger y gestionar la información, principalmente para la conservación del negocio.

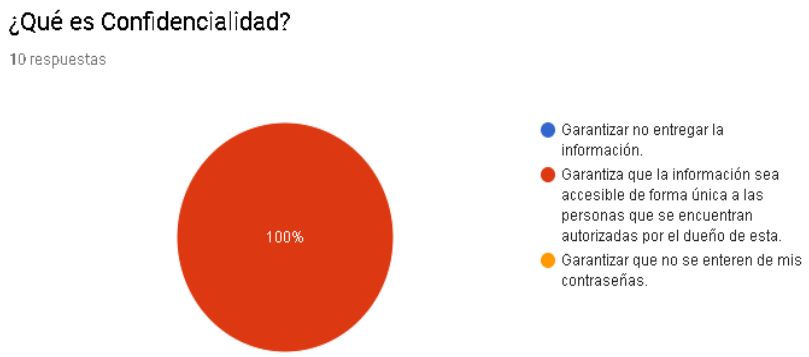
Imagen 60. Que es integridad



Fuente : Autores

Se observa claramente en la imagen 60 el grado de conocimiento en el curso a la pregunta de integridad de la información como componente fundamental.

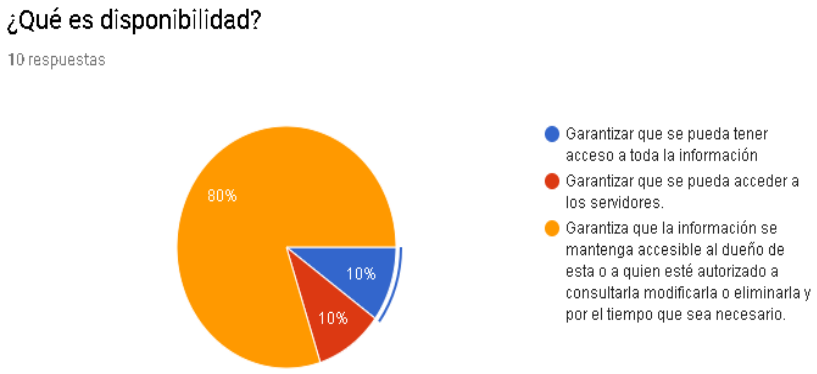
Imagen 61. Que es confidencialidad



Fuente : Autores

La confidencialidad de los datos en la seguridad de la información es vital para las organizaciones en protección de datos y de negocio como se observa en la imagen 61 claramente se evidencia el conocimiento.

Imagen 62 . Que es disponibilidad



Fuente. Autores

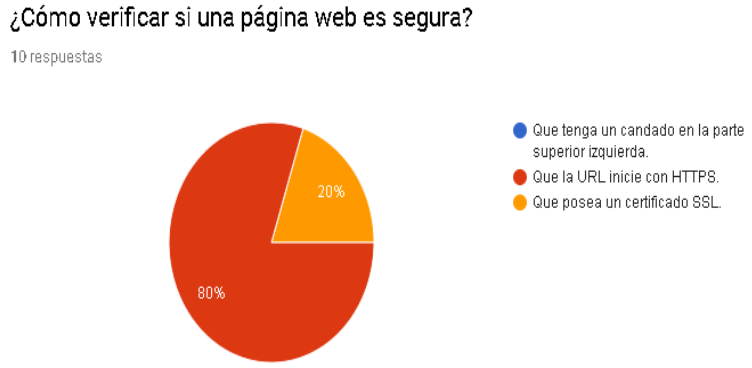
A pesar de los esfuerzos en el feedback en la imagen 62 se observa que, la concientización en el tema de disponibilidad de la información se observa que un 10% color azul que solo se puede garantizar el acceso a la información y un 10% color rojo de garantizar solo el acceso a los servidores y un 80% color naranja contesto asertivamente .

Imagen 63. Que es seguridad de la información

Fuente. Autores

El concepto de seguridad de la información se encuentra excelente de acuerdo a la imagen 63 y cuenta con un 100% de asertividad.

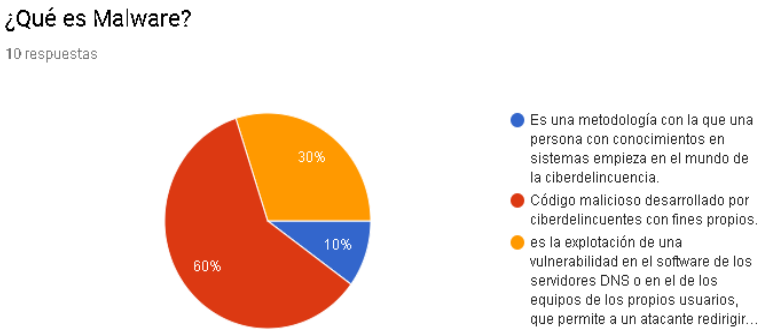
Imagen 64. Como verificar si una página web es segura



Fuente. Autores

Esta respuesta es impactante para los resultados, no es suficiente la concientización como se muestra en la imagen 64 aun no pueden identificar como saber si una página web es completamente segura un 80% contesto erróneamente que es URl inicie con https y un 20 % contesto correctamente certificado SSl con un 20 %.

Imagen 65. Que es malware



Fuente: Autores

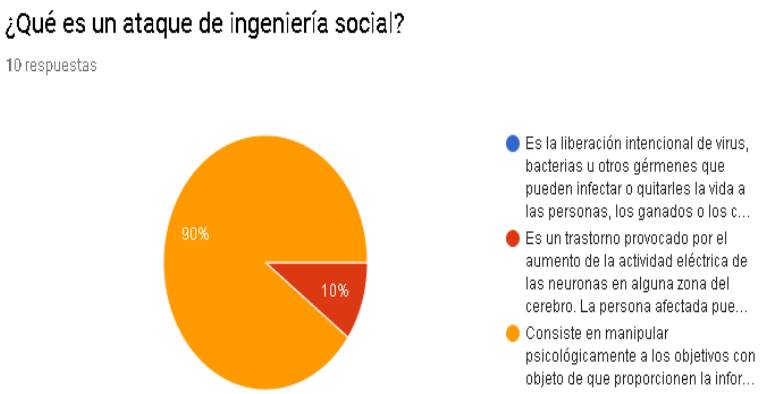
De todas las recomendaciones que se hicieron en el laboratorio 5 en las instalaciones de la universidad católica de Colombia en el aula de clase de sistemas de redes convergentes los estudiantes aun no tienen claro como identificar o concepto de malware como se observa en la imagen 65 un 10 % color azul cree que es una metodología con las personas y sistemas de la ciberdelincuencia , el 30% color amarillo cree que es una explotación de DNS y el 60 % color rojo sabe el concepto de código malicioso desarrollado.

Imagen 66. Qué es un delincuente informático

Fuente: Autores

De acuerdo con la imagen 66 se evidencia que el 10% no sabe que es un delincuente informático y un 90% tiene conocimientos claros del tema.

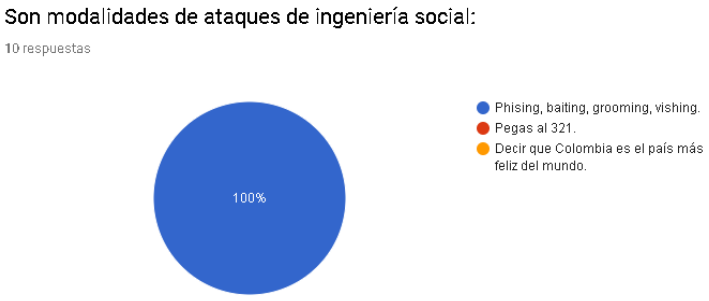
Imagen 67. Qué es un ataque de ingeniería social



Fuente: Autores

Los datos son aun preocupantes como lo muestra la imagen 68 aún se observa desconocimiento del 10% en que consiste la ingeniería social y un 90 % tiene conocimiento claro.

Imagen 68. Modalidades de ataques de ingeniería social



Fuente : Autores

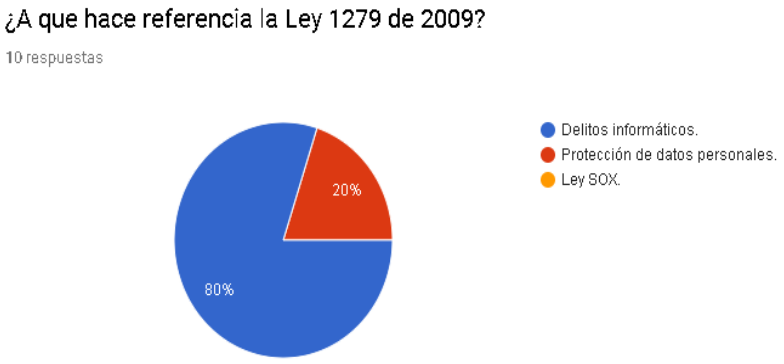
De acuerdo a la imagen 68 la pregunta modalidades de ataques de ingeniería un 100% tiene conocimientos claros del tema

Imagen 69. Qué es un Phishing

Fuente: Autores

Aun después del ataque y después la retroalimentación de conceptos en que es phishing de acuerdo con los resultados reflejados en la imagen 69 un 20% color amarillo contesto declaración y sospecha para que oyentes crean, un 10 % considera que es un tipo de actividad tradicional de poco desarrollo y un 70% tiene los conceptos claros.

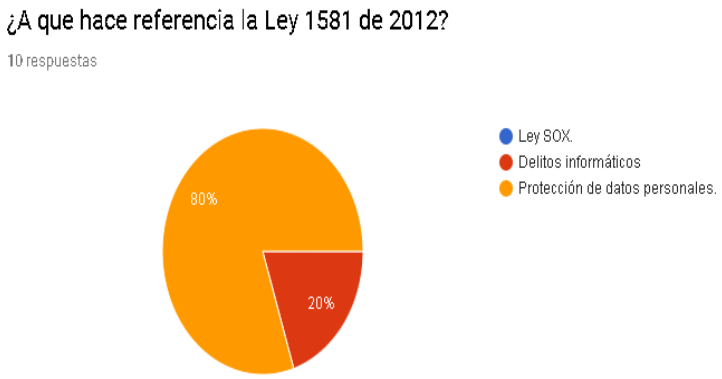
Imagen 70. A qué hace referencia la ley 1279 de 2009



Fuente : Autores

De acuerdo con la imagen 70 se observa que el 20% aún no tiene claro a que hace referencia la ley 1279 de 2009 y un 80 % reforzó los conocimientos satisfactoriamente

Imagen 71. A qué hace referencia la ley 1581 de 2012



Fuente : Autores

En la imagen 71 aún se observa desconocimiento en la ley 1581 de 2012 de protección de datos personales con un 20% de color rojo y un 80% de color amarillo que identifican satisfactoriamente la normatividad .

3.17 Limitaciones del proyecto

Implementación del ejercicio académico ya que es necesario un visto bueno de la Universidad Católica de Colombia una vez verifique toda la parte jurídica respecto a la normatividad legal vigente respecto a estos temas relacionados en los anexos de este documento.

- Implicaciones legales.
- Público sin dispositivo móvil.
- Público sin acceso a internet desde su dispositivo móvil.
- La participación de público debido al poco interés respecto al tema.
- La participación de público debido al desconocimiento del tema.
- La participación de público debido al conocimiento del tema.

4 PRODUCTOS A ENTREGAR

- Informe con análisis de los resultados obtenidos y las recomendaciones de seguridad de la información y mejores prácticas.

- Obtener e identificar una muestra significativa del comportamiento de la población respecto al código QR, a partir de una muestra.

- Presentar datos reales que puedan demostrar al curso de pregrado el nivel de seguridad de la lectura de los códigos QR y sensibilización, además exposición de cifras y datos probabilísticos.
- Artículo científico con los resultados del ejercicio académico y experiencia obtenida.

5 RESULTADOS ESPERADOS E IMPACTOS

- Obtener e identificar una muestra significativa del comportamiento de la población respecto al código QR, a partir de una muestra.
- Presentar datos reales que puedan demostrar al curso de pregrado el nivel de seguridad de la lectura de los códigos QR y sensibilización, además exposición de cifras y datos probabilísticos.

6 ESTRATEGIAS DE COMUNICACIÓN

- Publicación de la investigación en la biblioteca de la universidad católica de Colombia
- Análisis de los resultados estadísticos de la investigación
- Los datos obtenidos, estudiar la viabilidad y retroalimentación de resultados a los participantes del experimento.
- Socialización del resultado del estudio con la población participante
- Artículo científico con los resultados del ejercicio académico y experiencia obtenida.

7 CONCLUSIONES

Se dio el cumplimiento total tanto del objetivo general como el de los específicos, ya que se logró diseñar e implementar el ataque controlado de ingeniería social a los alumnos de los cursos diseño de redes convergentes e ingeniería social del programa de ingeniera de sistemas de la universidad Católica de Colombia.

Efectivamente el vector de ataque de ingeniería social viene creciendo de manera vertiginosa , en diferentes sectores tanto como en lo empresarial, publico, financiero , se realizó una prueba piloto con estudiantes 'conocedores de la problemática' como son cursos de redes convergentes e ingeniería social y nos encontramos que efectivamente son nativos digitales pero el desconocimiento total del vector de ataque con códigos QR es preocupante y alarmante , dado los resultados encontrados se evidencia que efectivamente el 62.5% de los estudiantes desconocen el vector de ataque, manifiestan saber de seguridad informática porque a través de la técnica de persuasión efectiva cayeron como victimas fácilmente .

La metodología implementada en la investigación, técnica de ingeniería social y persuasión fue exitosa , falta mucho a nivel de investigación de temática de ingeniería social y códigos QR , se evidencia que cualquier ciber delincuente con conocimientos pueden descargar un emulador y copia una página web en ficheros comprimidos y alojarlo e un servidor gratuito y realiza el vector de ataque , QR debe mejorar también muchos criterios de seguridad para hacer y crear sitios seguros.

Mayor cultura de seguridad de la información, la ingeniería social es uno de los modos operandi más comunes de los delincuentes informáticos para realizar estafas a través de la red, no se trata solamente de asegurar nuestra infraestructura tecnológica únicamente ya que es más que evidente que las personas son el eslabón más débil de la cadena de seguridad de la información, por ende debemos reforzar y dar prioridad al tema de la concientización no solo en el trabajo, también en el estudio y a nivel personal, construir el conocimiento de seguridad de nuestra información y más en una era donde la tecnología invade cada vez más nuestra intimidad poniendo en riesgo

nuestra propia integridad.

8 BIBLIOGRAFÍA

[1] «HITHUB,» Tecnologia productora , 17 05 2018. [En línea]. Available: https://github.com/OWASP/QRLJacking. [Último acceso: 15 8 2019].

[2] Secpronet, «Secpronet,» Segurite, 17 9 2017. [En línea]. Available: https://secpronet.blogspot.com/2018/03/qrljacking-new-social-engineering.html. [Último acceso: 15 05 2019].

[3] «centro criptológico nacional,» CCN-CERT, 31 05 2015. [En línea]. Available: www.ccn-cert.cni.es/seguridad-al-dia/noticias-seguridad/2031-2015-03-31-12-24-04.html. [Último acceso: 15 7 2019].

[4] E. O. S. W. C. Z. y. L. C. T. Vidas, «The Susceptibility of Smartphone Users to QR code Phishing attacks,» de *Financial Cryptography and Data Security, vol. 7*, ATAIS, 7, 2013, pp. 52-69.

[5] C. Muñoz, «FayerWayer,» 29 03 2018. [En línea]. Available: https://www.fayerwayer.com/2018/03/hackeo-lector-codigos-qr-ios-apple. [Último acceso: 17

] 7 2019].

C. T. Vidas, QRishing: The Susceptibility of Smartphone Users to, Carnegie Mellon
6 University, Estados Unidos : Gipsr3, 2015.
]

G. Peri, «Unitac,» 15 3 2019. [En línea]. Available:
7 https://www.unitag.io/es/qrcode/what-is-a-qrcode. [Último acceso: 28 8 2019].
]

D. D. Sanchez, Lectura y verificacion de Codigos QR, Girona-España: Salvator,
8 Aigieru-Medrano.
]

T. S. y. M. V. N. Demidova, «SECURELIST,» 28 05 23. [En línea]. Available:
9 https://securelist.lat/spam-and-phishing-in-q1-2018/86992/. [Último acceso: 5 06 2019].
]

Ingenieria Social explotando a los Humanos (Scan BOX), Cataluña: S.A, 2015.
1
0
]

O. LatamTour, Ingenieria Social Hacker Psicologico, Republica Dominicana : Sismap,
1

1 2016.
]

Escuela Superior de Educacion Publica SISTEM , SISTEM SARGSI, Bogota : 1 SARGSI, 2018.
2
]

Direccion General de Sistemas , ómo protegerse del phishing, España : Transeguriti, 1 2018.
3
]

COLEGIO OFICIAL DE INGENIEROS DE TELECOMUNICACIÓN, Correo 1 Electronico y Spam, Ibergraphi 2002, Madrid : S.L.L, 2002.
4
]

NORTON BY SIMATEC, «Amenazas emergentes,» 17 2 2019. [En línea]. Available: 1 https://mx.norton.com/internetsecurity-emerging-threats-what-is-social-engineering.html.
5 [Último acceso: 1 10 2019].
]

Ciencia y tecnologia , « Informatica forense de colombia (Vishing),» 31 8 2019. [En 1 línea]. Available: https://www.informaticaforense.com.co/vishing/. [Último acceso: 31 10
6

] 2019].

Ruben ramiro , «Mmétodos de búsqueda de amenazas de ciberseguridad,» 26 8 2018.
1 [En línea]. Available: https://ciberseguridad.blog/metodos-de-busqueda-de-amenazas-de-
7 ciberseguridad/. [Último acceso: 31 5 2019].
]

kaspersky., «¿Qué es el pharming y cómo evitarlo?,» 25 11 2018. [En línea]. Available:
1 https://latam.kaspersky.com/resource-center/definitions/pharming. [Último acceso: 31 8 2019].
8
]

G. d. gismaki, HACKING CON INGENIERÍA SOCIAL. TÉCNICAS PARA
1 HACKEAR HUMANOS. MUNDO HACKE, España -Valencia: RA-MA , 2017.
9
]

E. O. S. W. C. Z. L. C. T. Vidas, QRishing: The Susceptibility of Smartphone Users to,
2 Texas, 2015.
0
]

R. Menendez, «Comunidad Peru crack,» Hacker master,» 24 4 2019. [En línea].
2 Available: http://www.perucrack.net/2014/09/ataque-por-medio-de-codigo-qr.html. [Último
1 acceso: 31 5 2019].

]

Hacking Tecnicas , «INGENIERÍA SOCIAL. TÉCNICAS PARA HACKEAR
2 HUMANOS.,» 31 5 2017. [En línea]. Available: http://www.perucrack.net/2014/09/ataque-
2 por-medio-de-codigo-qr.html. [Último acceso: 31 8 2019].
]

CISCO, «Reporte Anual de Ciberseguridad,» Cisco Systems (EE. UU.), Masashusett:
2 Cisco Systems, 2018.
3
]

T. S. y. M. V. N. Demidova, «SECURELIST,» 28 05 2018. [En línea]. Available:
2 https://securelist.lat/spam-and-phishing-in-q1-2018/86992. [Último acceso: 10 31 2019].
4
]

European Cybercrime Centro, Contexto de Cibercrimen en Colombia, Bogota : Centro
2 Cibernético Policial,, 2018.
5
]

cioperu.pe/articulo, «Reportajes y analisis de seguridad,» 15 6 2009. [En línea].
2 Available: https://cioperu.pe/articulo/24726/saml-que-es-para-que-se-usa-como-funciona/.
6 [Último acceso: 1 5 2019].

]

MINISTERIO DE TECNOLOGIAS DE INFORMACION, «Constitución Politica de Colombia,» 1 12 2012. [En línea]. [Último acceso: 21 4 2019].
27
]

WinHTTrack es la versión de Windows, «httrack.com,» 31 7 2015. [En línea]. Available: https://www.httrack.com/. [Último acceso: 31 7 2019].
28
]

XAMPP, «apachefriends v3,» 31 05 2014. [En línea]. Available: https://www.apachefriends.org/es/index.html. [Último acceso: 31 7 2019].
29
]

IMB, «IBM knowledge,» 15 08 2017. [En línea]. Available: https://www.ibm.com/support/knowledgecenter/es/SSQL82_9.5.0/com.ibm.bigfix.doc/Platform/Config/c_what_is_saml_2_0.html.
30
]

IMB, «IBM knowledgecenter,» IBM, 15 08 2017. [En línea]. Available: https://www.ibm.com/support/knowledgecenter/es/SSQL82_9.5.0/com.ibm.bigfix.doc/Platform/Config/c_what_is_saml_2_0.html. [Último acceso: 31 10 2019].
31

]

es.qr-code-generator, «Generador de Codigo QR,» 31 5 2018. [En línea]. Available: https://es.qr-code-generator.com/a1/?ut_source=google_c&ut_medium=cpc&ut_campaign=spanish_top_kw&ut_content=qr_code_generator_exact&ut_term=qr%20code%20generator_e&gclid=EAIaIQobChMIjrrH1ZHI5QIVGKSzCh1BFAiFEAAYASAAEgKTb_D_BwE. [Último acceso: 21 9 2019].

[3]
[2]
[]

9 ANEXOS

Anexos 1 Normatividad LEY 1273 DE DELITOS INFORMATICOS

LEY 1273 DE 2009

(Enero 5)

Diario Oficial No. 47.223 de 5 de enero de 2009

CONGRESO DE LA REPÚBLICA

Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado “de la protección de la información y de los datos”- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.

EL CONGRESO DE COLOMBIA

DECRETA:

ARTÍCULO 1o. Adiciónase el Código Penal con un Título VII BIS denominado "De la Protección de la información y de los datos", del siguiente tenor:

CAPITULO I

De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos

Artículo 269A: *Acceso abusivo a un sistema informático*. <Ver Notas del Editor> El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.

Artículo 269B: *Obstaculización ilegítima de sistema informático o red de telecomunicación.* El que, sin estar facultado para ello, impida u obstaculice el funcionamiento o el acceso normal a un sistema informático, a los datos informáticos allí contenidos, o a una red de telecomunicaciones, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con una pena mayor.

Artículo 269C: *Interceptación de datos informáticos*. El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los transporte incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses.

Artículo 269D: *Daño Informático*. El que, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos, o un sistema de tratamiento de información o sus partes o componentes lógicos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.

Artículo 269E: *Uso de software malicioso*. El que, sin estar facultado para ello, produzca, trafique, adquiera, distribuya, venda, envíe, introduzca o extraiga del territorio nacional software malicioso u otros programas de computación de efectos dañinos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.

Artículo 269F: *Violación de datos personales*. El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes, incurrirá en pena de prisión de cuarenta y

ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

Artículo 269G: *Suplantación de sitios web para capturar datos personales*. El que con objeto ilícito y sin estar facultado para ello, diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con pena más grave.

En la misma sanción incurrirá el que modifique el sistema de resolución de nombres de dominio, de tal manera que haga entrar al usuario a una IP diferente en la creencia de que acceda a su banco o a otro sitio personal o de confianza, siempre que la conducta no constituya delito sancionado con pena más grave.

La pena señalada en los dos incisos anteriores se agravará de una tercera parte a la mitad, si para consumarlo el agente ha reclutado víctimas en la cadena del delito.

Artículo 269H: *Circunstancias de agravación punitiva*: Las penas imponibles de acuerdo con los artículos descritos en este título, se aumentarán de la mitad a las tres cuartas partes si la conducta se cometiere:

1. Sobre redes o sistemas informáticos o de comunicaciones estatales u oficiales o del sector financiero, nacionales o extranjeros.

2. Por servidor público en ejercicio de sus funciones.

3. Aprovechando la confianza depositada por el poseedor de la información o por quien tuviere un vínculo contractual con este.

4. Revelando o dando a conocer el contenido de la información en perjuicio de otro.

5. Obteniendo provecho para sí o para un tercero.

6. Con fines terroristas o generando riesgo para la seguridad o defensa nacional.

7. Utilizando como instrumento a un tercero de buena fe.

8. Si quien incurre en estas conductas es el responsable de la administración, manejo o control de dicha información, además se le impondrá hasta por tres años, la pena de inhabilitación para el ejercicio de profesión relacionada con sistemas de información procesada con equipos computacionales.

CAPITULO II

De los atentados informáticos y otras infracciones

Artículo 269I: *Hurto por medios informáticos y semejantes*. El que, superando medidas de seguridad informáticas, realice la conducta señalada en el artículo 239 manipulando un sistema informático, una red de sistema electrónico, telemático u otro medio semejante, o suplantando a un usuario ante los sistemas de autenticación y de autorización establecidos, incurrirá en las penas señaladas en el artículo 240 de este Código.

Artículo 269J: *Transferencia no consentida de activos*. El que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consiga la transferencia no consentida de cualquier activo en perjuicio de un tercero, siempre que la conducta no constituya delito sancionado con pena más grave, incurrirá en pena de prisión de cuarenta y ocho (48) a ciento veinte (120) meses y en multa de 200 a 1.500 salarios mínimos legales mensuales vigentes. La misma sanción se le impondrá a quien fabrique, introduzca, posea o facilite programa de computador destinado a la comisión del delito descrito en el inciso anterior, o de una estafa.

Si la conducta descrita en los dos incisos anteriores tuviere una cuantía superior a 200 salarios mínimos legales mensuales, la sanción allí señalada se incrementará en la mitad.

ARTÍCULO 2o. Adiciónese al artículo 58 del Código Penal con un numeral 17, así:

Artículo 58. *Circunstancias de mayor punibilidad*. Son circunstancias de mayor punibilidad, siempre que no hayan sido previstas de otra manera:

(...)

17. Cuando para la realización de las conductas punibles se utilicen medios informáticos, electrónicos o telemáticos.

ARTÍCULO 3o. Adiciónese al artículo 37 del Código de Procedimiento Penal con un numeral 6, así:

Artículo 37. *De los Jueces Municipales*. Los jueces penales municipales conocen:

(...)

6. De los delitos contenidos en el título VII Bis.

ARTÍCULO 4o. La presente ley rige a partir de su promulgación y deroga todas las disposiciones que le sean contrarias, en especial el texto del artículo 195 del Código Penal.

El Presidente del honorable Senado de la República,

HERNÁN ANDRADE SERRANO.

El Secretario General del honorable Senado de la República,

EMILIO RAMÓN OTERO DAJUD.

El Presidente de la honorable Cámara de Representantes,

GERMÁN VARÓN COTRINO.

El Secretario General de la honorable Cámara de Representantes,

JESÚS ALFONSO RODRÍGUEZ CAMARGO.

REPUBLICA DE COLOMBIA - GOBIERNO NACIONAL

Publíquese y cúmplase.

Dada en Bogotá, D. C., a 5 de enero de 2009.

ÁLVARO URIBE VÉLEZ

El Ministro del Interior y de Justicia,

FABIO VALENCIA COSSIO.

<Consultar norma en SUIN JURISCOL: http://www.suin.gov.co/viewDocument.asp?ruta=Leyes/1676699>

Anexos 2 CIRCULAR EXTERNA 006 SEGURIDAD Y CALIDAD OPERACIONES MEDIANTE CODIGOS QR

La Superintendencia Financiera emitió la Circular Externa 006 del 21 de marzo de 2019, la cual tiene como referencia: Impartir instrucciones relacionadas con la seguridad y calidad para la realización de operaciones mediante códigos QR

El siguiente es el texto completo de la Circular 006 completo:

Apreciados señores:

Con el propósito de promover alternativas para realizar pagos electrónicos, consolidar la estandarización e interoperabilidad de los sistemas de pago y continuar con el proceso de fortalecimiento de la inclusión financiera y la reducción del uso del efectivo, la Superintendencia Financiera de Colombia, en ejercicio de sus facultades legales, en especial las conferidas en el numeral 5 del artículo 11.2.1.4.2 del Decreto 2555 de 2010 imparte las siguientes instrucciones:

PRIMERA: Modificar el numeral 2.2 y el subnumeral 2.3.4 del Capítulo I, Título II, Parte I de la Circular Externa 026 de 2014 Circular Básica Jurídica, con el fin de establecer el estándar y los requerimientos que se deben atender en materia de seguridad y calidad para la realización de

operaciones monetarias mediante códigos QR.

SEGUNDA: Las entidades que a la fecha de expedición de la presente circular soporten pagos a través de códigos QR deben ajustarse a las instrucciones aquí contenidas dentro de los seis meses siguientes a su entrada en vigor.

TERCERA: La presente Circular rige al momento de su publicación.

Se anexan las páginas objeto de modificación.

Cordialmente,

JORGE CASTAÑO GUTIÉRREZ

Superintendente Financiero de Colombia

Anexo 3. Tabla ANALISIS DE TECNICAS DE INGENIERIA SOCIAL

CODIGOS QR

La ingeniería social ha desarrollado diferentes técnicas de persuasión a las personas, para manipular sus actos, con diferentes técnicas para obtener información confidencial, en empresas, instituciones y personas, se realizara comparativo y análisis de los que aplican en el proyecto de ataque controlado de ingeniería social por medio de códigos QR.

Check List de modalidades de Ataques de ingenieria Social 19%

#	TIPOS DE TECNICAS DE INGENIERIA SOCIAL	TECNICA	DESCRIPCIONES	Estado (Hace parte de la
1	**Tecnica Social 1**			☑
1.1	Ingeniería Social Inversa (Reverse Social Engineering)	Sabotaje iductivo	Esta técnica se usa por los atacantes, el hacker causa	☐
1.2	Desarrollar Confianza (Establishing Trust)	Sabotaje iductivo	El objetivo principal en esta metodología de ataque como su nombre lo indica es establecer confianza con el objetivo; una vez que la	☐
~~1.3~~	~~Difusión de Responsabilidades (Diffusion)~~	~~Sabotaje iductivo~~	~~La difusión de responsabilidades hace sentir al objetivo que le cargaran con la~~	☑
1.4	Buscar en la Basura (Dumpster Diving)	Sabotaje Singular	Para las compañías incluso incurre en riesgos en botar la basura puesto que	☐
~~2.1~~	~~Suplantación de Identidad (Impersonation)~~	~~Engaño fisico o virtual~~	~~Otra metodología muy usada por los ingenieros sociales es la~~	☑
2.2	Llamadas telefónicas	Engaño fisico o virtual	Una de las técnicas más conocidas por los Hackers es la de	☐
2.3	Ataques internos y empleados descontentos	Camuflarse y persuadir dentro de una organización	Un atacante puede inducir y con éxito aprovechando el lenguaje interno de la	☐
2.4	Obtener acceso físico (Tailgating & Piggybacking)	Persuación a obtener credenciales	Los administradores y oficiales de seguridad poseen mucha información que puede facilitar al atacante de	☐
3	**Tipos de Phishig 3**			☑
3.1	Estafa CEO	Estafa	La estafa al CEO , se produce cuando el delincuente se hace	☐
3.2	CLON Phishing	Replica virtual	Este tipo de técnica es aprovechar mensajes legítimos por la victima	☐
~~3.3~~	~~Suplantación de Dominio~~	~~Falsificación del Dominio~~	~~La falsificación de dominios se produce cuando un~~	☑
3.4	Evil Twin	Aprovechamiento WIFI	Un «Evil Twin» es una forma de phishing que	☐
3.5	Phishing Https	URL falso	El enfoque del ataque se refleja en enviar un correo electrónico con un enlace de aspecto legítimo en el	☐
3.6	Smishing	Mensaje de texto Falso	El phishing por mensajes de texto, aprovecha este medio para enviar una URL maliciosa con algún tipo de oferta o contenido ~~Ataque de Spear~~	☐
	Spear Phishing	Vista de contraseñas	PHISHING es una forma específica de phishing. A diferencia de los correos electrónicos de suplantación de identidad (phishing) generales, el	☐
4	**Otros**			☐
4.1	Vishing	Llamada suplantada	Un ataque de vishing ocurre cuando un delincuente llama por	☐

ANEXO 4 .LINK DE VERIFICACION DE ENCUESTA INICIAL DE SEGURIDAD DE LA INFORMACIÓN

Se puede realizar la verificación del contenido de primera encuesta en el siguiente link):https://docs.google.com/forms/d/e/1FAIpQLScSW4dElNXZJWdhEN5E68vXD1Z33K3wZj6xe3FCAb5Yo_s-Ew/viewform

ANEXO 4. INSTITUTO NACIONAL DE ESTÁNDARES Y TECNOLOGÍA NIST

Referencia para la definición de Ingeniería Social y phishing, este es el Instituto Nacional de Estándares y Tecnología **NIST,** es la agencia de la Administración de Tecnología del Departamento de Comercio de los Estados Unidos.

- https://csrc.nist.gov/glossary/term/phishing
- https://csrc.nist.gov/glossary/term/social-engineering
- https://seguridad.syr.es/glosario-de-terminos