LA SEGURIDAD INFORMÁTICA EN LA VIDA COTIDIANA DE LAS PERSONAS (INGENIERÍA SOCIAL) CASO CREZCAMOS S.A.

CRISTHIAN CAMILO MONARES MARÍN

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BUCARAMANGA
2020

LA SEGURIDAD INFORMÁTICA EN LA VIDA COTIDIANA DE LAS PERSONAS (INGENIERÍA SOCIAL) CASO CREZCAMOS S.A.

CRISTHIAN CAMILO MONARES MARÍN

MONOGRAFÍA
Trabajo de grado para optar el título de
Especialista en Seguridad Informática

Director
Alexander Larrahondo Nuñez
Docente Ocasional ECBTI
MSc, CISM

Tutor
SALOMÓN GONZÁLEZ GARCÍA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
FACULTAD DE SISTEMAS
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BUCARAMANGA
2020

AGRADECIMIENTOS

Infinitas gracias a Dios por su amor y por la oportunidad de llevar a feliz término este proyecto. Agradezco todas las Dioscidencias.

CONTENIDO

LISTA DE TABLAS

LISTA DE ILUSTRACIONES

RESUMEN

TÍTULO:

LA SEGURIDAD INFORMÁTICA EN LA VIDA COTIDIANA DE LAS PERSONAS (INGENIERÍA SOCIAL) CASO CREZCAMOS S.A.

AUTOR:

MONARES MARÍN, Cristhian Camilo

PALABRAS CLAVES: Seguridad informática, delitos informáticos, protección de datos personales, Carding, Sabotaje Informático, Suplantación, Vishing, Phishing, Smishing, Cibergrooming, Cibertaques, Ciberestafa, Piratería digital.

DESCRIPCIÓN:

El trabajo expuesto a continuación es el resultado de un estudio orientado al desarrollo de una prueba de Ingeniería Social sencilla aplicada a una muestra focal de los colaboradores de la compañía Crezcamos S.A.

El desarrollo metodológico de este proyecto se basa en la aplicación de importantes áreas del conocimiento concernientes a la seguridad informática y a la protección de los datos personales en todas sus dimensiones, las cuales reflejan un resultado de importancia en el diagnóstico de los niveles de conocimiento frente a una amenaza tan cotidiana como lo son los delitos informáticos. Mediante el análisis de encuestas, la aplicación de conocimiento vía capacitaciones, la evaluación de aspectos referentes a la ingeniería social, la exposición al riesgo de ser investigado por medios públicos y gratuitos, entre otros aspectos que son fundamentales para la ingeniería social, permitieron un adecuado acercamiento y materialización de las amenazas que implican no aplicar la seguridad informática.

DEFINICIÓN DEL PROYECTO

TÍTULO:

LA SEGURIDAD INFORMÁTICA EN LA VIDA COTIDIANA DE LAS PERSONAS, (INGENIERÍA SOCIAL) CASO CREZCAMOS S.A.

MODALIDAD: Investigatición explorativa

RESPONSABLES:

NOMBRE AUTOR:	**Cristhian Camilo Monares Marín**
E-MAIL AUTOR:	**ccmonares@gmail.com**
TELÉFONO AUTOR:	**3003817017**
FIRMA AUTOR:	_____
NOMBRE DIRECTOR:	**Alexander Larrahondo Nuñez**
E-MAIL DIRECTOR:	
TELÉFONO DIRECTOR:	
FIRMA DIRECTOR:	_____
NOMBRE TUTOR:	**Salomón González García**
E-MAIL TUTOR:	**salomon.gonzalez@unad.edu.co**
TELÉFONO TUTOR:	**Skype: Salomon_gonzalez16**
FIRMA TUTOR:	_____

INTRODUCCIÓN

En la informática, los sistemas se encuentran en constante maduración con el uso de estándares, modelos y metodologías que garantizan que cualquier proceso que se analice, evalúe y gestione bajo un sistema de información, está cada vez más cerca a los índices robustos de seguridad. Esto permite que no solo se protejan los activos físicos más importantes en las organizaciones e instituciones, si no, toda la información y los sistemas que las posean.

En la actualidad, los avances tecnológicos a nivel de los sistemas de información y comunicación dan pasos enormes, ayudando a crecer íntegramente a la tecnología en hardware; Por esto, se hace necesario establecer las recomendaciones más apropiadas que permitan proteger la información en un contexto en donde es más creciente y latente el aumento de los delitos informáticos y los riesgos que amenazan los recursos físicos y de la información de las distintas organizaciones e instituciones propietarias de éstas.

Es por esto que las organizaciones deben adoptar todas las políticas, planes y estrategias de seguridad que les provean las herramientas funcionales más eficaces y eficientes que permitan salvaguardar todos los activos informáticos junto con sus sistemas de información, y de esta forma mitigar y minimizar las distintas vulnerabilidades, riesgos y amenazas que puedan generarse, así como aquellas preexistentes, que son buscadas y aprovechadas por los atacantes para eludir los controles y penetrar la seguridad en las distintas organizaciones.

Los riesgos informáticos pueden desembocar en la configuración de delitos informáticos cuando estos no fueron tratados dentro de un estudio serio y concertado de las vulnerabilidades adquiridas con los activos tecnológicos y de información; aún cuando cada vez hay nuevos tipos de delitos, el universo de los actores que intervienen en éstos, varía de forma muy rápida y dando poco tiempo

para adaptarse y tomar los controles internos para evitar los mismos incidentes en un futuro, lo que demanda una serie de políticas de prevención y controles periódicos que permitan minimizar y mitigar los posibles factores de riesgo para una organización.

Éste proyecto y su desempeño serán importantes para que en Crezcamos S.A. puedan identificar los factores tanto internos como externos que puedan llegar a comprometer la seguridad de los activos informáticos y sus sistemas de información, con la simulación de escenarios de ingeniería social que permitan la evaluación objetiva de cada uno de los factores analizados, y así generar políticas de prevención en cada uno de las personas que hacen parte de la compañía, estableciendo no solo políticas generales de prevención y protección de datos relacionados a la organización, sino, generando así mismo, una cultura de autoprotección en cada uno de los miembros de Crezcamos S.A., la cual generará un cambio significativo en el desempeño personal y laboral de la compañía, teniendo en cuenta que muchas de éstas personas podrán evaluar sus deficiencias y establecer políticas de mejora y crecimiento.

1 PLANTEAMIENTO DEL PROBLEMA

Crezcamos S.A., es una organización constituida como sociedad anónima, fue creada en el año 2008, y está sujeta a las normas y regulaciones comerciales aplicables dentro del territorio colombiano. Es vigilada por la Superintendencia de Sociedades desde el 01 de Abril del año 2010. El 2013 fue un año lleno de satisfacción y crecimiento para los colaboradores y accionistas, pues con la celebración del aniversario número quinto en el mes de Abril, se consolida como una de las compañías más importantes de la región, siendo una fuente generadora de empleo en los municipios donde actualmente hace presencia.

La misión de Crezcamos S.A se fundamenta en acompañar con servicios financieros adecuados y responsables el desarrollo de las familias emprendedoras del territorio nacional, principalmente brindando apoyo para el sector rural. Por otro lado, su visión se concentra en ser en el 2022 el principal banco rural, con políticas innovadoras, prestando servicios de excelencia en toda Colombia.

Actualmente la compañía cuenta con dos Políticas de Seguridad aprobadas en comité de gerencia y junta de accionistas, siendo éstas: la Política de Seguridad Informática y la Política de Seguridad Física y Bancaria.

En la Política de Seguridad Informática se plasmaron todos los requerimientos que permiten garantizar una excelente operación en las transacciones comerciales con los más de 70 mil clientes que acceden a los servicios financieros de la compañía.

Internamente se cuenta con servidores de dominio, firewalls de red, consolas de antivirus y sistemas de detección de intrusiones. En cuanto a la seguridad e integridad de las bases de datos, cuenta con un área altamente capacitada que gestiona herramientas propietarias y auditorías internas y externas constantes a los procedimientos del área TIC.

En la Política de Seguridad Física y Bancaria se establecieron los parámetros para el gestionar la seguridad en las oficinas a través de los sistemas de alarma

conectados a central de monitoreo, circuitos cerrados de televisión y control de acceso al edificio principal de la compañía. No obstante, se requiere generar constantes capacitaciones al personal en donde se cree la cultura de prevención ante delitos informáticos en entidades financieras.

Como resultado a la importancia de proteger los datos de los clientes y de la misma forma, de los colaboradores; en la actualidad se está documentando una política que permita aplicar la ley Nacional de protección de datos.

Con lo anterior, se hace necesario que los colaboradores de la compañía conozcan las distintas exposiciones al riesgo de delitos informáticos que tiene el uso de tecnologías de la información y comunicación, en especial, deben conocer la ingeniera social que suele afectar en gran medida a las instituciones financieras de Colombia, por tanto deben comunicar y establecer los comportamientos institucionales adecuados que aseguren la protección de su información.

2 JUSTIFICACIÓN

Este proyecto se plantea debido a la necesidad que se percibió en términos de seguridad informática al interior de la compañía. También, con la necesidad de identificar de manera detallada el nivel de conocimiento respecto a un riesgo cotidiano latente como lo es la Ingeniería social y al cual están expuestos los cerca de 200 colaboradores de la Dirección General de Crezcamos S.A.

Actualmente, la compañía concibe la tecnología como un componente estratégico, lo cual representa la implementación de políticas y procedimientos de seguridad, así como una cultura basada en la prevención y protección de todo tipo de interacción con el mundo digital atendiendo la Ley 1273 "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"[1] norma que tipifica los peligros a los cuales se enfrentan los colaboradores en el manejo de información ya sea personal o corporativa.

Las personas en la actualidad desconocen muchos de los peligros reales de tener una vida digital conectada, esto implica estar conectados todo el tiempo a la red mundial de Internet y este desconocimiento hace que las personas den un mal uso de las tecnologías y coloquen en peligro sus datos e identidad, lo que genera un riesgo potencial para su información y la de las personas que las rodean, dentro de su ámbito personal, familiar y laboral, teniendo en cuenta que, muchas de éstas personas no están conscientes del nivel de riesgo al que se someten al compartir su información en redes sociales o en comunidades en línea, sea de entretenimiento o profesional, lo que genera una ventana en la que una persona u organización con intenciones desconocidas, siendo en varias ocasiones malintencionadas, puede hacer uso o apropiarse de información que pueda

[1] CONGRESO DE LA REPÚBLICA DE COLOMBIA, Decreto de Ley 1273 de 2009

perjudicar al propietario de la misma y a aquellas personas que lo rodean o se encuentran vinculadas a la misma.

Así mismo, existe una amenaza constante y creciente en la red, lo que significa que una persona que desconozca de estas amenazas y no ponga en práctica una política de seguridad y prevención se puede considerar como un objetivo vulnerable para ciber ataques o para la ingeniería social, por lo que, se hace necesario realizar un análisis dentro de la compañía para evaluar el nivel de conocimiento previo de los colaboradores con respecto a estos factores de riesgo y un análisis posterior, en el que se evalúe el impacto de las capacitaciones a nivel personal de los participantes, en la que se pueda generar una política de prevención y protección de sus datos personales que se pueda reflejar y aplicar en la protección de los activos de la información de la compañía.

3 OBJETIVOS

3.1. OBJETIVO GENERAL

Diagnosticar el nivel de seguridad mediante metodologías de ingeniería Social, a los colaboradores de la IMF (Institución Micro Financiera) Crezcamos S.A.

3.2. OBJETIVOS ESPECÍFICOS

- Determinar las metodologías y técnicas de ingeniería social sujetas a aplicación para los colaboradores de la IMF Crezcamos S.A.
- Realizar el diagnóstico de nivel de conocimiento frente a ataques informáticos aplicando metodologías de ingeniería social en los colaboradores administrativos de la IMF Crezcamos S.A.
- Mejorar la percepción de seguridad informática en la vida digital y la exposición de los participantes a los delitos informáticos por desconocimiento, vía capacitaciones.
- Realizar las recomendaciones e implementar las estrategias de prevención de delitos informáticos e ingeniería social y fomentar la cultura organizacional.

4. MARCO DE REFERENCIA

En Crezcamos S.A. por requerimiento de la junta directiva de la compañía, anualmente se realizan dos (2) auditorías externas, que tienen por objetivo medir el nivel de seguridad de la información que se maneja en la compañía a nivel de los procedimientos y política establecidas para tales fines, sin embargo nunca se ha realizado en la compañía un estudio a nivel administrativo y comercial de la percepción de seguridad informática en los colaboradores de Crezcamos S.A., que les permita determinar y asegurar su identidad digital, para que de ésta forma, puedan entender los distintos riesgos a los que se pueden enfrentar al ser parte una institución micro financiera que maneja un enorme volumen de datos persales e información ultra confidencial, que puede llegar a ser accedida por métodos de ingeniera social hacia los colaboradores de la compañía, pudiendo llegar a causar un gran daño a los activos informáticos que se lleguen afectar.

Por lo que, dentro del presente proyecto se busca identificar, calcular y capacitar acerca del nivel de riesgo y las conductas potencialmente riesgosas relacionadas con la protección de datos personales, para que así, a través de las capacitaciones, charlas, actividades y material suministrado, se pueda generar de manera directa un impacto positivo en cada individuo, para lograr que éste pueda autodeterminar sus errores y tomar los consejos presentados que permitan aplicarlos a su vida personal y a la forma en que interactúa con el medio digital, el cual se verá reflejado directamenteen el manejo de los activos de la información de la Compañía Crezcamos S.A., minimizando así el factor de riesgo en su vida personal, social y profesional.

4.1. MARCO METODOLÓGICO

Como metodología para el desarrollo de los objetivos planteados, al grupo de muestra se le aplicará una encuesta previa a la primera jornada de capacitación, con el fin de conocer el nivel de seguridad digital establecida por los colaboradores administrativos de Crezcamos S.A. Esta encuesta contara con 20 preguntas, las cuales estarán encaminadas a conocer cómo actúan las personas en casos claros de ingeniería social.

Posterior a la primera encuesta, se realizará una capacitación acerca de temas relacionados con la seguridad informática, la cual se enfocará en la seguridad digital, con los métodos y estrategias más usadas por los delincuentes para acceder y obtener los datos de las personas a través de la ingeniería social.

Semanas después de la jornada de capacitación, se evaluara en una segunda encuesta las medidas de seguridad establecidas y la percepción de las personas posterior a la capacitación impartida a los participantes, dentro del marco de la seguridad informática.

Tras analizar esta segunda encuesta, se realizara la última jornada de capacitación, en donde, basados en los resultados obtenidos, se realizarán las recomendaciones y consejos de seguridad y prevención para que sean aplicados por los colaboradores administrativos tanto en su vida personal, como en las prácticas corporativas que realicen dentro de Crezcamos S.A.

A la Gerencia de la compañía, se le socializarán los resultados de las encuestas y las recomendaciones que deben adoptar, teniendo en cuenta el análisis obtenido.

5. ALCANCE Y DELIMITACIÓN

Con el presente proyecto se pretende diseñar una estrategia de mejora basada en la identificación de las distintas falencias identificadas durante y al final de las capacitaciones, la cual requerirá de la creación de un material de apoyo novedoso y una serie de recomendaciones para que los colaboradores de la Micro Financiera Crezcamos S.A comprendan los retos que involucra una vida digital conectada y un mejor uso de las tecnologías de la información y comunicación.

Mejorar la percepción de seguridad informática en la vida digital y la exposición de los participantes a los delitos informáticos por desconocimiento, por lo que, el presente proyecto se encuentra dirigido a los colaboradores de la compañía Crezcamos, dentro de distintas áreas de trabajo, del cual, se tomará un grupo de muestra poblacional equivalente a cien personas, de distintas edades, para así realizar una evaluación de su conocimiento previo acerca de los riesgos de la navegación en internet, su vida digital, la protección de sus datos personales y la ingeniería social, para lograr la creación de políticas personales de protección, prevención y así generar conciencia en éstas personas acerca de los riesgos de una vida conectada y de las distintas modalidades de ciber riesgos con los que se pueden encontrar día a día con su interacción con la red, ya sea para fines sociales, de entretenimiento o profesionales, los cuales pueden convertirlos en posibles víctimas de delitos informáticos.

6. PRODUCTOS A ENTREGAR

A continuación, se relacionan los productos tipo entregable del actual proyecto:

Tabla 1: Entregables

- *Material digital de las capacitaciones (Ver anexo C)*	Este material se compartió a través de correo electrónico a los participantes, que contenía las definiciones, ejemplos y recomendaciones en materia de seguridad informática e ingeniería social.
- *Encuesta previo jornada 1 y 2 (Cuantitativa)*	Primera encuesta realizada, donde se identificaron los principales riesgos de seguridad y el nivel de conocimiento sobre las amenazas existentes por parte de los participantes.
- *Resultados y estadísticas previo jornada 1 y 2 (Ver numeral 10)*	Análisis de los resultados con las encuestas aplicadas, realizando una comparativa estadística sobre el impacto obtenido con las capacitaciones impartidas en las distintas jornadas.
- *Socialización de resultados con la gerencia de la compañía y los colaboradores participantes. (Ver anexo G)*	Exhibición de los resultados obtenidos con las actividades realizadas a los colaboradores de la compañía, en la que se evidenció el impacto personal de las capacitaciones y en la autoevaluación personal de los participantes sus falencias y la forma en la que podían corregirse.
- *Recomendaciones generales (Ver Anexo G)*	De acuerdo a los resultados que se entregaron a los participantes.

7. RECURSOS

En la tabla 2 se reunieron los recursos indispensables que se usaron para llevar a cabo el actual Proyecto:

Humano	Materiales
1. Colaboradores administrativos vigentes en Crezcamos S,A, 2. Personal del área de formación de apoyo de Crezcamos S.A.	3. Herramienta colaborativa Google Apps de Crezcamos S.A. para el desarrollo de las encuestas y material para las presentaciones. 4. Salones de capacitación de Crezcamos S.A. 5. Computadores portátiles para el desarrollo y análisis de los datos obtenidos.

8. CRONOGRAMA

El siguiente cronograma, establece las actividades a las que hace referencia el desarrollo del proyecto:

Actividad	Octubre 2016	Septiembre 2017				Octubre 2017				Noviembre 2017				Dic 2017
	14	S1	S2	S3	S4	S1	S2	S3	S4	S1	S2	S3	S4	S1
1. Entrega de la solicitud formal a la Gerencia de la compañía seleccionada para realizar el Proyecto (Ver Anexo D)														
2. Aprobación por parte del Gerente general de Crezcamos S.A. para realizar el proyecto en la compañía.														
3. Desarrollo de las encuestas que se realizarán en el 2017 en el desarrollo del proyecto														
4. Desarrollo del material que se														

empleará en las capacitaciones a los colaboradores														
5. Aplicación de encuesta vía formulario de Google que permitirá conocer la percepción de seguridad digital de cada colaborador administrativo que participle (Ver anexo E)														
6. Realización de la jornada de capacitación														
7. Analizar cuantitativamente la encuesta 1														
8. Envío de encuesta 2 para conocer las medidas de seguridad establecidas por los usuarios (Ver anexo F)														
9. Analizar														

cuantitativamente la encuesta 2														
10. Presentación del análisis de la encuesta a los participantes, así como recomendaciones seguridad														
11. Entrega de recomendaciones que se deben implementar en la compañía según los resultados obtenidos (Ver anexo G)														

9. DESARROLLO OBJETIVOS

El lunes 09 de octubre de 2017 se compartió a 100 personas, la encuesta en línea sobre conocimiento general en términos y temas de seguridad informática. Esta primera encuesta se llevó a cabo con la finalidad de identificar las distintas metodologías y métodos de ingeniería social a aplicar a los colaboradores de la IMF Crezcamos S.A. donde se eligió la más indicada para generar el mayor impacto positivo en los participantes y así se lograron obtener los mejores resultados de las capacitaciones y consejos impartidos durante las distintas jornadas realizadas; Los colaboradores se basaron en una lista generada por el área de formación de Crezcamos S.A. que disponía según el horario y tiempo de las personas participantes. Durante la semana se envió recordatorio a través del sistema de correo electrónico hasta completar la muestra. Las respuestas fueron tabuladas para posteriormente realizar un análisis cualitativo.

Se generó el contenido de la encuesta y con base en los resultados se diseñó la primera capacitación dirigida a 100 colaboradores administrativos de Crezcamos S.A. integrado por personal de las áreas críticas. La primera capacitación se realizó el día viernes 13 de octubre de 2017, duró aproximadamente una hora y fue dirigida un grupo de 25 personas donde se formó en seguridad digital enfocados en la ingeniera social. Como propuesta a la logística de la capacitación, se formaron dos grupos en la mañana y dos en la tarde.

Los colaboradores citados fueron informados por el área de formación de Crezcamos S.A. vía calendario, en donde se agregó la descripción de este proyecto de grado. Para ver las invitaciones ver ANEXO B.

Una vez aplicada la primera encuesta, la cual tenía por objeto la cuantificación del nivel de conocimiento de riesgo y la ingeniería social de los participantes, se procedió a realizar las charlas y capacitaciones con los conceptos y ejemplos de los distintos riesgos y prácticas habituales de los delincuentes para obtener información personal, así como la socialización de la actividad de ingeniería social

realizada, la cual permitió el diagnóstico aplicando metodologías de ingeniería social en los colaboradores administrativos de la IMF Crezcamos S.A., logrando que los participantes realizaran una autoevaluación del nivel de exposición de riesgo que consciente o inconscientemente aceptan al mantener una interacción con el mundo virtual y que permite a terceras personas realizar consultas de sus datos personales, familiares, sociales, económicos, culturales y profesionales. Al finalizar las actividades de socialización y capacitación se realizaron una serie de recomendaciones para implementar las estrategias de prevención de delitos informáticos e ingeniería social, así mismo, se fomentó la cultura organizacional, la cual se verá reflejada en la vida personal y laboral de los participantes.

10. METODOLOGIA Y TÉCNICA A APLICAR

Para el presente proyecto de grado, se diseñaron dos encuestas, las cuales fueron aplicadas en dos etapas: antes y después de la capacitación central. En medio de estas dos etapas se crearon y aplicaron tres técnicas de ataque a 10 personas que estuvieron en la capacitación:

- Se enviaron mensajes de texto anónimos a 5 personas a través de Whatsapp solicitando información relevante de cada individuo, sin individualizar o llegar a intimidar al participante.
  (la presente actividad no se pudo realizar, teniendo en cuenta las políticas de protección de datos personales de la compañía Crezcamos S.A., por lo que, los resultados obtenidos dentro del presente proyecto, obedecen a las dos actividades restantes)
- Se solicitó a 5 personas llenar una hoja de 25 preguntas sobre temas de cultura general, al final encontraron conmo sorpresa ataques a la invasión de la información que manejen estas personas.
- Se realizó a 10 personas una investigación a través de Google y sus buscadores para tratar de conocer la información pública más relevante que se pueda tener de ellas.
  (la actividad realizada demostró a los participantes, los riesgos asociados a los que está expuesta la información que comparten en redes sociales y distintas páginas de la web, además de la importancia de políticas de seguridad y privacidad para la protección de sus datos personales, los cuales se encuentran publicados en la red y son de fácil acceso a través de una consulta usando un motor de búsqueda como Google).

El temario contemplado tiene una duración máxima de una hora en cada capacitación y va a tratar los temas siguientes:

Tabla 3. Temario capacitación 1

1. **Esclavos tecnológicos**
2. **¿Estamos seguros?**
3. **Delitos informáticos**
4. **¿Qué es la ingeniería social?**
5. **Tipos de ingeniería social**
    a. Online
        i. Ciber Estafas
        ii. Suplantación de personas
        iii. Suplantación compañíarial
        iv. Phishing
        v. Telefónicas
        vi. Smishing
        vii. Vishing
    b. Personal
        i. Carding
        ii. Piratería
        iii. Keylogger
    c. Recolección urbana
        i. Ciber Grooming
        ii. Ciber extorsión
        iii. Incumplimiento de contratos
        iv. Divulgación de secretos compañíariales
        v. Sabotaje informático
6. **¿Cómo inicia la ingeniería social?**
7. **Avances tecnológicos comerciales**
8. **Validación social**

9. Fases de la ingeniería social a. Fase 1 – Investigación b. Fase 2 – Desarrollo de relación de confianza c. Fase 3 – Captura de información d. Fase 4 – Plan de acción

Fuente: Cristhian Camilo Monares Marin

Tabla 4. Temario capacitación 2

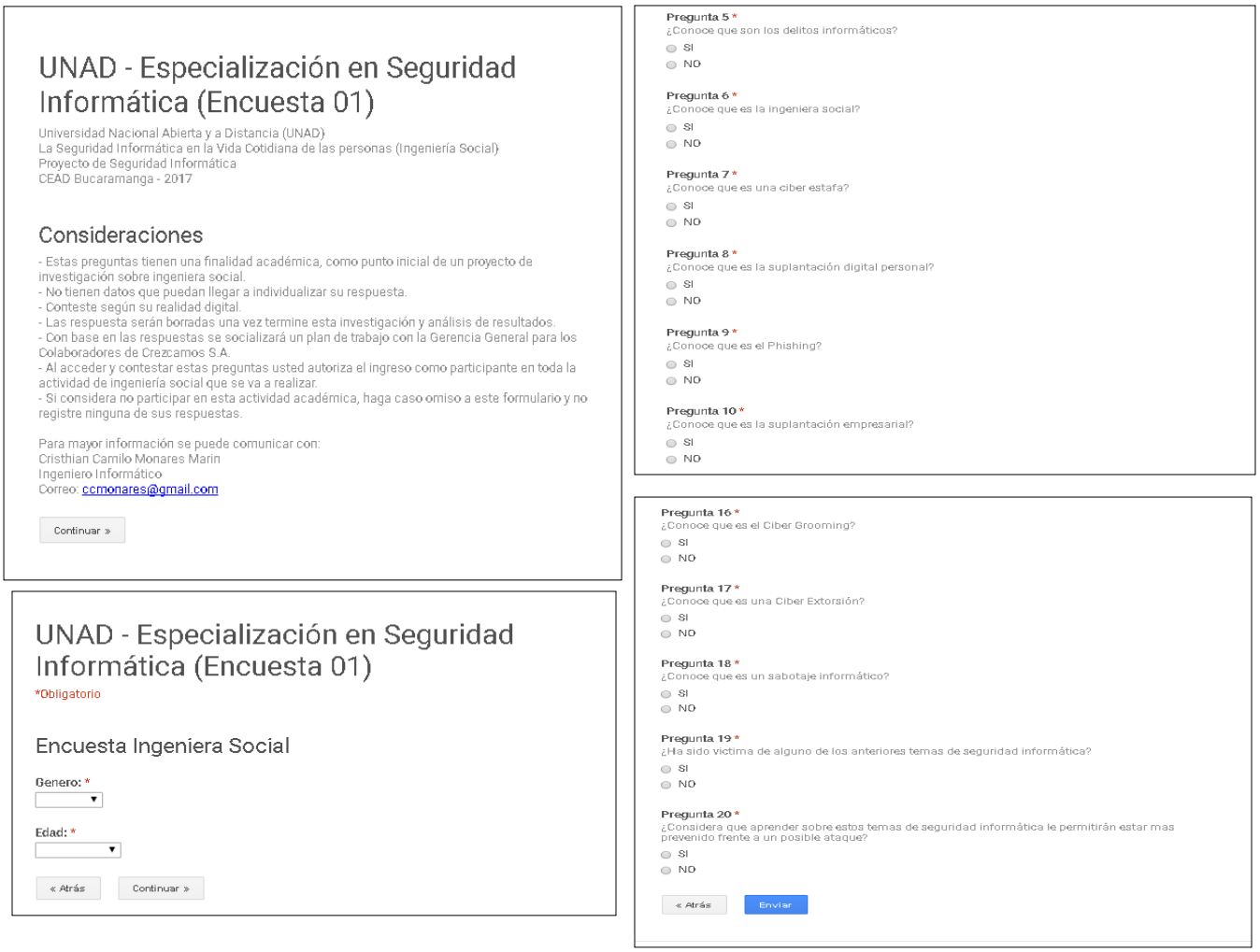
1. Resultados de la encuesta **2.** Resultados de las actividades realizadas a las 10 personas **3.** Ataques informáticos que son potencializados gracias a la ingeniería social **4.** Recomendaciones para no caer en la trampa de la ingeniería social

Fuente: Cristhian Camilo Monares Marin

11. DIAGNÓSTICO NIVEL DE CONOCIMIENTO DE LAS METODOLOGÍAS DE INGENIERÍA SOCIAL

Por medio de una primera encuesta se estableció la orientación que se le daría a las capacitaciones, teniendo en cuenta los resultados de la misma, en donde se tuvieron en cuenta los conceptos básicos del contexto de la Ingeniería social. La encuesta utilizada fue hecha por formulario de google, se socializó a los participantes de la muestra y se describe a continuación:

Ilustración 1. Formulario encuesta ingenieria social



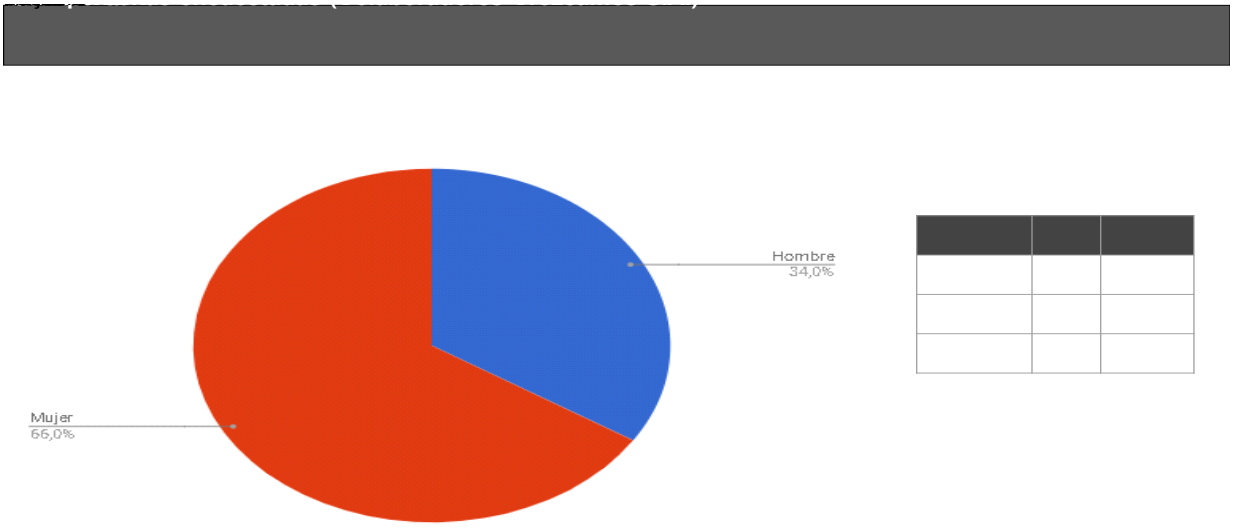
Fuente: Cristhian Camilo Monares Marín

10.1. REGISTRO, ANÁLISIS E INTERPRETACIÓN DE RESULTADOS DE LAS ENCUESTAS

A continuación, se relaciona el resultado de la encuesta 1, respondiendo al diagnóstico de cada uno de los conceptos asociados a la Ingeniería Social:

- **Total de encuestados**

Ilustración 2. Total de personas encuestadas.

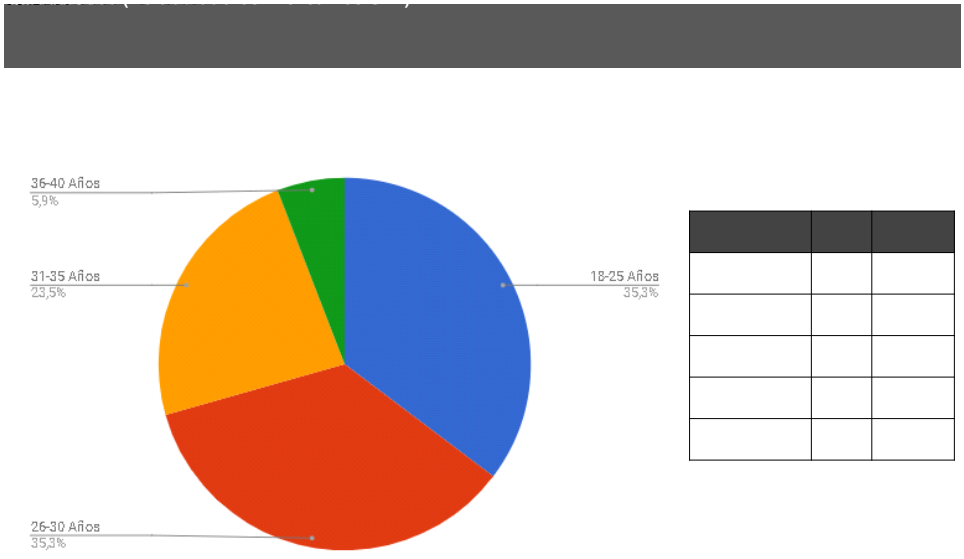


Fuente: Cristhian Camilo Monares Marín

Análisis: Se tomó una muestra de 100 personas a encuestar pertenecientes a la compañía Crezcamos S.A., obteniendo que de los encuestados el 66% correspondió al genero femenino y el restante 34% al género masculino.

- **Edad de los hombres encuestados**

Ilustración 3. Edades hombres encuestados.

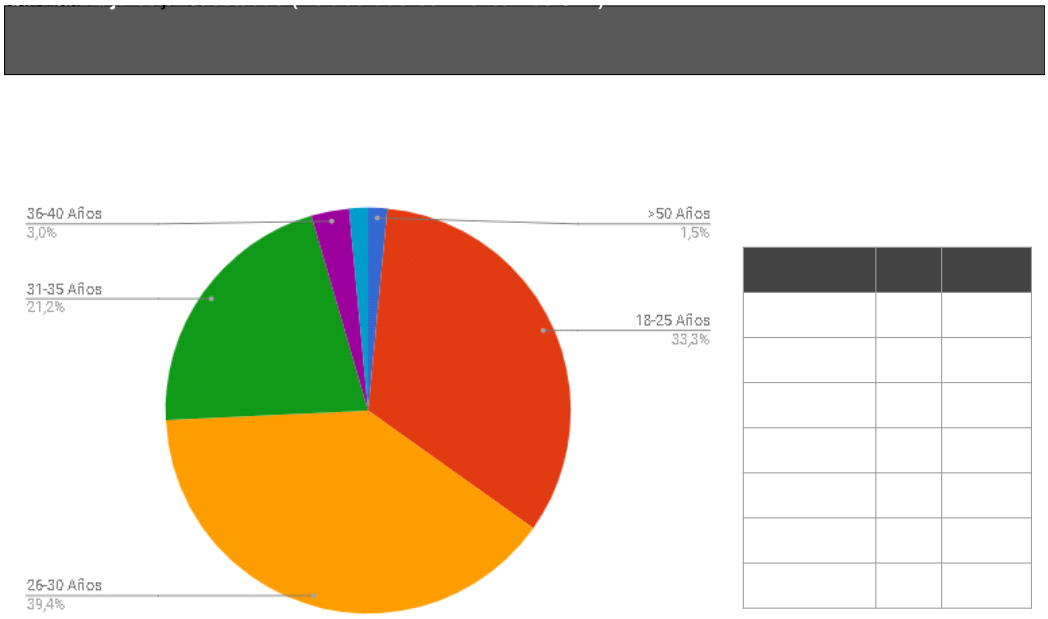


Fuente: Cristhian Camilo Monares Marin

Análisis: Se encontró que la población masculina encuestada se ubica en su mayoría, en las edades de 18 a 25 años y de 26 a 30 años, obteniendo un mismo porcentaje para ambos con un 35.3%, así mismo solo el 23.5% de los hombres encuestados se ubican entre los 31 y 35 años y tan solo el 5.9% de los hombres encuestados es mayor de 36 años.

- **Edad de las mujeres encuestadas**

Ilustración 4. Edades mujeres encuestadas.

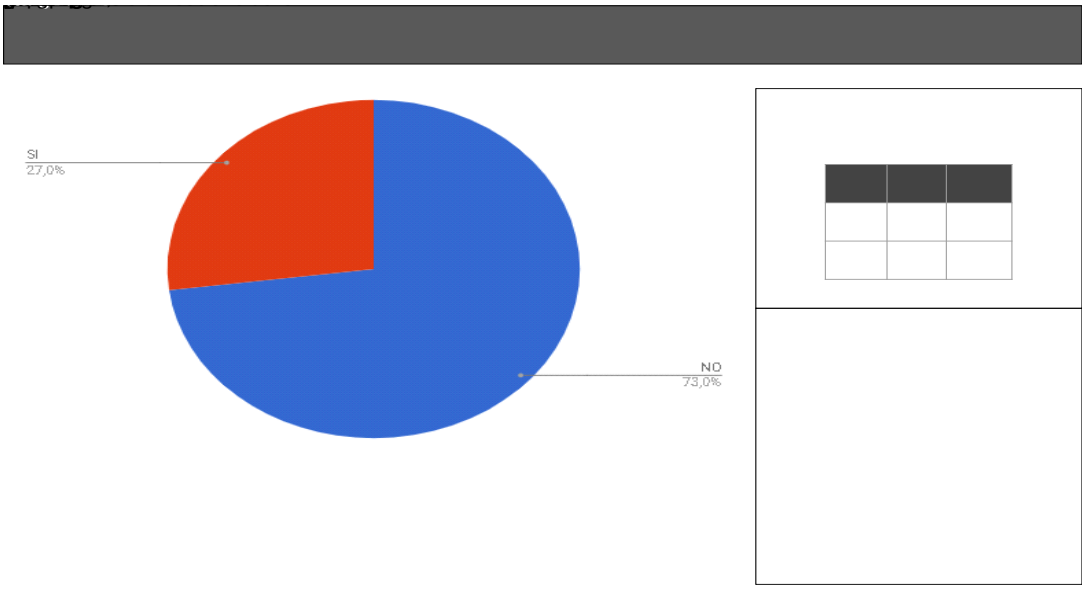


Fuente: Cristhian Camilo Monares Marín

Análisis: Se encontró que la población femenina encuestada se ubica en su mayoría, en las edades de 26 a 30 años con un 39.4%, de esta manera, el 33.3% de las mujeres encuestadas corresponden a la edad de entre 18 y 25 años, así mismo, solo el 1.5% de los mujeres encuestadas se ubican entre los 41 y 45 años y el 1.5% es mayor a 50 años. El restante 21.2% tienen entre 31 a 35 años de edad.

- **¿Se considera un esclavo de la tecnología?**

Ilustración 5. Pregunta 01.

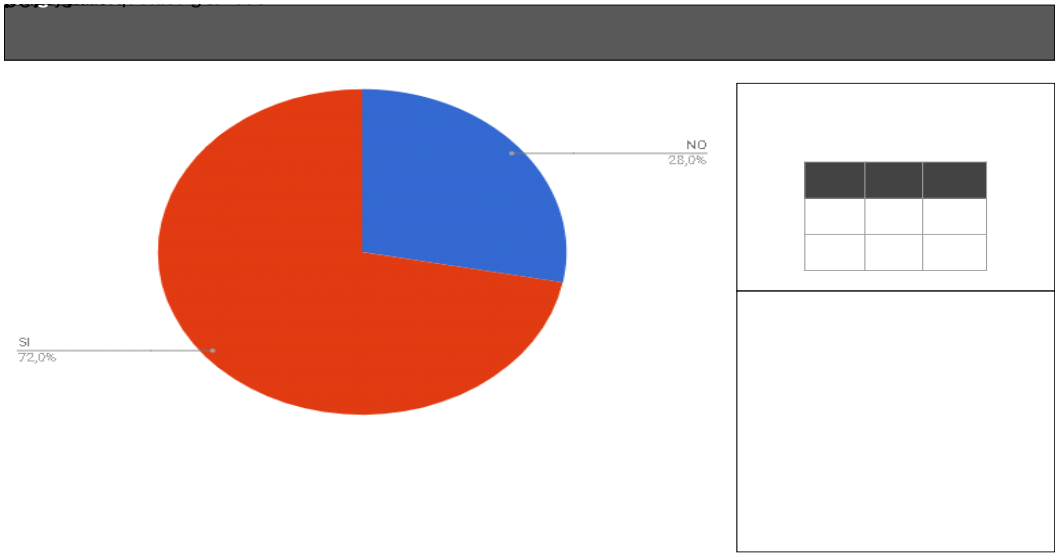


Fuente: Cristhian Camilo Monares Marín

Análisis: El 73% de las personas NO se consideran esclavos tecnológicos, 22 son Hombres y 51 son Mujeres. El 27% de las personas SÍ se consideran esclavos tecnológicos, 12 son Hombres y 15 son Mujeres.

- **¿Considera que tiene un buen manejo de su vida digital personal?**

Ilustración 6. Pregunta 02.



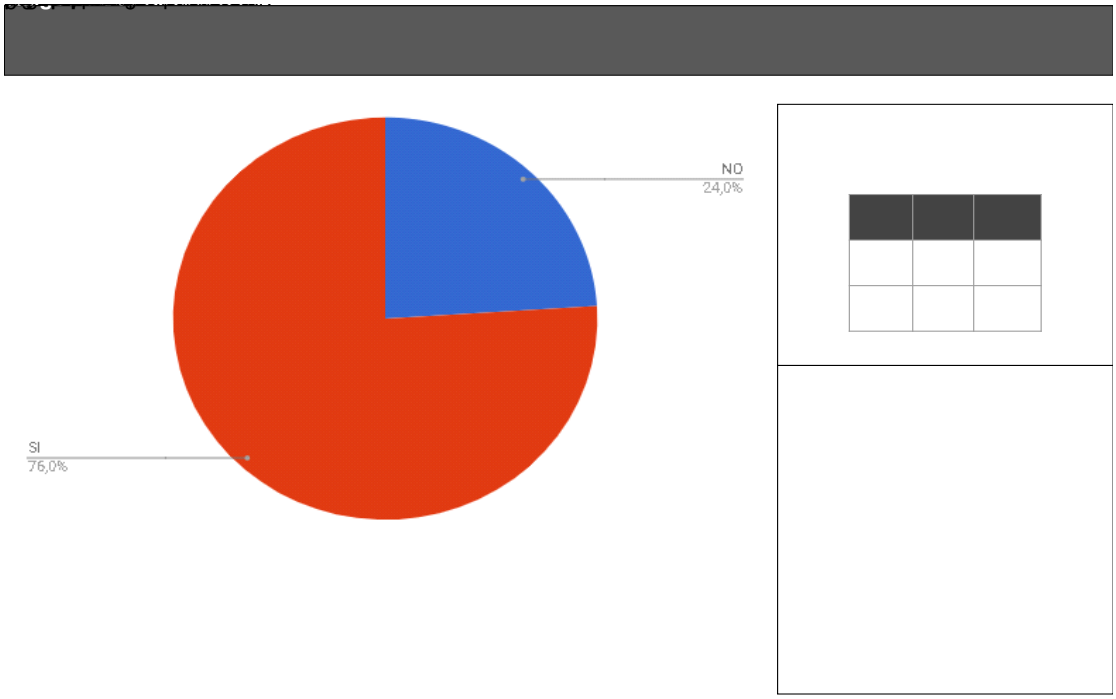
Fuente: Cristhian Camilo Monares Marín

Análisis: El 28% de las personas NO consideran tener un buen manejo de su vida digital, 10 son Hombres y 18 son Mujeres.

El 72% de las personas SI consideran tener un buen manejo de su vida digital, 24 son Hombres y 48 son Mujeres.

- **¿Considera que puede ser víctima de Ingeniería Social?**

Ilustración 7. Pregunta 03.



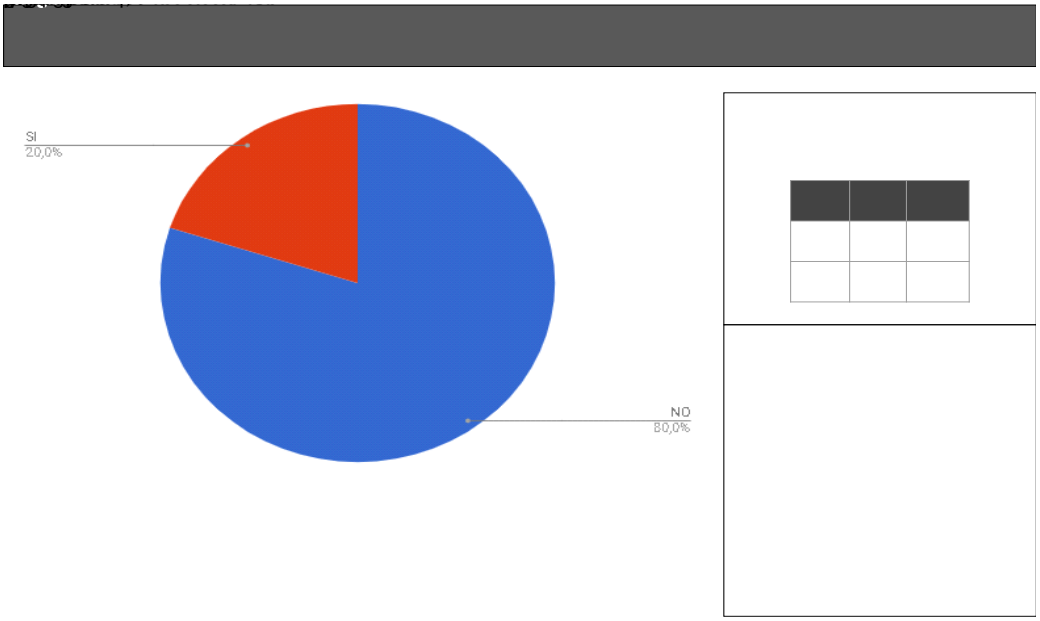
Fuente: Cristhian Camilo Monares Marín

Análisis: El 24% de las personas NO consideran que pueden ser víctimas de ingeniería social, 10 son Hombres y 14 son Mujeres.

El 76% de las personas SI consideran que pueden ser víctimas de ingeniería social, 24 son Hombres y 52 son Mujeres.

- **¿Considera que tiene medidas de seguridad suficientes en su vida digital?**

Ilustración 8. Pregunta 04.



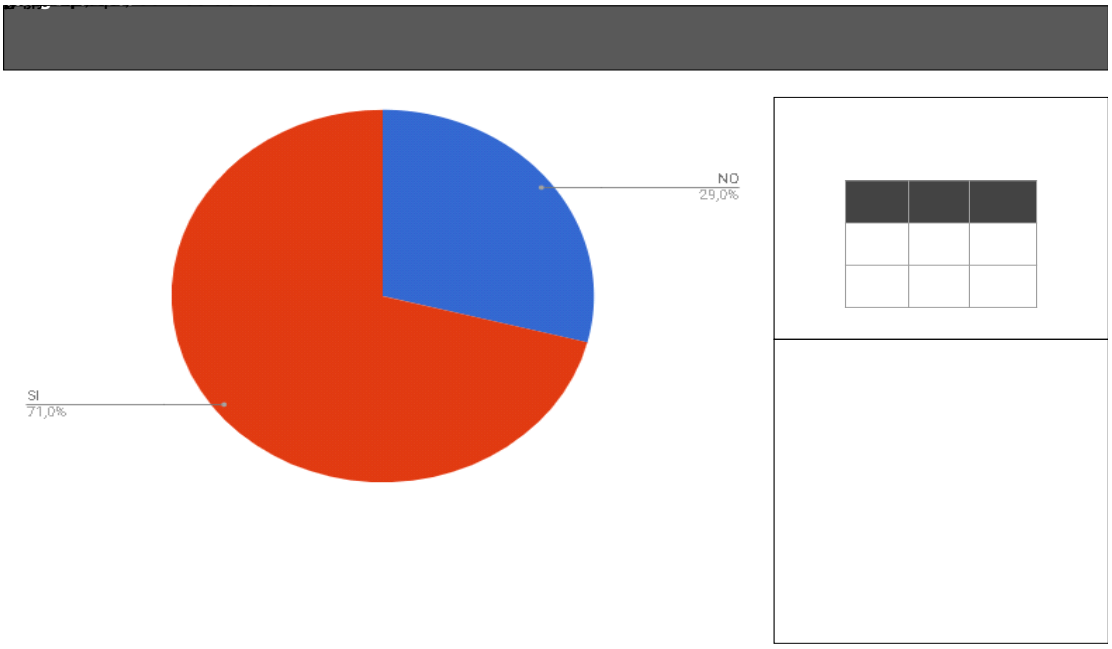
Fuente: Cristhian Camilo Monares Marín

Análisis: El 80% de las personas NO consideran tener medidas de seguridad suficientes en su vida digital, 26 son Hombres y 54 son Mujeres.

El 20% de las personas SI consideran tener medidas de seguridad suficientes en su vida digital, 8 son Hombres y 12 son Mujeres.

- **¿Conoce qué son los delitos informáticos?**

Ilustración 9. Pregunta 05.



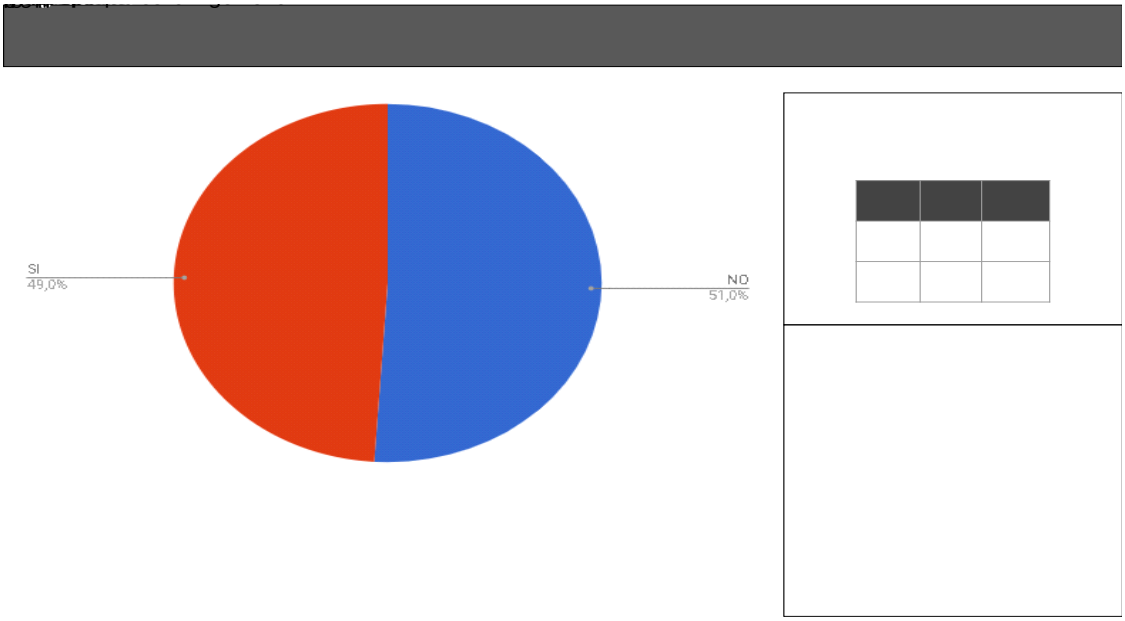
Fuente: Cristhian Camilo Monares Marín

Análisis: El 29% de las personas NO conocen que son delitos informáticos, 5 son Hombres y 24 son Mujeres.

El 71% de las personas SI conocen que son delitos informáticos, 29 son Hombres y 42 son Mujeres.

- **¿Conoce qué es la Ingeniería Social?**

Ilustración 10. Pregunta 06.



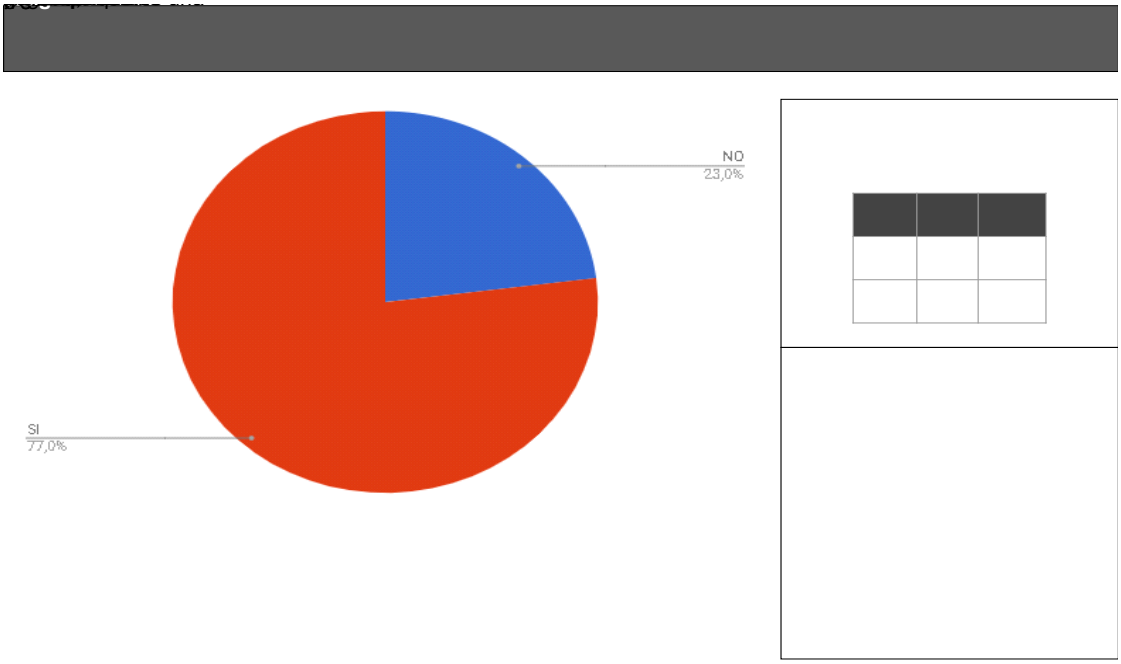
Fuente: Cristhian Camilo Monares Marín

Análisis: El 51% de las personas NO conocen que es la ingeniería social, 15 son Hombres y 36 son Mujeres.

El 49% de las personas SI conocen que es la ingeniería social, 19 son Hombres y 30 son Mujeres.

- **¿Conoce qué es una ciberestafa?**

Ilustración 11. Pregunta 07.



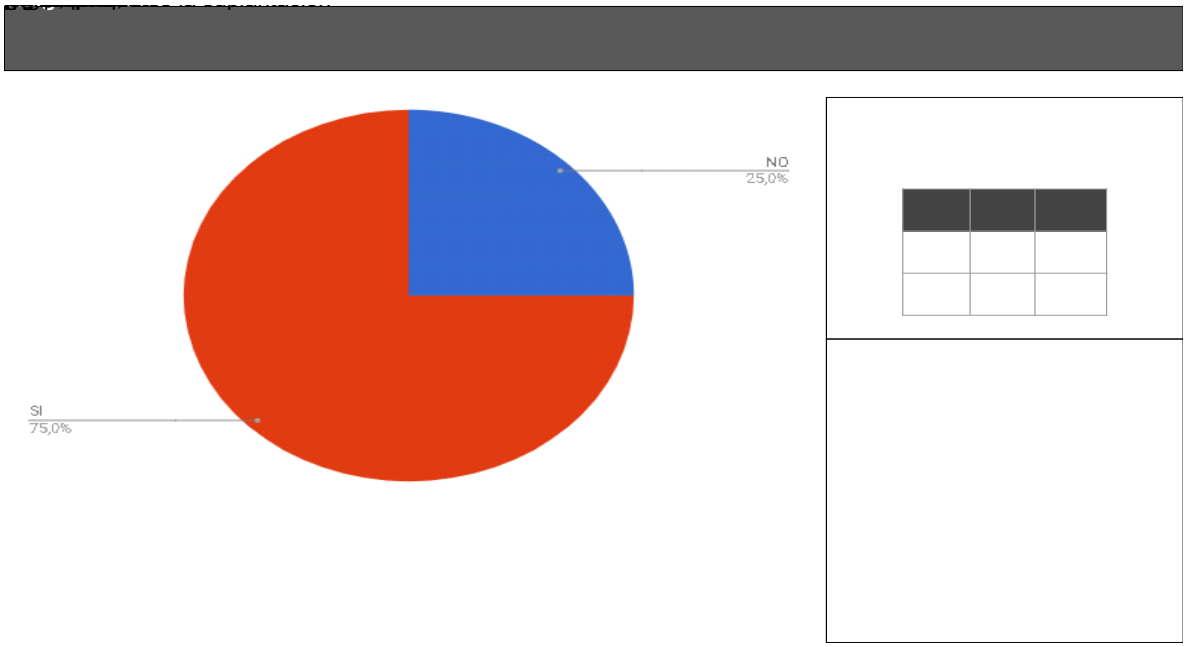
Fuente: Cristhian Camilo Monares Marín

Análisis: El 23% de las personas NO conocen que es una ciberestafa, 5 son Hombres y 18 son Mujeres.

El 77% de las personas SI conocen que es una ciberestafa, 29 son Hombres y 48 son Mujeres.

- **¿Conoce qué es una suplantación digital personal?**

Ilustración 12. Pregunta 08.



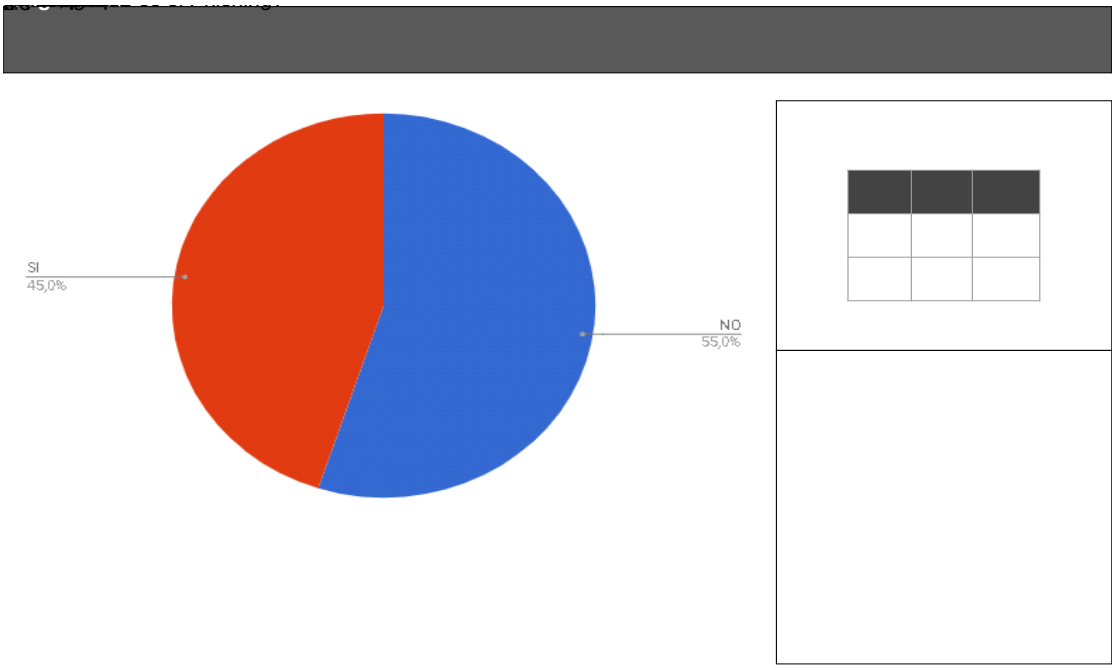
Fuente: Cristhian Camilo Monares Marín

Análisis: El 25% de las personas NO conocen que es una suplantación digital personal, 5 son Hombres y 20 son Mujeres.

El 75 % de las personas SI conocen que es una suplantación digital personal, 29 son Hombres y 46 son Mujeres.

- **¿Conoce qué es Phishing?**

Ilustración 13. Pregunta 09.

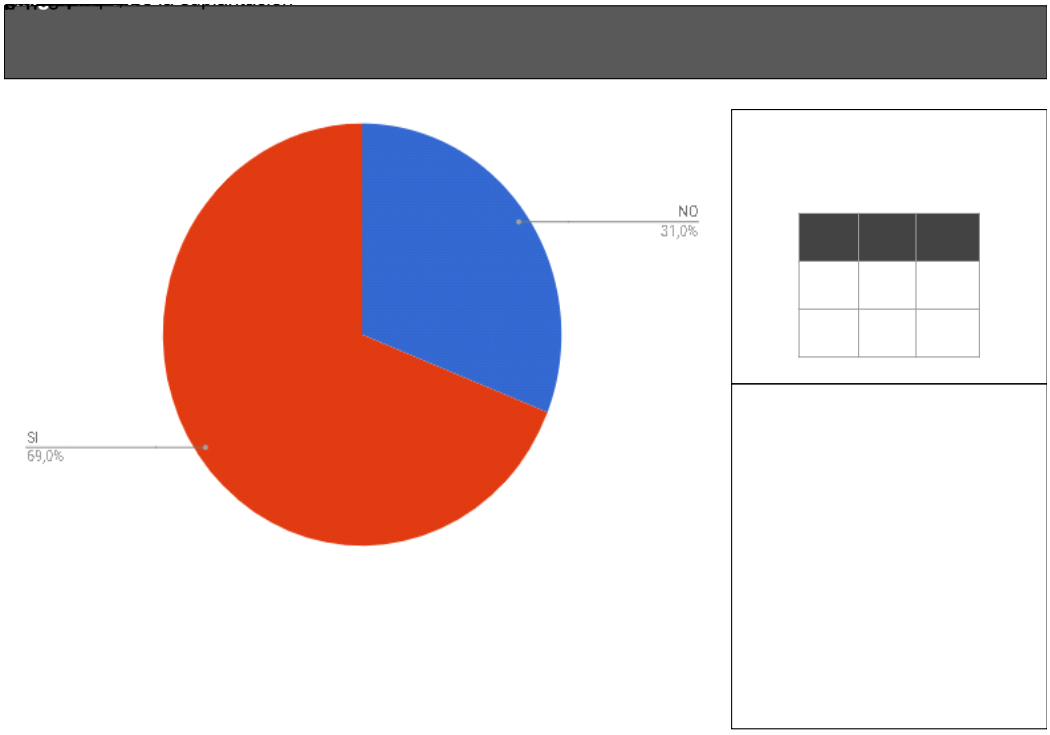


Fuente: Cristhian Camilo Monares Marín

Análisis: El 55 % de las personas NO conocen que es el Phishing, 15 son Hombres y 40 son Mujeres. El 45 % de las personas SI conocen que es el Phishing, 19 son Hombres y 26 son Mujeres.

- **¿Conoce qué es la suplantación empresarial?**

Ilustración 14. Pregunta 10.



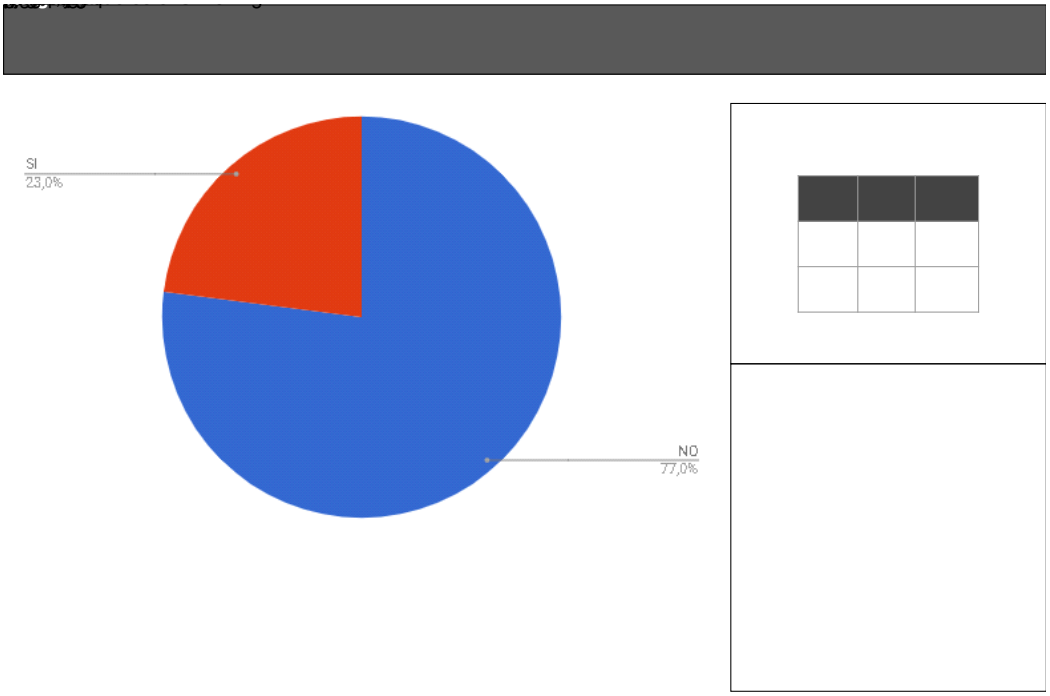
Fuente: Cristhian Camilo Monares Marín

Análisis: El 31 % de las personas NO conocen que es la suplantación empresarial, 6 son Hombres y 25 son Mujeres.

El 69 % de las personas SI conocen que es la suplantación empresarial, 28 son Hombres y 41 son Mujeres.

- **¿Conoce qué es el Smishing?**

Ilustración 15. Pregunta 11.



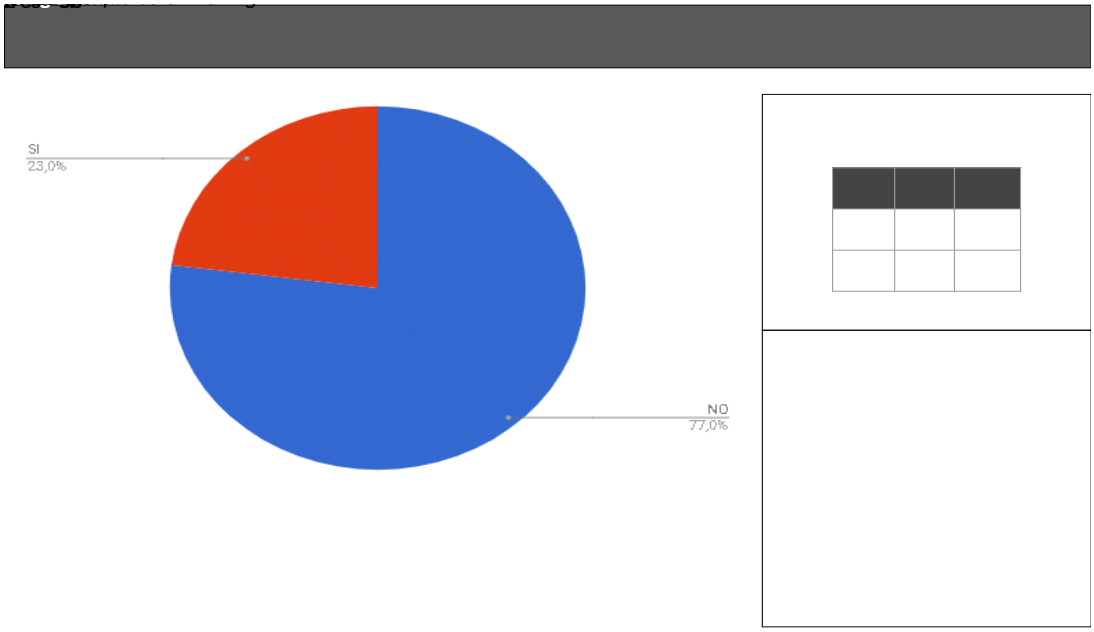
Fuente: Cristhian Camilo Monares Marín

Análisis: El 77 % de las personas NO conocen que es el Smishing, 22 son Hombres y 55 son Mujeres.

El 23 % de las personas SI conocen que es el Smishing, 12 son Hombres y 11 son Mujeres.

- **¿Conoce qué es Vishing?**

Ilustración 16. Pregunta 12.



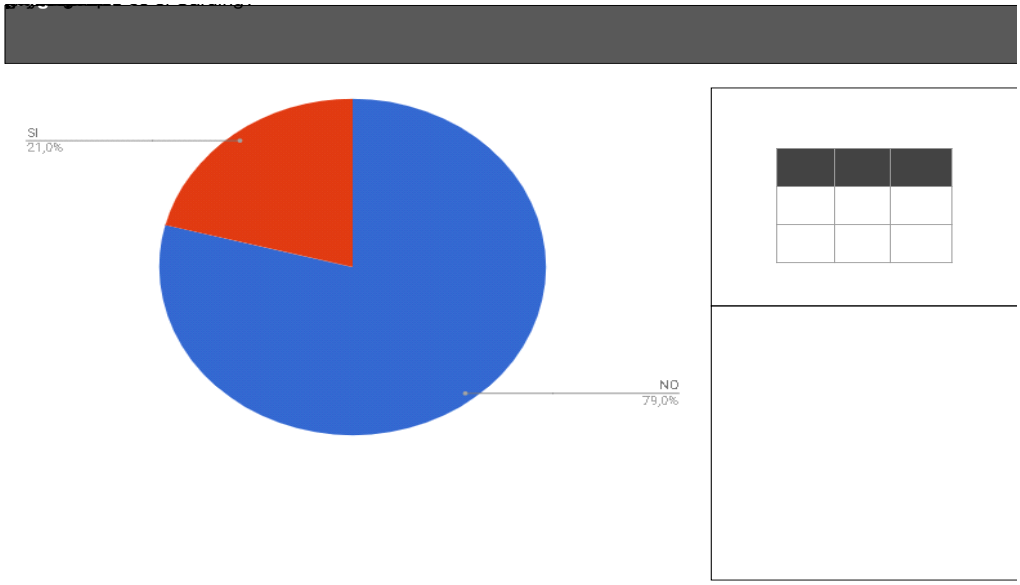
Fuente: Cristhian Camilo Monares Marín

Análisis: Del 77 % de las personas NO conocen que es el Vishing, 23 son Hombres y 54 son Mujeres.

El 23 % de las personas SI conocen que es el Vishing, 11 son Hombres y 12 son Mujeres.

- **¿Conoce qué es el carding?**

Ilustración 17. Pregunta 13.



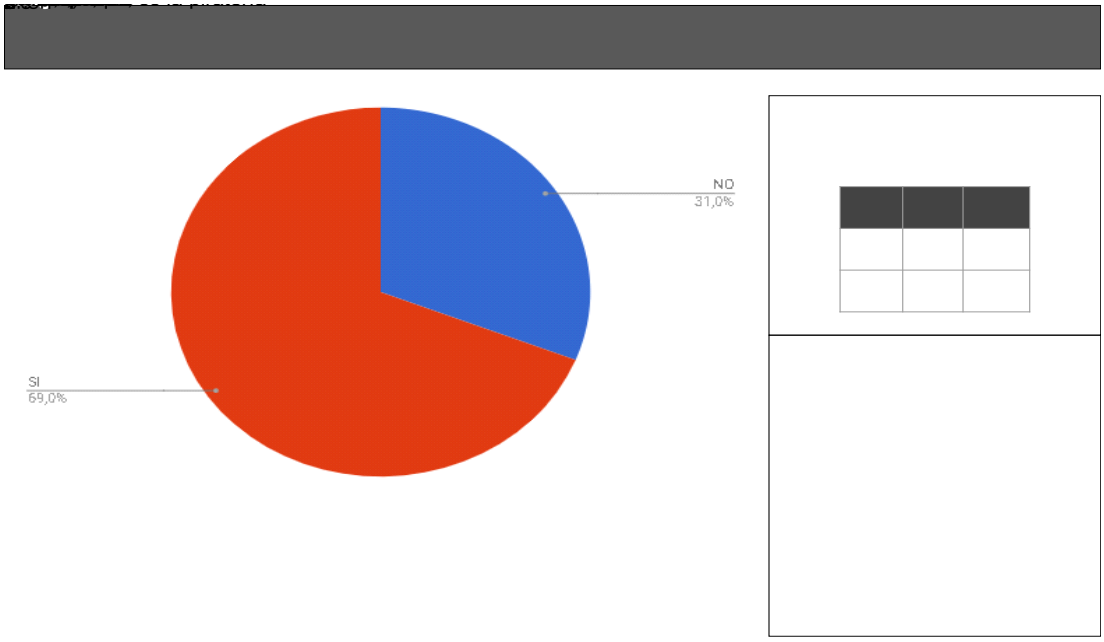
Fuente: Cristhian Camilo Monares Marín

Análisis: El 79 % de las personas NO conocen que es el Carding, 24 son Hombres y 55 son Mujeres.

El 21 % de las personas SI conocen que es el Carding, 10 son Hombres y 11 son mujeres.

- **¿Conoce qué es la piratería digital?**

Ilustración 18. Pregunta 14.



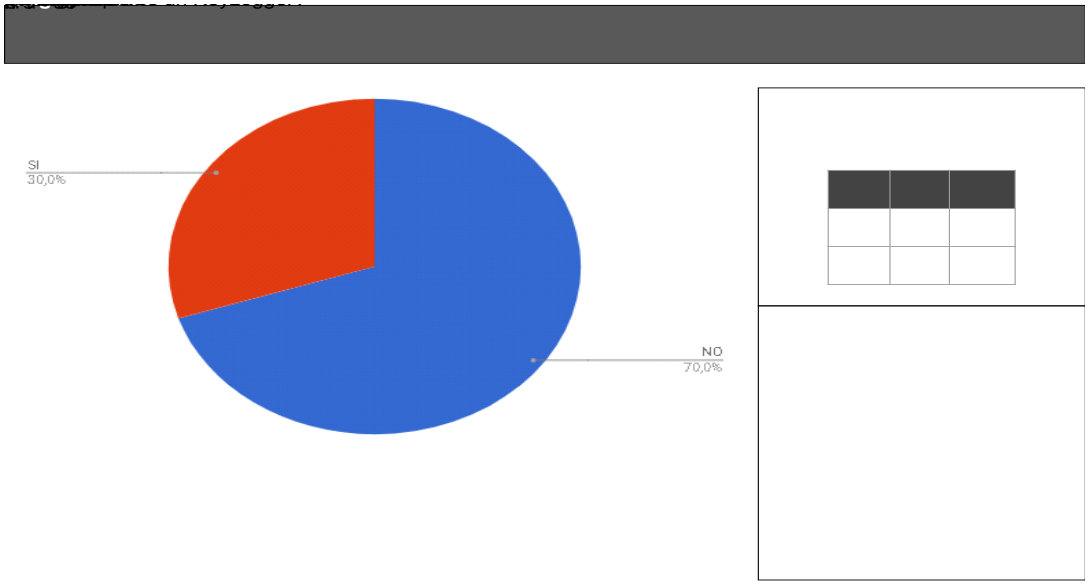
Fuente: Cristhian Camilo Monares Marín

Análisis: El 31 % de las personas NO conocen que es el piratería digital, 9 son Hombres y 22 son Mujeres.

El 69 % de las personas SI conocen que es el piratería digital, 25 son Hombres y 44 son Mujeres.

- **¿Conoce qué es un Keylogger?**

Ilustración 19. Pregunta 15.



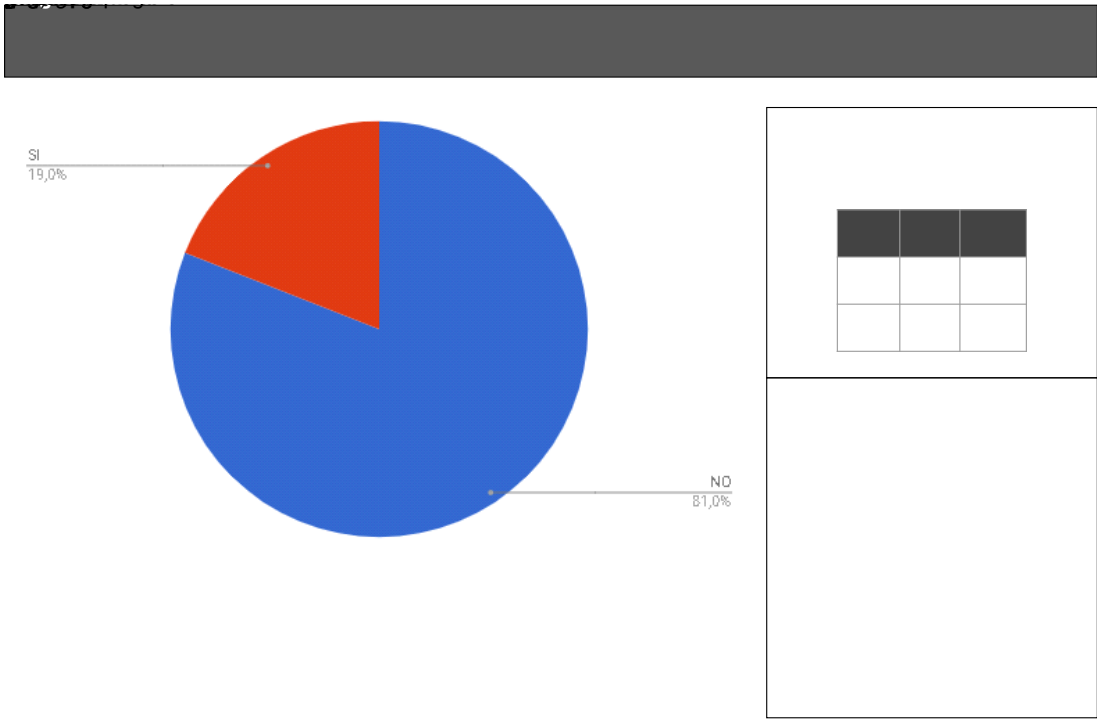
Fuente: Cristhian Camilo Monares Marín

Análisis: Del 70 % de las personas que NO conocen que es un KeyLogger, 20 son Hombres y 50 son Mujeres.

Del 30 % de las personas SI conocen que es un KeyLogger, 14 son Hombres y 16 son Mujeres.

- **¿Conoce qué es el Grooming?**

Ilustración 20. Pregunta 16.



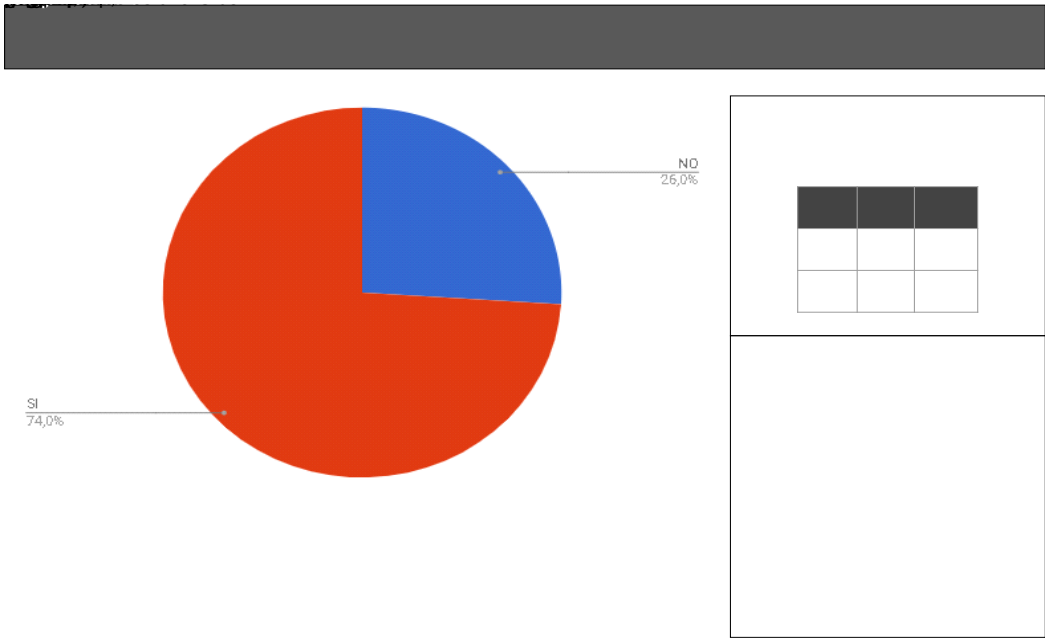
Fuente: Cristhian Camilo Monares Marín

Análisis: El 81 % de las personas NO conocen que es el Cibergrooming, 25 son Hombres y 56 son Mujeres.

El 19 % de las personas SI conocen que es el Cibergrooming, 9 son Hombres y 10 son Mujeres.

- **¿Conoce qué es una ciberextorsión?**

Ilustración 21. Pregunta 17.



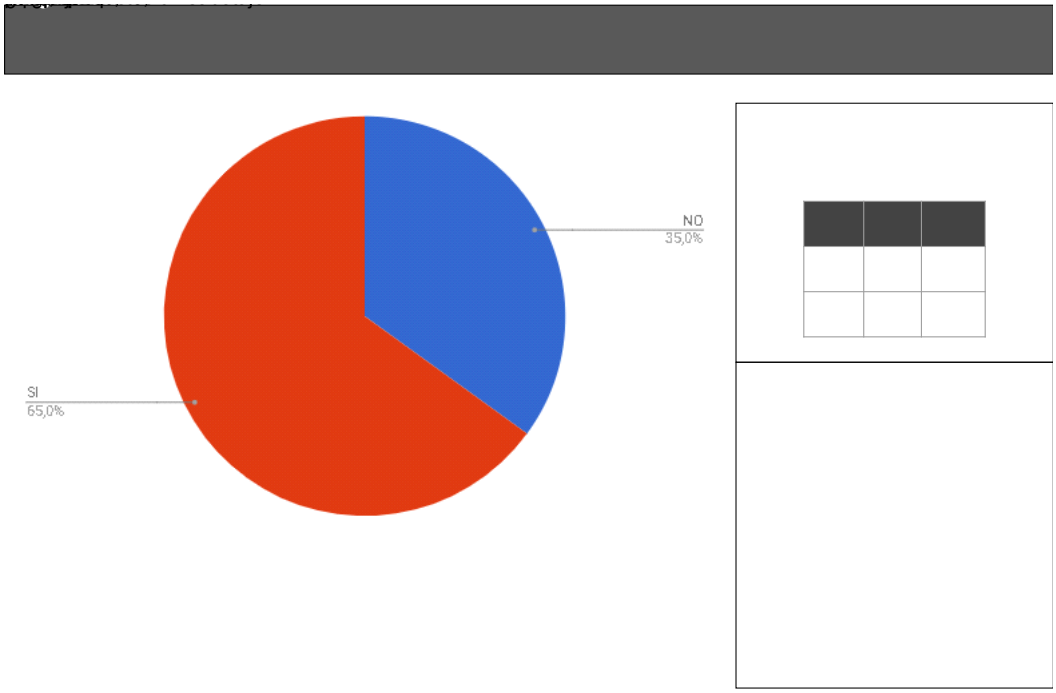
Fuente: Cristhian Camilo Monares Marín

Análisis: El 26 % de las personas NO conocen que es una Ciber Extorsión, 5 son Hombres y 21 son Mujeres.

El 74 % de las personas SI conocen que es una Ciber Extorsión, 29 son Hombres y 45 son Mujeres.

- **¿Conoce qué es un sabotaje informático?**

Ilustración 22. Pregunta 18.



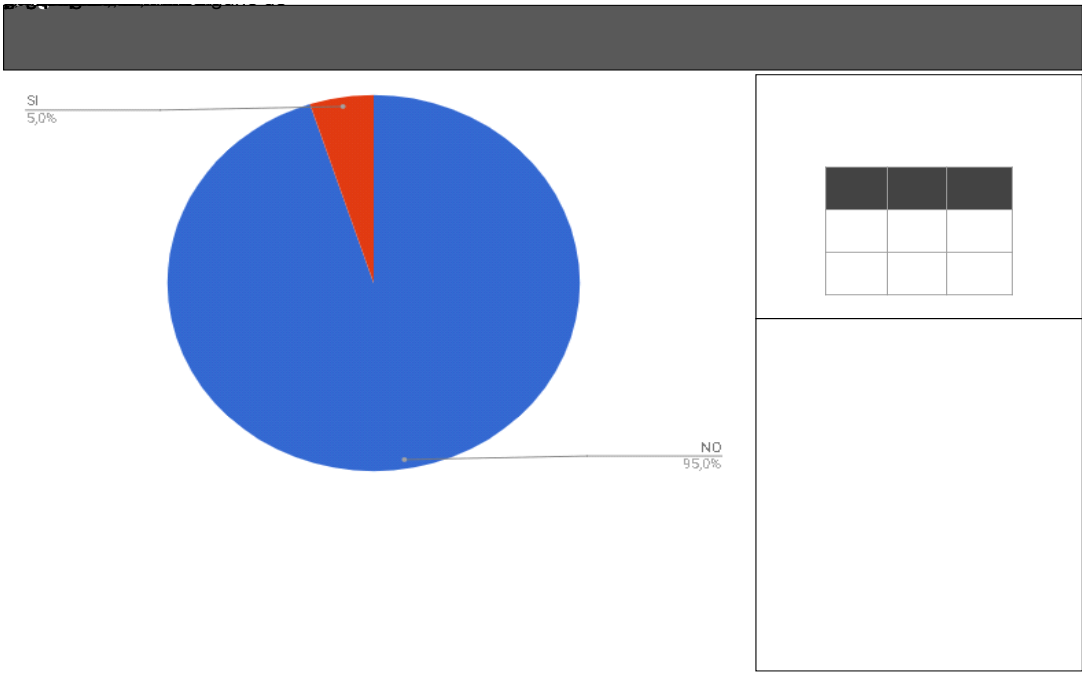
Fuente: Cristhian Camilo Monares Marín

Análisis: El 35 % de las personas NO conocen que es un sabotaje informático, 7 son Hombres y 28 son Mujeres.

El 65 % de las personas SI conocen que es un sabotaje informático, 27 son Hombres y 38 son Mujeres.

- **¿Ha sido víctima de alguno de los anteriores temas de seguridad informática?**

Ilustración 23. Pregunta 19.



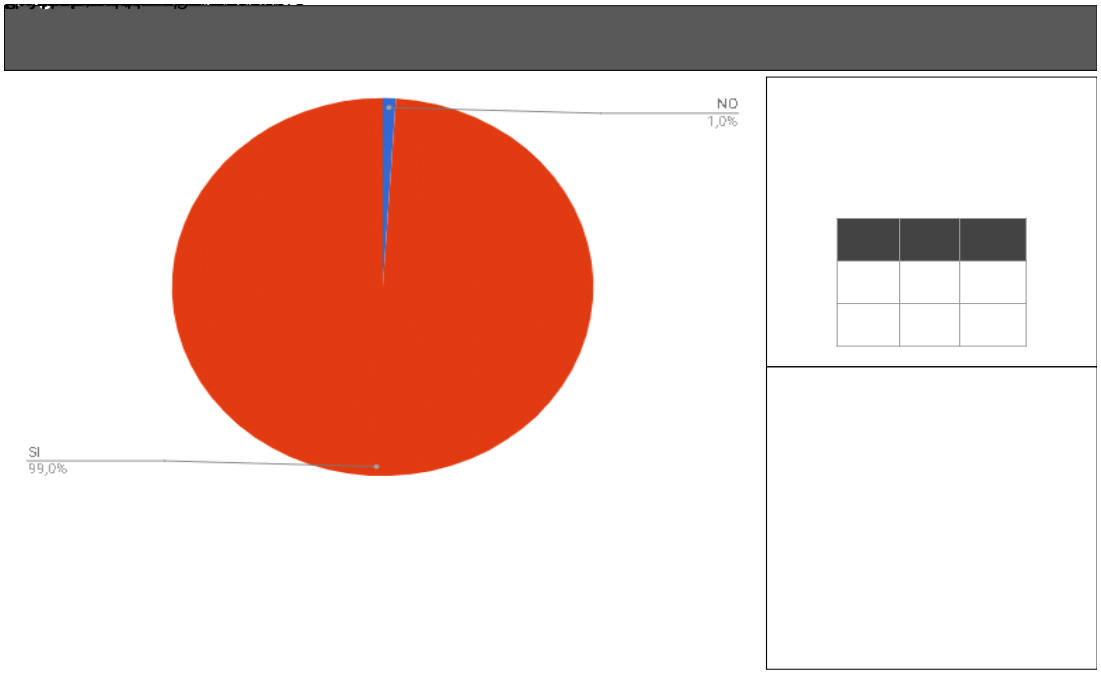
Fuente: Cristhian Camilo Monares Marín

Análisis: El 95 % de las personas NO han sido víctima de alguno de los anteriores temas de seguridad informática nombrados, 33 son Hombres y 62 son Mujeres.

El 5 % de las personas que SI han sido víctima de alguno de los anteriores temas de seguridad informática nombrados, 1 son Hombres y 4 son Mujeres.

- **¿Considera que aprender sobre estos temas de seguridad informática le permitirán estar más prevenido frente a un posible ataque?**

Ilustración 24. Pregunta 20.



Fuente: Cristhian Camilo Monares Marín

Análisis: El 1 % de las personas NO considera que aprender sobre estos temas de seguridad informática le permitirán estar más prevenido frente a un posible ataque, es una Mujer.

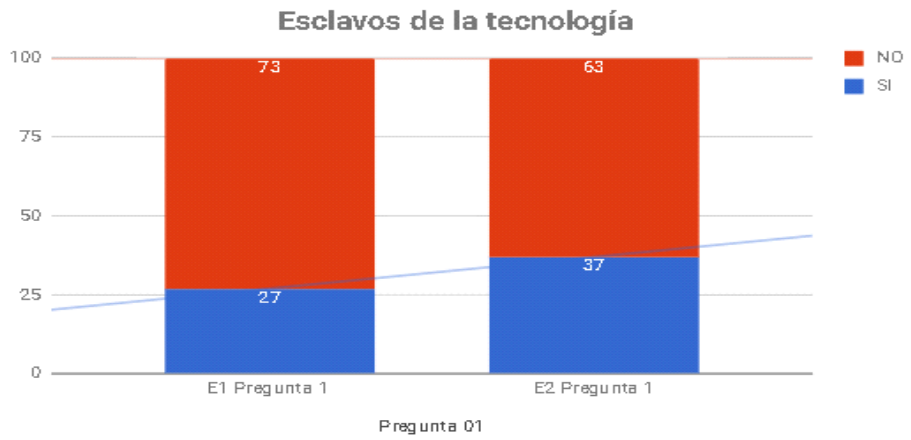
El 99 % de las personas que SI considera que aprender sobre estos temas de seguridad informática le permitirán estar más prevenido frente a un posible ataque, 34 son Hombres y 65 son Mujeres.

10.2. RELACIÓN ENTRE LAS DOS ENCUESTAS Y LA CAPACITACIÓN

Luego de realizada la encuesta y la capacitación 1, de orientación en el conocimiento de la seguridad informática, de esta forma, se aplicó una segunda encuesta con las mismas preguntas para detectar las brechas llenadas frente a cada una de las temáticas. De esta manera se obtuvo lo siguiente:

- **Esclavos de la tecnología**

Ilustración 25. Resultados comparativa pregunta 01.

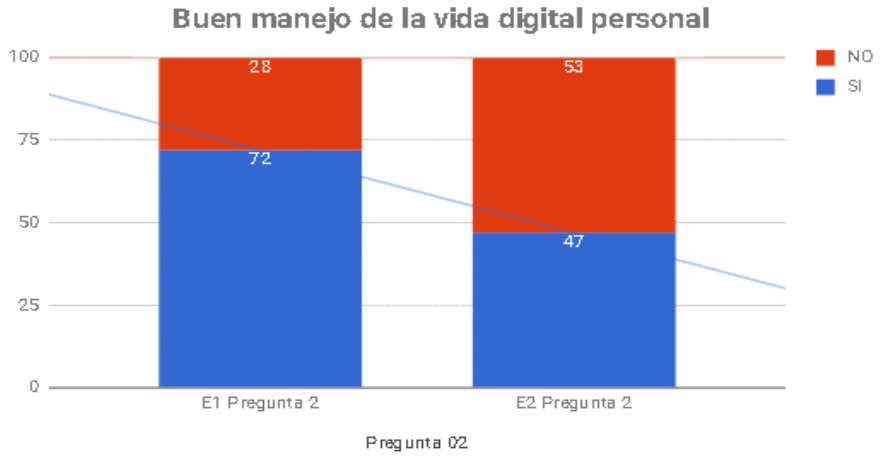


Fuente: Cristhian Camilo Monares Marín

Análisis: Se evidencia que el grupo de muestra varió la forma en la que se consideran a sí mismos como esclavos de la tecnología con posterioridad a la capacitación presentada, viendo un incremento equivalente al 10% de éstas personas.

- **Buen manejo de la vida digital personal**

Ilustración 26. Resultados comparativa pregunta 02.

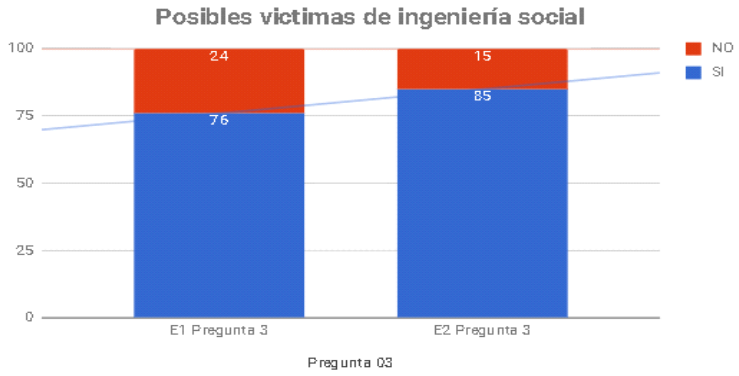


Fuente: Cristhian Camilo Monares Marín

Análisis: Se evidencia en la gráfica una disminución en el porcentaje de personas que consideraban dar un buen manejo de su vida personal en la red, por lo que, gracias a la capacitación impartida, viendo un impacto del 25% de las personas.

- **Posibles víctimas de Ingeniería Social**

Ilustración 27. Resultados comparativa pregunta 03.

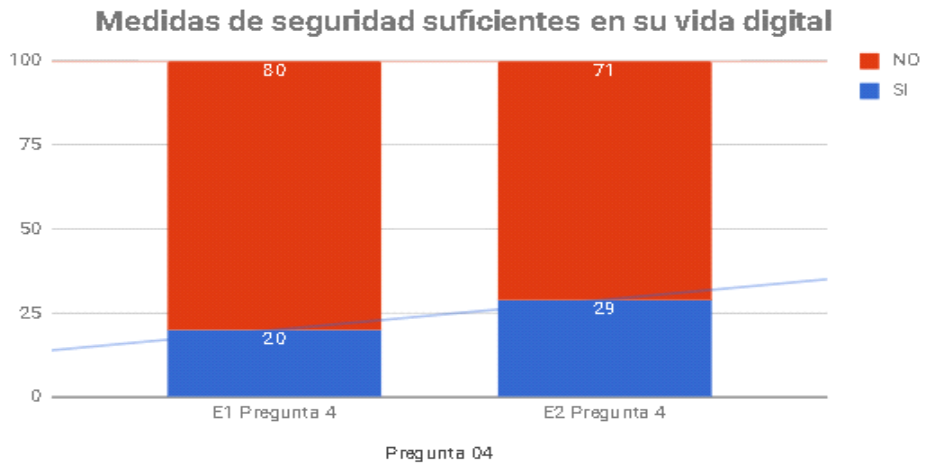


Fuente: Cristhian Camilo Monares Marín

Análisis: Se evidencia una disminución en el porcentaje de personas que consideraban poco susceptibles a ser víctimas de la ingeniería social, por lo que, gracias a la capacitación impartida, se observa un impacto del 9% de personas que se concientizaron acerca de la posibilidad de ser víctimas de la ingeniería social.

- **Medidas de seguridad suficientes en su vida digital**

Ilustración 28. Resultados comparativa pregunta 04.

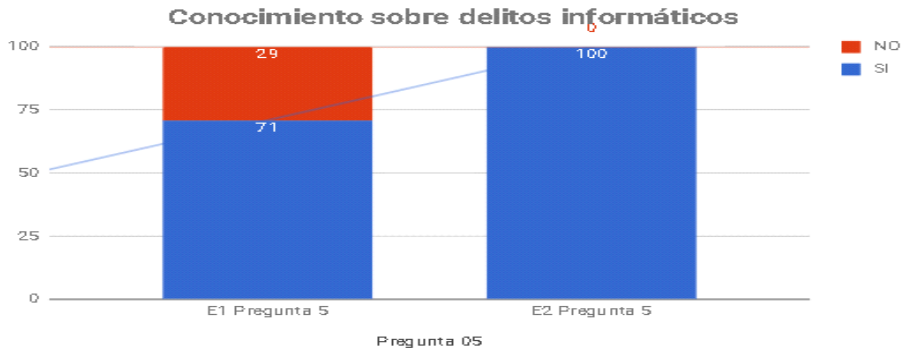


Fuente: Cristhian Camilo Monares Marín

Se evidencia en la gráfica un aumento en el porcentaje de personas que consideran la implementación de medidas de seguridad para la protección de su vida digital, por lo que, gracias a la capacitación impartida, viendo un impacto del 9% en las personas.

- **Conocimiento sobre delitos informáticos**

Ilustración 29. Resultados comparativa pregunta 05.

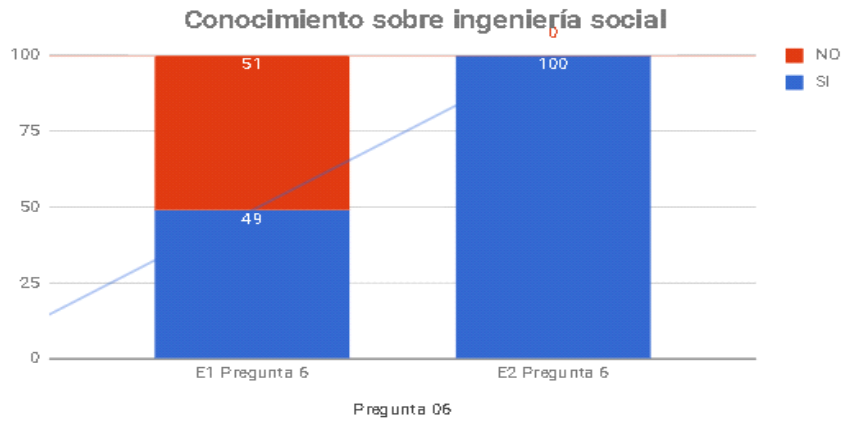


Fuente: Cristhian Camilo Monares Marín

Análisis: Se evidencia incremento en el porcentaje de personas correspondiente al nivel de conocimiento y alcance de los distintos tipos de delitos informáticos, por lo que, gracias a la capacitación impartida, viendo un impacto del 29% en la personas.

- **Conocimiento sobre Ingeniería Social**

Ilustración 30. Resultados comparativa pregunta 06.

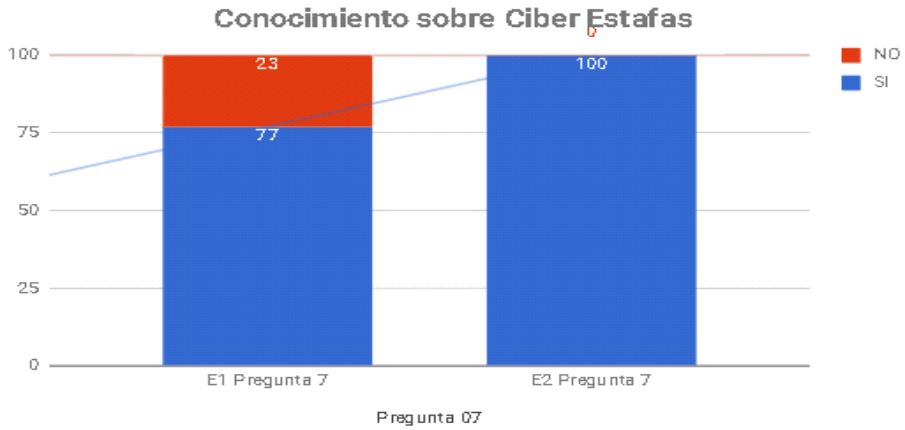


Fuente: Cristhian Camilo Monares Marín

Análisis: Gracias a la implementación de la capacitación, se logró un incremento equivalente al 51% de las personas, acerca del conocimiento sobre la ingeniería social y sus alcances.

- **Conocimiento sobre Ciberestafas**

Ilustración 31. Resultados comparativa pregunta 07.

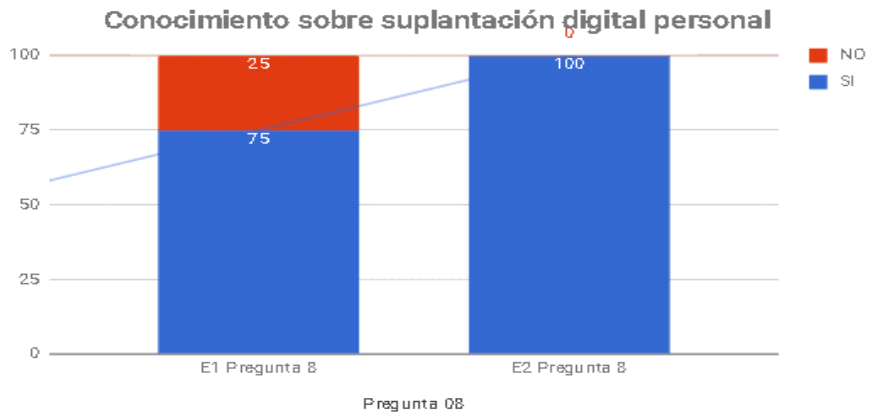


Fuente: Cristhian Camilo Monares Marín

Análisis: En la gráfica se refleja el incremento del nivel de conocimiento acerca de las Ciber Estafas, por lo que se logró un incremento del 23%, logrando así que la totalidad de las personas pertenecientes al grupo de muestra conocieran esta modalidad de estafa.

- **Conocimiento sobre suplantación digital personal**

Ilustración 32. Resultados comparativa pregunta 08.

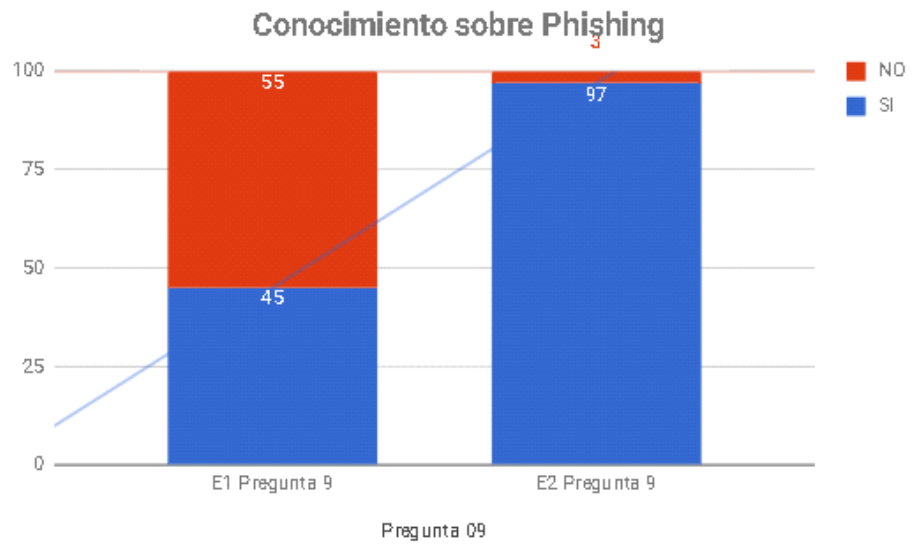


Fuente: Cristhian Camilo Monares Marín

Análisis: En la gráfica se refleja el aumento del nivel de conocimiento acerca de la suplantación digital, por lo que se logró un incremento del 25%, gracias a la implementación de las capacitaciones, logrando así que la totalidad de las personas pertenecientes al grupo de muestra conocieran los riesgos de la suplantación personal en la web.

- **Conocimiento sobre Phishing**

Ilustración 33. Resultados comparativa pregunta 09.



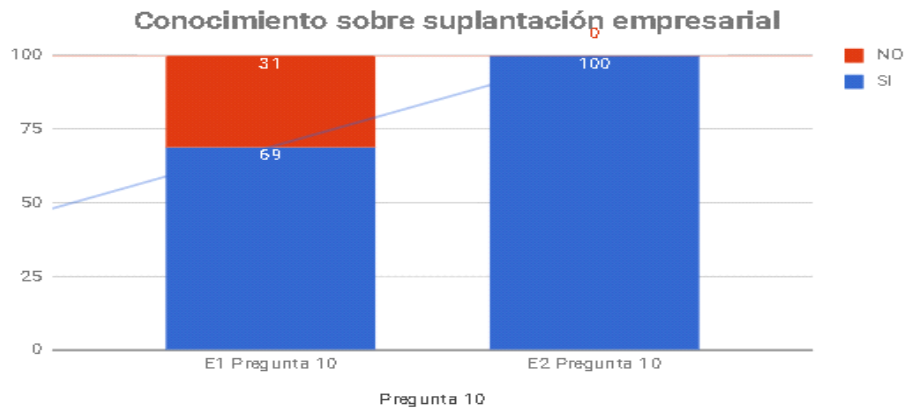
Fuente: Cristhian Camilo Monares Marín

Análisis: En la gráfica se refleja el incremento del nivel de conocimiento acerca del Phising, por lo que se logró un incremento del 52%, logrando así que casi la

totalidad de las personas pertenecientes al grupo de muestra conocieran este factor de riesgo al navegar y utilizar el internet.

- **Conocimiento sobre suplantación empresarial**

Ilustración 34. Resultados comparativa pregunta 10.

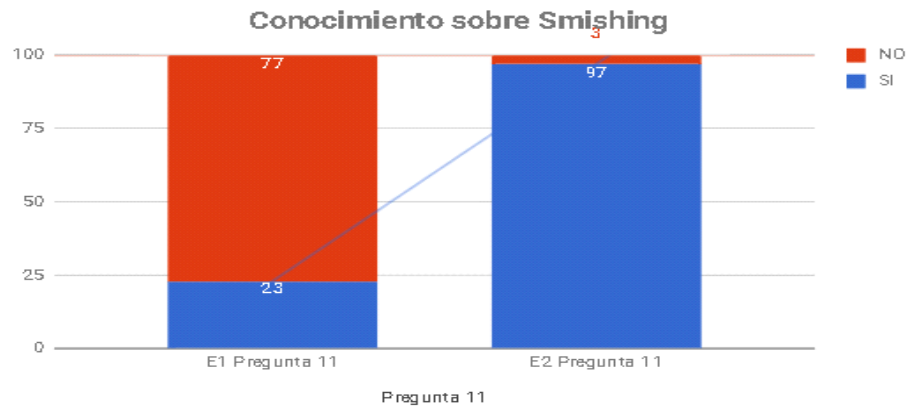


Fuente: Cristhian Camilo Monares Marín

Análisis: En la gráfica se puede evidenciar un incremento del nivel de conocimiento relacionada con la suplantación, por lo que se logró un impacto positivo en el nivel del 31%, logrando así que la totalidad de las personas pertenecientes al grupo de muestra conocieran este factor de riesgo al navegar y utilizar el internet.

- **Conocimiento sobre Smishing**

Ilustración 35. Resultados comparativa pregunta 11.

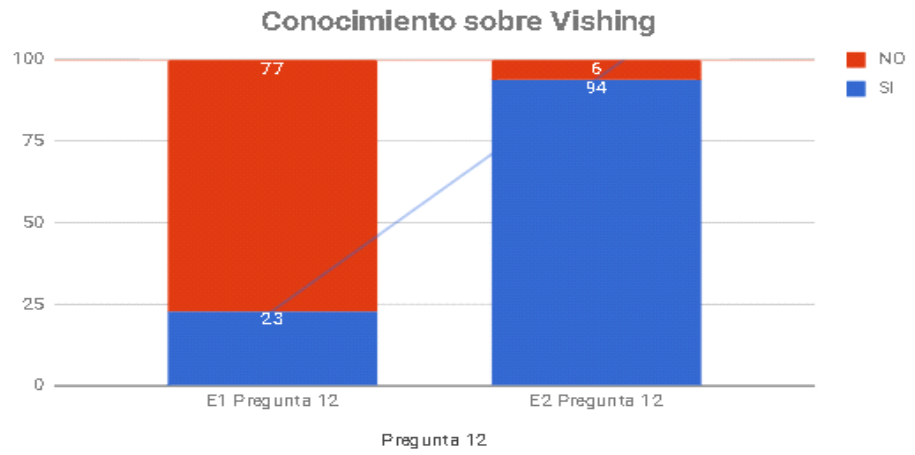


Fuente: Cristhian Camilo Monares Marín

Análisis: En la gráfica se observa un gran incremento del nivel de conocimiento acerca del Smishing, por lo que se logró un incremento del 74%, logrando así que casi la totalidad de las personas pertenecientes al grupo de muestra conocieran este y complementaran su conocimiento acerca del Smishing.

- **Conocimiento sobre Vishing**

Ilustración 36. Resultados comparativa pregunta 12.

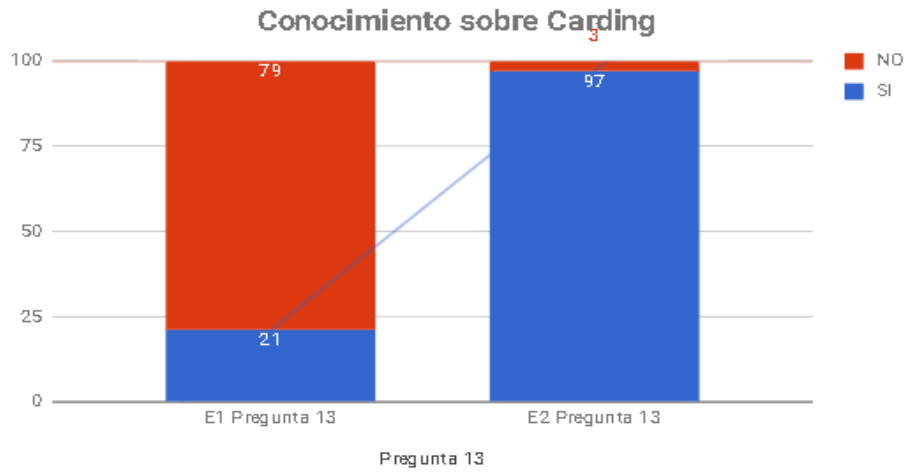


Fuente: Cristhian Camilo Monares Marín

Análisis: En la gráfica se puede observar un crecimiento significativo en del nivel de conocimiento acerca del Vishing, por lo que se logró un incremento del 71%, logrando así que casi el 100% de las personas participantes conocieran este factor de riesgo al navegar y utilizar el internet.

- **Conocimiento sobre carding**

Ilustración 37. Resultados comparativa pregunta 13.

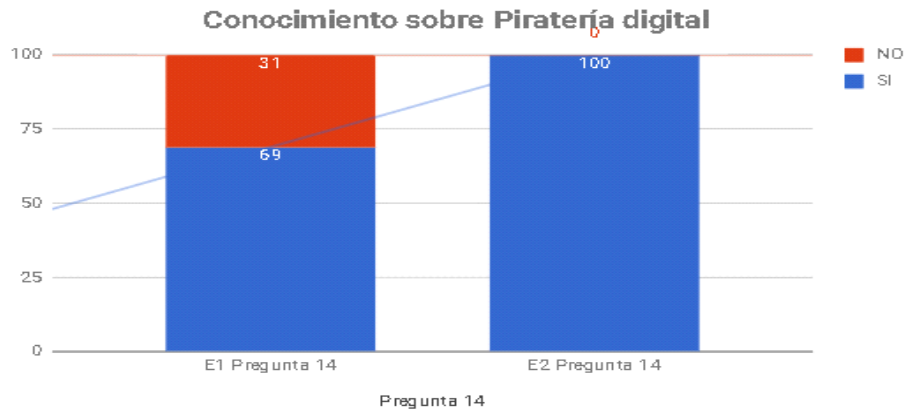


Fuente: Cristhian Camilo Monares Marín

Análisis: En la gráfica se observa un gran incremento del nivel de conocimiento acerca del Carding, por lo que se logró un incremento del 76%, logrando así que casi la totalidad de las personas pertenecientes al grupo de muestra conocieran este y complementaran su conocimiento acerca del Carding.

- **Conocimiento sobre piratería digital**

Ilustración 38. Resultados comparativa pregunta 14.

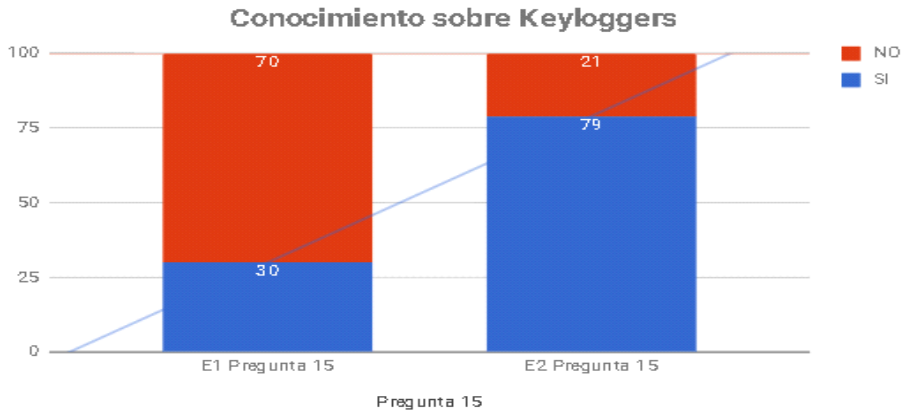


Fuente: Cristhian Camilo Monares Marín

Análisis: En la gráfica se puede observar un significativo incremento en el nivel de conocimiento acerca de la piratería digital, por lo que se logró un incremento equivalente al 31% de conocimiento en las personas participantes, logrando así que la totalidad de las personas pertenecientes al grupo de muestra conocieran acerca de ésta práctica desleal, por lo que, se generó conciencia acerca de los riesgos de la misma.

- **Conocimiento sobre Keyloggers**

Ilustración 39. Resultados comparativa pregunta 15.

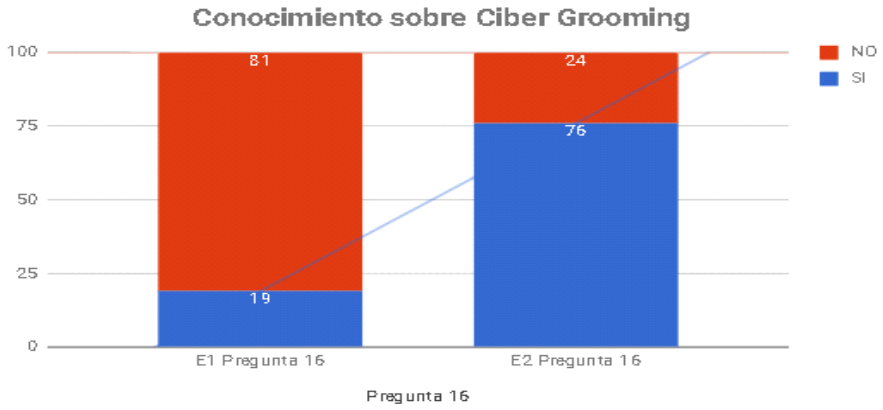


Fuente: Cristhian Camilo Monares Marín

Análisis: En la gráfica se puede observar un incremento significativo en el nivel de conocimiento acerca de la definición y ejemplos de Keyloggers, por lo que se logró un incremento equivalente al 49% en el conocimiento en las personas participantes acerca de ésta práctica, logrando así que una buena parte de las personas pertenecientes al grupo de muestra conocieran de éste método, por lo que, se generó conciencia acerca de los riesgos de la misma.

- **Conocimiento sobre Ciber grooming**

Ilustración 40. Resultados comparativa pregunta 16.

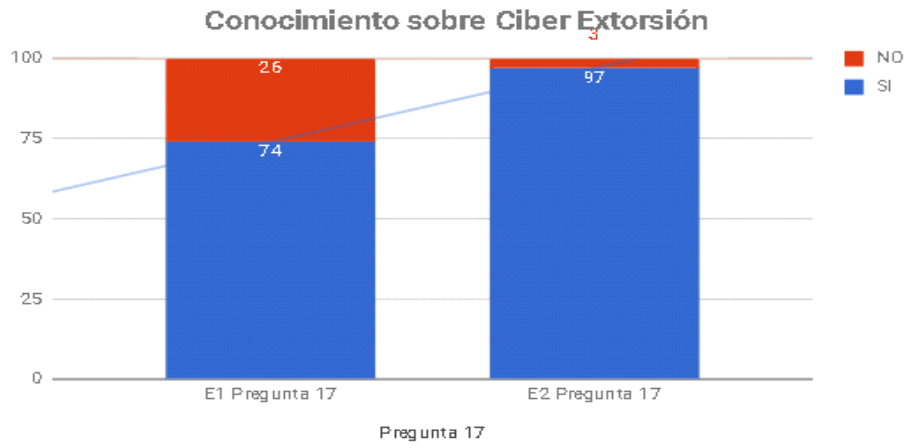


Fuente: Cristhian Camilo Monares Marín

Análisis: En la gráfica se puede observar un incremento significativo en el nivel de conocimiento acerca de la definición y ejemplos de Ciber Grooming, teniendo en cuenta que se tenía un bajo nivel de conocimiento previo del tema, por lo que se logró un incremento equivalente al 57% en el conocimiento en las personas participantes acerca de ésta práctica, logrando así que una buena parte de las personas pertenecientes al grupo de muestra conocieran de éste método, por lo que, se generó conciencia acerca de los riesgos de la misma.

- **Conocimiento sobre Ciberextorsión**

Ilustración 41. Resultados comparativa pregunta 17.

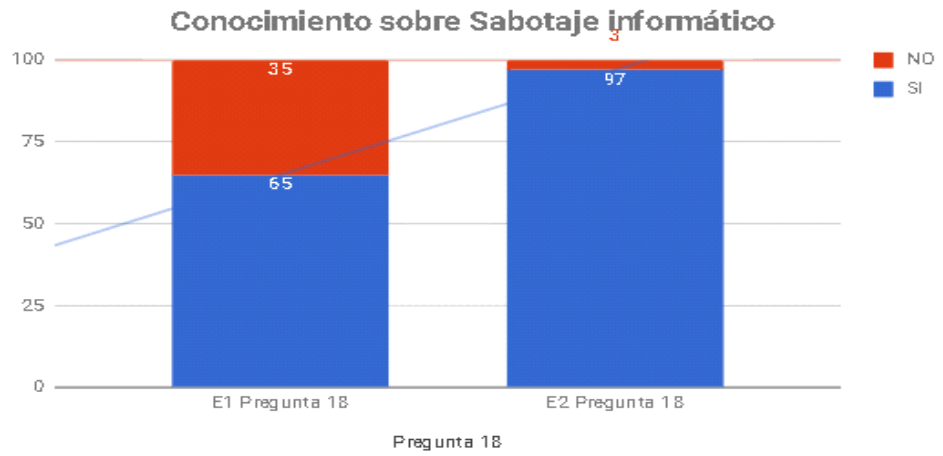


Fuente: Cristhian Camilo Monares Marín

Análisis: De la gráfica se puede deducir un incremento en el nivel de conocimiento acerca de la definición y ejemplos de Ciber Extorsión, por lo que se logró un incremento equivalente al 23% en el conocimiento en las personas participantes, logrando así, que caso la totalidad de estas personas pertenecientes al grupo de muestra conocieran de éste método, por lo que, se generó conciencia acerca de los riesgos de la misma.

- **Conocimiento sobre sabotaje informático**

Ilustración 42. Resultados comparativa pregunta 18.

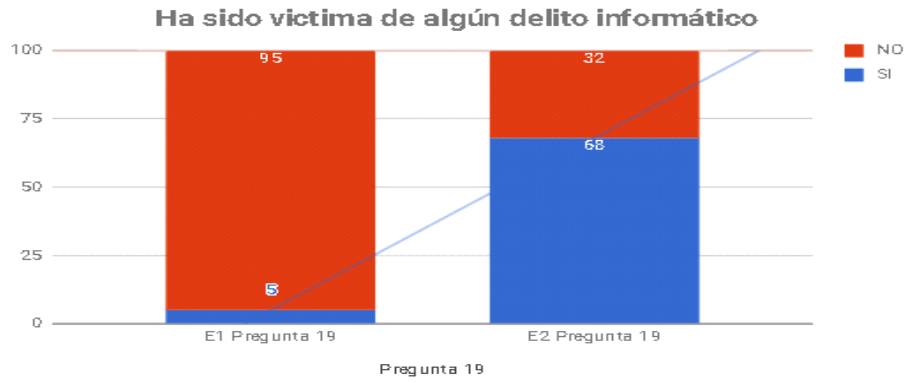


Fuente: Cristhian Camilo Monares Marín

Análisis: En la gráfica se observa un incremento significativo en el nivel de conocimiento previo acerca del sabotaje informático, por lo que se logró un incremento del 32%, logrando así que casi la totalidad de las personas pertenecientes al grupo de muestra conocieran esta clase de práctica desleal y tomaran las medidas tendientes a prevenir ser víctima de las mismas.

- **¿Ha sido víctima de algún delito informático?**

Ilustración 43. Resultados comparativa pregunta 19.

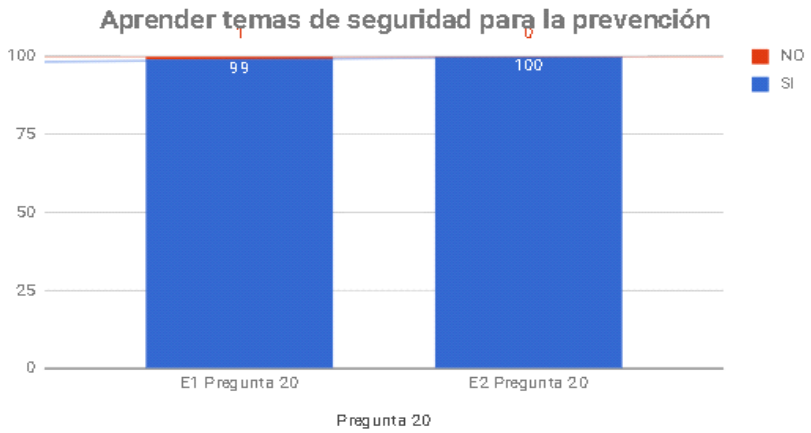


Fuente: Cristhian Camilo Monares Marín

Análisis: En la gráfica se observa que muchos de los participantes consideraban no haber sido víctima de delitos informáticos antes de recibir las capacitaciones, en parte, debido a la falta de conocimiento sobre la existencia de prácticas que se puedan considerar como delito, por lo qué, se generó conciencia acerca de muchas prácticas que se pueden considerar como delictivas y de las que muchas personas habían sido víctimas sin saberlo y evitando así que muchos de ellos incurran en dichas conductas o sean víctimas de las mismas.

- **Importancia de aprender temas de seguridad para la prevención.**

Ilustración 44. Resultados comparativa pregunta 20.

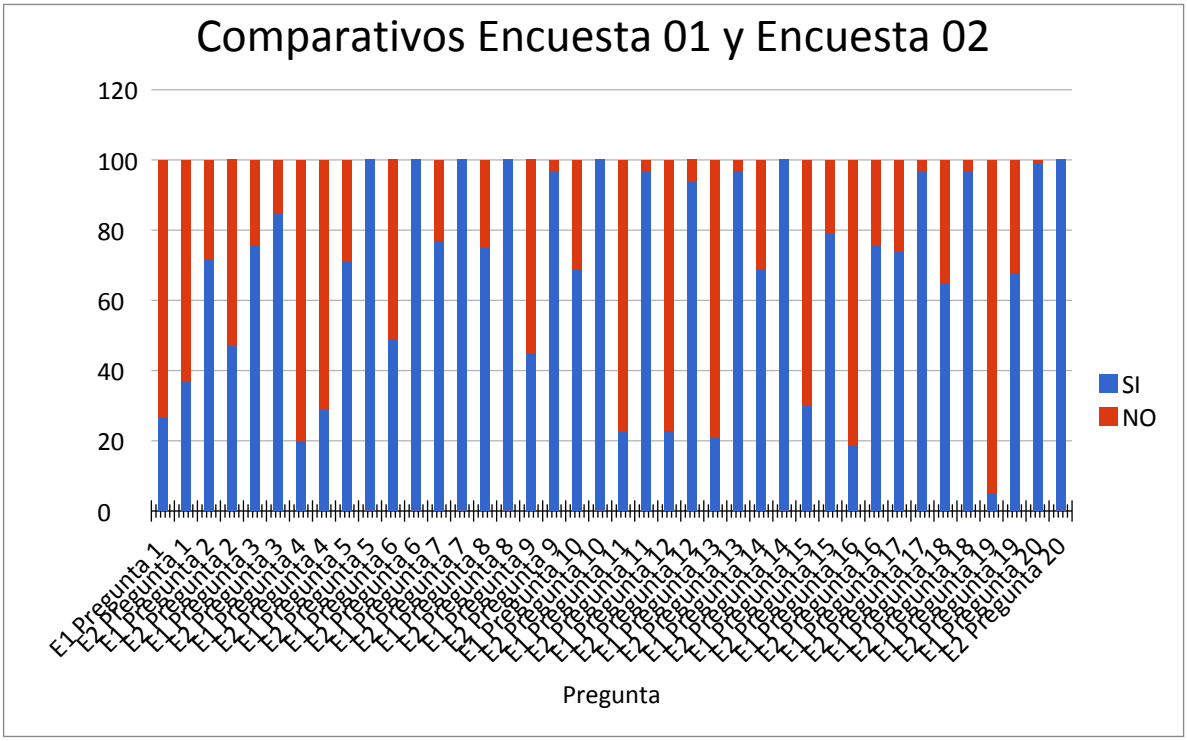


Fuente: Cristhian Camilo Monares Marín

Análisis: Se puede establecer que casi en su totalidad, el grupo de muestra tenía interés por aprender temas relacionados con seguridad y prevención en internet, para al final del ejercicio e implementación de las capacitaciones, establecer un interés generalizado en las personas participantes acerca de la importancia de las prácticas de prevención para la seguridad de la información que se publica en la red.

- **Cuadro comparativo general.**

Ilustración 45. Resultados comparativos generales.



Fuente: Cristhian Camilo Monares Marín

Descripción: Como resultado de las capacitacioens realizadas dentro de Crezcamos S.A., se observa de manera global, un gran avance en materia de seguridad informatica y el impacto que se tuvo en el grupo de colaboradores que se encuestaron, obteniendo un incremento significativo en el interés de las personas en la materia y de la concientización acerca de los errores que se cometen diariamente con los riesgos potenciales que generan una vida personal conectada a la red.

Por lo anterior, es posible afirmar que el proyecto realizado generó un impacto positivo en las personas participantes, el cual se verá reflejado en su vida personal y profesional.

RECOMENDACIONES

- Hacer constantes recomendaciones a todos los colaboradores sobre cómo comprobar la autenticidad de los perfiles con el objetivo de que no acepten invitaciones, correos y solicitudes para acceder a información enviados por particulares “sospechosos”. Asimismo si reciben correos con marcas o empresas comprobar que estas sean procedentes de los dominios y cuentas oficiales.
- Reforzar con las campañas de protección de datos personales, para que los usuarios no facilitan ningún dato personal propio o de un tercero sin autorización. Esto ayuda sustancialmente para que no puedan ser usados para un futuro ataque por el simple descuido de un colaborador que abría un correo que simulaba ser de la propia empresa.
- Invitar a rechazar y denunciar si localizan un perfil sospechoso con un comportamiento extraño en las redes internas y externas de la empresa. Es importante denunciar y alertar sobre ello para que otros usuarios puedan estar preavisados. Lo más importante es reiterar acerca del cuidado con lo que se comparte en documentos, videos, fotografías, estados de ánimo entre otros por las redes sociales.
- De todos los riesgos vistos y mencionados durantes las capacitaciones, la única medida de mitigación es hallarse siempre alerta de la información que se comparte y con quién se comparte sea cual sea su naturaleza (Personal y corporativa).
- En el caso de las redes corporativas no es solo esencial tener soluciones adaptadas a las necesidades particulares del negocio; se debe velar para que los usuarios estén siempre actualizados sobre estos temas de seguridad informática en los cuales la ingeniería social es el punto de partida para los ataques.

CONCLUSIONES

- Las metodologías y técnicas utilizadas mediante la simulación de escenarios de ingeniería social fueron idóneas para este estudio, ya que permitió la evaluación objetiva de cada uno de los factores analizados y por ende logró que los participantes autoevaluaran el nivel de exposición de riesgo que consciente o inconscientemente aceptaron al mantener en la interacción con el mundo virtual
- El diagnósticos permitió identificar factores internos como externos que ponen en riesgo la seguridad de los activos informáticos y los sistemas de información de la organización, centrados en el recurso humano o activos de personal.
- A través de actividades de socialización y capacitación se mejoró la percepción de seguridad informática en la vida digital y la exposición de los participantes a los delitos informáticos por desconocimiento
- Las recomendaciones que se realizaron al finalizar las capacitaciones permitieron concientizar a los participantes y adquirir habilidades para prevenir los delitos informáticos que se vieron reflejadas de forma positiva en su vida pesonal y laboral, aunado a esto, se adquirió un compromiso por parte de la Gerencia de Tecnología y la Coordinación de Seguridad Informática, donde se establecieron las políticas de prevención en cada uno de las personas que hacen parte de la compañía, no solo políticas generales de prevención y protección de datos relacionados a la organización sino la generación de una cultura de autoprotección en cada uno de los miembros de Crezcamos S.A., la cual generará un cambio significativo en el desempeño personal y laboral de la compañía teniendo

en cuenta que muchas de éstas personas podrán evaluar sus deficiencias y establecer políticas de mejora.

- Gracias a los resutados obtendos de la realizacion de las distintas actividades de capacitación y las encuentas al personal y colaboradores de Crezcamos S.A., se logra concluir que existen algunos factores a mejorar en materia de la seguridad de la información que se comparte en la red, teniendo en cuenta que muchas de éstas personas pueden llegar a ser victimas de delitos informaticos o de una indebida utulización y aprovechamiento de los datos privados, los cuales se comparten de manera públicavy a los que se han expuesto debido al exceso de confianza o al desconocimiento de la materia.

- Se observó que los colaboradores de Crezcamos S.A. no están exentos de ser victimas de la ingenieria social, pero se evidenció un interés en mejorar sus pacticas e interacciones en el internet, por lo que, se sugiere la aplicación depoliticas empresariales que permitan alos colaboradores generar conciencia y tomar medidas mínimas de seguridad que les permitan reducir la exposición al riesgo de ser victimas de delitos informáticos y de ingeniera social.

- Teniendo en cuenta los indices de mejora en el grupo participante, se propone a la gerencia de la compañía Crezcamos S.A., la adoptar algunas de las sugerencias que hacen parte de los anexos del presente docuemento, en base a los resultados obtenidos y a los beneficios que pueden significar para la vida personal y profesional de sus trabajadores, la cual, se vería reflejado en un beneficio para la compañía.

- Se logró evidenciar que muchos de los colaboradores de Crezcamos S.A. consideraban no haber sido víctima de delitos informáticos, debido a su

desconocimiento acerca de las conductas que pueden ser consideradas como indebidas o delictivas, quienes una vez recibieron las capacitaciones, fueron concientizados acerca de las acciones que se encuentran tipificadas dentro de la normatividad colombiana, mejorando así su conciencia acerca de los riesgos de compartir información personal en internet.

- Se concluye que una vez gracias a la aplicaciòn de las actividades dentro del proyecto, un gran porcentaje de los participantes logró conocer y entender mejor los distintos tipos de ciberestafas, delitos informáticos y la ingeniera social.

- Se logra concluir que un porcentaje muy inferior de los encuestados se considera esclavo de la tecnología.

- Un gran porcentaje (85%) considera que ha sido víctima de Ingeniería social en algunas de sus manifestaciones.

- Al final del experimento, se logró determinar la importancia de la información acerca de los riesgos que conlleva una vida conectada al internet y como cada uno de los usuarios, puede generar un riesgo potencial en su informaciòn privada al no establecer normas de seguridad en su interacción con en la red.

- Para finalizar se concluye que el nivel de seguridad de la empresa identificado a través del diagnóstico es muy bajo, la cual debe ser mayor para el tipo de organización que es CREZCAMOS S.A, una financiera. Aún cuando se conoce la importancia de la seguridad informática para la financiera no se le ha dado el valor que requiere, no obstante, este estudio permitió concientizar y proponer opciones de mejora para fortalecer dicha

área y por ende aumentar la protección de los datos privados, contenidos digitales y recursos tecnológicos que la organización posee.

BIBLIOGRAFÍA

- ✓ ARCOS, Sergio Sebastian. Ingeniería social: Psicología aplicada a la seguridad informática, 1 de Junio de 2011, disponible en: http://es.slideshare.net/evilbyteperu/tesis-ingenieria-social {Consultado el dìa 21 de Noviembre de 2017}

- ✓ CONGRESO DE LA REPÚBLICA DE COLOMBIA, Ley 1273 “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”.

- ✓ DE LOS SANTOS Sergio. Una al día, 16 años de seguridad informática. Ed. HISPASEC. Disponible en: http://0xword.com/es/libros/43-libro-una-al-dia.html {Consultado el día: 21 de noviembre de 2017}.

- ✓ GASTESI Mikel y CREUS Daniel, Fraude Online abierto 24 horas. S21sec. Disponible en: http://0xword.com/es/libros/21-libro-fraude-online.html {Consultado el día: 18 de noviembre de 2017}.

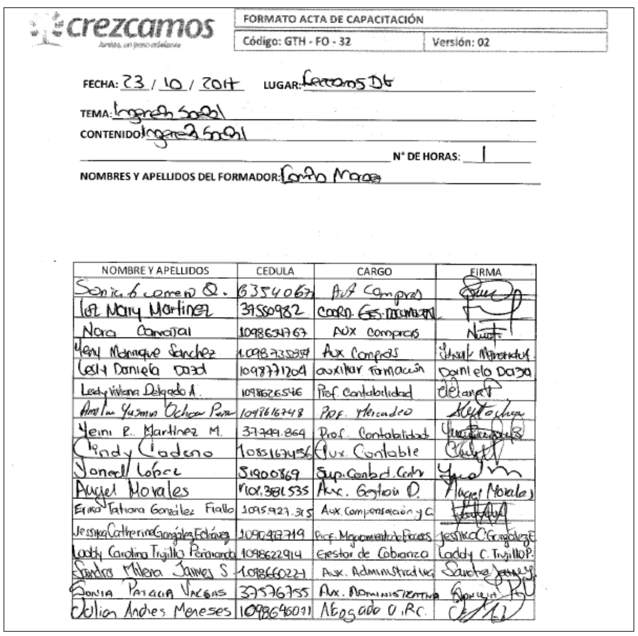
- ✓ Google corporation, www.google.com/intl/es-419_co/forms/about/, autor. Nombre: formulario encuesta ingenieria social, autor.

ANEXOS

ANEXO A. Actas de capacitación.

Como anexo del presente documento, se adjunta las actas de las capacitaciones realizadas, dentro de las que se evidencia la asistencia a las actividades programadas.

Ejemplo:



crezcamos

FORMATO ACTA DE CAPACITACIÓN

Código: GTH - FO - 32 | Versión: 02

FECHA: 23 / 10 / 2014 LUGAR: [illegible]

TEMA: [illegible]

CONTENIDO: [illegible]

N° DE HORAS: 1

NOMBRES Y APELLIDOS DEL FORMADOR: [illegible]

NOMBRE Y APELLIDOS	CEDULA	CARGO	FIRMA
Sonia Romero Q.	63540671	Aux Compras	[illegible]
Luz Mary Martinez	37550982	Coord. Ges. Documental	[illegible]
Nora Carvajal	1098654767	Aux compras	[illegible]
Yeny Manrique Sanchez	1.098735354	Aux Compras	[illegible]
Lesly Daniela Daza	1098771204	auxiliar formación	Daniela Daza
Leidy Viviana Delgado A.	1098626546	Prof. Contabilidad	[illegible]
Amelia Yasmin Ochoa Parra	1098616748	Prof. Mercadeo	[illegible]
Yeini R. Martinez M.	37.749.864	Prof. Contabilidad	[illegible]
Cindy Cadena	1085167456	Aux. Contable	[illegible]
Yonell López	5900869	Sup. Contab. Cartera	[illegible]
Angel Morales	1102.381535	Aux. Gestion D.	Angel Morales
Erika Tatiana González Fiallo	1095.927.315	Aux. Compensación y C.	[illegible]
Jessica Catherine González Echávez	1090417719	Prof. Mejoramiento de Procesos	Jessica C. González E.
Laddy Carolina Trujillo Peñaranda	1098622914	Gestor de Cobranza	Laddy C. Trujillo P.
Sandra Milena Jaimes S.	1098660227	Aux. Administrativa	[illegible]
Sonia Patricia Vargas	37576755	Aux. Administrativa	[illegible]
Julian Andres Meneses	1098646071	Abogado O.R.C.	[illegible]

ANEXO B. Invitaciones a las capacitaciones y socializaciones

Anexo al presente documentos, se adjuntan las distintas constancias y solicitudes realizadas a la compañía Crezcamos S.A., para la realización de las actividades previstas.

Ejemplo:

Capacitación Ingeniería Social

Creado por: shirley.gomez@crezcamos.com · Tu respuesta: ✓Sí, asistiré.

Hora
14:00 - 15:00 (Bogotá)

Fecha
lun 23 oct 2017

Dónde
Salón 2 de Capacitación - Terraza

Descripción
Buenas Tardes:

Se ha programado una capacitación con el objetivo de diagnosticar el nivel de seguridad mediante metodologías de Ingeniería Social a los colaboradores de Crezcamos.

Agradecemos su asistencia y participación,

Mis notas

Invitados
- ✓ Andrea Regueros
- ✓ Beatriz Plata Caballero
- ✓ brayan.contreras@crezcamos.com
- ✓ Camilo Monares
- ✓ ivonne.hernandez@crezcamos.com
- ✓ James Hernandez
- ✓ Jhair Moreno
- ✓ johanna.portilla@crezcamos.com
- ✓ jullie.mantilla@crezcamos.com
- ✓ Jully Florez
- ✓ Katherine Solano Solano
- ✓ Martha Lucia Duarte
- ✓ Mery Ovalle
- ✓ Shirley Gomez
- ✓ Yeraldin Bohórquez
- ? Javier Andres Ballesteros Castellanos
- ✗ Alexander Pena
- ✗ Fredy Asael Angarita Fonseca
- Albert Ortiz
- Enia Calderon
- juan.murallas@crezcamos.com
- NATHALIA MACIAS JAIMES
- lesly.daza@crezcamos.com
- Liliana Calvo
- Paola Rico
- Mauricio Caceres
- Oscar Velasquez
- Romario Fajardo
- Yerson Andres Suarez Yerson Suarez

ANEXO C. Material de capacitación

Anexo con el presente documento, se adjuntan los archivos PPT de las capacitaciones realizadas, siendo éstos las presentaciones de la capacitación 01, 02 y la presentación gerencial.

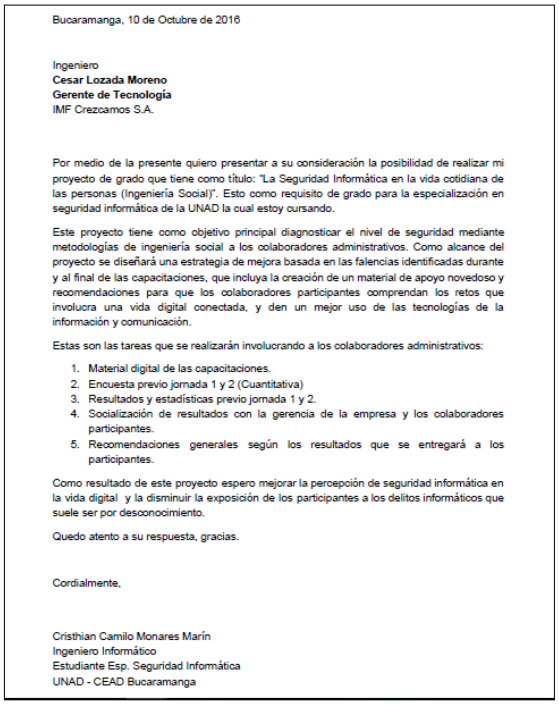
Ejemplo:

La Seguridad Informática en la vida cotidiana de las personas (Ingenieria Social) Parte II

ANEXO D. Solicitudes de participación

Adjunto con el presente documento, se anexan los archivos correspondientes a las solicitudes realizadas a los colaboradores para llevar a cabo las actividades descritas anteriormente dentro del presente proyecto.

Ejemplo:



Bucaramanga, 10 de Octubre de 2016

Ingeniero
Cesar Lozada Moreno
Gerente de Tecnología
IMF Crezcamos S.A.

Por medio de la presente quiero presentar a su consideración la posibilidad de realizar mi proyecto de grado que tiene como título: "La Seguridad Informática en la vida cotidiana de las personas (Ingeniería Social)". Esto como requisito de grado para la especialización en seguridad informática de la UNAD la cual estoy cursando.

Este proyecto tiene como objetivo principal diagnosticar el nivel de seguridad mediante metodologías de ingeniería social a los colaboradores administrativos. Como alcance del proyecto se diseñará una estrategia de mejora basada en las falencias identificadas durante y al final de las capacitaciones, que incluya la creación de un material de apoyo novedoso y recomendaciones para que los colaboradores participantes comprendan los retos que involucra una vida digital conectada, y den un mejor uso de las tecnologías de la información y comunicación.

Estas son las tareas que se realizarán involucrando a los colaboradores administrativos:

1. Material digital de las capacitaciones.
2. Encuesta previo jornada 1 y 2 (Cuantitativa)
3. Resultados y estadísticas previo jornada 1 y 2.
4. Socialización de resultados con la gerencia de la empresa y los colaboradores participantes.
5. Recomendaciones generales según los resultados que se entregará a los participantes.

Como resultado de este proyecto espero mejorar la percepción de seguridad informática en la vida digital y la disminuir la exposición de los participantes a los delitos informáticos que suele ser por desconocimiento.

Quedo atento a su respuesta, gracias.

Cordialmente,

Cristhian Camilo Monares Marín
Ingeniero Informático
Estudiante Esp. Seguridad Informática
UNAD - CEAD Bucaramanga

Anexo E. Encuesta precapacitación

Anexo con el presente documento, se adjunta las preguntas realizadas en la campaña de encuestas de pre capacitación realizada al grupo de colaboradores de Crezcamos S.A.

Ejemplo:

Anexo F. Encuesta Postcapacitación

Anexo con el presente documento, se adjunta las preguntas realizadas en la campaña de encestas de pos capacitación realizada al grupo de colaboradores de Crezcamos S.A.

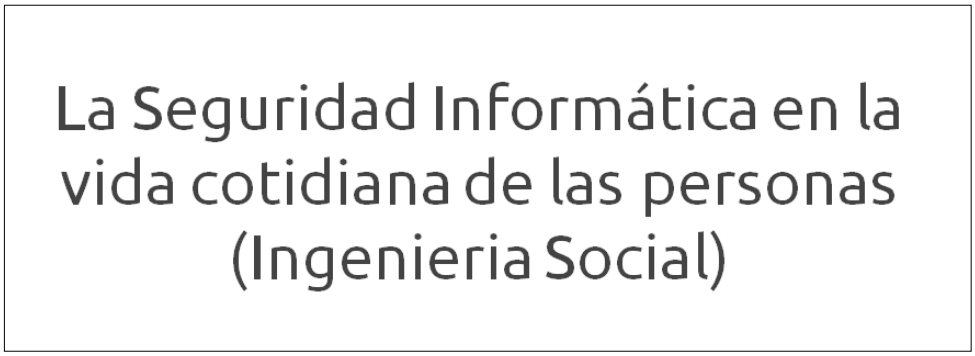
Ejemplo:

Fuente: https://docs.google.com/forms/d/e/1FAIpQLSfhvtmdxEK711iNh_U4mQQtY9gbQaB25enckYMlsm8czlBCjg/viewform

Anexo G. Presentación Gerencial

Anexo con el presente documento, se adjuntan el archivo PPT de la capacitación realizada, a las cual se denomina Presentación Gerencial.

Ejemplo:



ANEXO H. RESUMEN ANALITICO ESPECIALIZADO R.A.E

TEMA: Los factores que puedan comprometer la seguridad de los activos informáticos y sus sistemas de información en CREZCAMOS S.A.

TÍTULO: LA SEGURIDAD INFORMÁTICA EN LA VIDA COTIDIANA DE LAS PERSONAS (INGENIERÍA SOCIAL) CASO CREZCAMOS S.A.

AUTORES : Monares Marín, Cristhian Camilo

FUENTES BIBLIOGRÁFICAS:

-ARCOS, Sergio Sebastian. Ingeniería social: Psicología aplicada a la seguridad informática, 1 de Junio de 2011, disponible en: http://es.slideshare.net/evilbyteperu/tesis-ingenieria-social {Consultado el día 21 de Noviembre de 2017}

-CONGRESO DE LA REPÚBLICA DE COLOMBIA, Ley 1273 “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”.

-DE LOS SANTOS Sergio. Una al día, 16 años de seguridad informática. Ed. HISPASEC. Disponible en: http://0xword.com/es/libros/43-libro-una-al-dia.html {Consultado el día: 21 de noviembre de 2017}.

-GASTESI Mikel y CREUS Daniel, Fraude Online abierto 24 horas. Disponible en: http://0xword.com/es/libros/21-libro-fraude-online.html {Consultado el día: 18 de noviembre de 2017}.

RESUMEN: El trabajo expuesto a continuación es el resultado de un estudio orientado al desarrollo de una prueba de Ingeniería Social sencilla aplicada a una muestra focal de los colaboradores de la compañía Crezcamos S.A.

El desarrollo metodológico de este proyecto se basa en la aplicación de importantes áreas del conocimiento concernientes a la seguridad informática y a la protección de los datos personales en todas sus dimensiones, las cuales reflejan un resultado de importancia en el diagnóstico de los niveles de conocimiento frente a una amenaza tan cotidiana como lo son los delitos informáticos. Mediante el análisis de encuestas, la aplicación de conocimiento vía capacitaciones, la evaluación de aspectos referentes a la ingeniería social, la exposición al riesgo de ser investigado por medios públicos y gratuitos, entre otros aspectos que son fundamentales para la ingeniería social, permitieron un adecuado acercamiento y materialización de las amenazas que implican no aplicar la seguridad informática.

PALABRAS CLAVES: Seguridad informática, delitos informáticos, protección de datos personales, Carding, Sabotaje Informático, Suplantación, Vishing, Phishing, Smishing, Cibergrooming, Cibertaques, Ciberestafa, Piratería digital.

CONTENIDOS: En primera estancia la problemática identificada alrededor del tema de investigación, seguido de los objetivos planteados que darán respuesta al problema a través de un diagnóstico sobre el nivel de conocimiento de las metodologías de ingeniería social, posteriormente se muestra el análisis de la información obtenida a través de encuestas y finalmente se realizan unas capacitaciones donde se medirá el impacto de las mismas a través de una segunda fase de evaluación, análisis de los resultados y recomendaciones.

DESCRIPCION DEL PROBLEMA:

Las personas en la actualidad desconocen muchos de los peligros reales de tener una vida digital conectada, esto implica estar conectados todo el tiempo a la red mundial de Internet y este desconocimiento hace que las personas den un mal uso de las tecnologías y coloquen en peligro sus datos e identidad, lo que genera un riesgo potencial para su información y la de las personas que las rodena, dentro de su ámbito personal, familiar y laboral, teniendo en cuenta que, muchas de éstas

personas no están conscientes del nivel de riesgo al que se someten al compartir muchas de su información en redes sociales o en comunidades en línea, sea de entretenimiento o profesional, lo que genera una ventana en la que una persona u organización con intenciones desconocidas, siendo muchas veces malintencionadas, puede hacer uso o apropiarse de información que pueda perjudicar al propietario de la misma y a aquellas personas que lo rodean o se encuentran vinculadas a la misma.

Con lo anterior, se hace necesario que los colaboradores de la compañía conozcan las distintas exposiciones al riesgo de delitos informáticos que tiene el uso de tecnologías de la información y comunicación, en especial, deben conocer la ingeniera social que suele afectar en gran medida a las instituciones financieras de Colombia, por tanto deben comunicar y establecer los comportamientos institucionales adecuados que aseguren la protección de su información.

METODOLOGÍA: Se aplicarán encuestas al grupo de muestra previa a la primera jornada de capacitación, encaminadaa conocer cómo actúan las personas en casos claros de ingeniería social. Luego, se realizará una capacitación acerca de temas relacionados con la seguridad informática. Tras analizar esta segunda encuesta, se realizara la última jornada de capacitación, en donde, basados en los resultados obtenidos, se realizarán las recomendaciones y consejos de seguridad y prevención. Se finaliza socializando los resultados y recomendaciones a la Gerencia de la compañía.

PRINCIPALES REFERENTES TEÓRICOS: Sistema de Gestión de Seguridad de la Información (SGSI), el cual está conformado por políticas, estándares (técnicos y generales de seguridad de la información), y las Políticas de Seguridad de la Información y Ciberseguridad

PRINCIPALES REFERENTES CONCEPTUALES:

Se utilizaron los conceptos de las siguientes palabras: Estándar de Seguridad de la Información, Evidencia Digital, Incidente de Seguridad de la Información,

Incidente de Ciberseguridad, Personas que prestan servicios al Banco, Usuario, Recursos de Tecnología de Información Las Tecnologías de la Información y las Comunicaciones (TIC)

De los resultados más significativos para el estudio, se evidencia un mayor porcentaje en las siguientes situaciones: Las personas del estudio no se consideran esclavos tecnológicos, pero si de tener un buen manejo de su vida digital, consideran que pueden ser víctimas de ingeniería social, pero son conscientes que deben tomar medidas de seguridad suficientes en su vida digital. Conocen temas de seguridad informática como: delitos informáticos, ciberestafa, suplantación digital, piratería digital, sabotaje informático, sin embargo, desconocen temas como: ingeniería social, Phishing, Smishing, Vishing, Carding, KeyLogger, aún así, el 99% nunca ha sido víctima de alguno de los anteriores temas de seguridad informática nombrados, no obstante, consideran que aprender sobre estos temas de seguridad informática le permitirán estar más prevenido frente a un posible ataque.

En la segunda fase del proyecto, después de ralizarse las capacitaciones sobre los diferntes temas mencionados anteriormente, se evidenció positivamente que el grupo de muestra varió la forma de pensar sobre los temas de seguridad informática, con un incremento hasta del 20% de la muestra encuestada.

Se concluye que el nivel de seguridad de la empresa identificado a través del diagnóstico es muy bajo, la cual debe ser mayor para el tipo de organización que es CREZCAMOS S.A, una financiera. Aún cuando se conoce la importancia de la seguridad informática para la financiera no se le ha dado el valor que requiere, no obstante, este estudio permitió concientizar y proponer opciones de mejora para fortalecer dicha área y por ende aumentar la protección de los datos privados, contenidos digitales y recursos tecnológicos que la organización posee.