ANÁLISIS DE LOS PROGRAMAS DE CONCIENTIZACIÓN DE SEGURIDAD DE LA INFORMACIÓN EN COMTEC

CAROLINA ROMERO
JAVIER MAURICIO CARABALLO LEON
ARTURO JOSÉ BOLÍVAR SÁNCHEZ

FUNDACIÓN UNIVERSITARIA LOS LIBERTADORES
FACULTAD DE INGENIERA
ESPECIALIZACIÓN EN SEGURIDAD DE LA INFORMACIÓN
BOGOTÁ D.C.
2021

LOS LIBERTADORES
FUNDACIÓN UNIVERSITARIA

ANÁLISIS DE LOS PROGRAMAS DE CONCIENTIZACIÓN DE SEGURIDAD DE LA INFORMACIÓN EN COMTEC

CAROLINA ROMERO
JAVIER MAURICIO CARABALLO LEON
ARTURO JOSÉ BOLÍVAR SÁNCHEZ

Proyecto de memoria de grado presentado como requisito parcial para optar el título de especialista en seguridad de la información

FUNDACIÓN UNIVERSITARIA LOS LIBERTADORES
FACULTAD DE INGENIERA
ESPECIALIZACIÓN EN SEGURIDAD DE LA INFORMACIÓN
BOGOTÁ D.C.
2021

LOS LIBERTADORES
FUNDACIÓN UNIVERSITARIA

Nota de aceptación

_____

_____

_____

_____

Firma del presidente del jurado

_____

Firma del jurado

_____

Firma del jurado

Bogota D.C. noviembre 20 de 2021

LOS LIBERTADORES
FUNDACIÓN UNIVERSITARIA

TABLA DE CONTENIDO

LOS LIBERTADORES
FUNDACIÓN UNIVERSITARIA

LISTA DE TABLAS

LOS LIBERTADORES
FUNDACIÓN UNIVERSITARIA

LISTA DE FIGURAS

1. INTRODUCCION

En el campo de la seguridad de la información, se busca tener en cuenta todas las posibles amenazas que pueden ocurrir sobre la información y los datos; uno de estos eventos, son los ataques de ingeniería social, en donde usualmente los usuarios finales de la entidad muchas veces se ven comprometidos, debido a que no cuentan con el conocimiento para afrontar este tipo de eventos.

Los atacantes buscan identificar diferentes brechas de seguridad, tomando como foco la conducta humana y explotando aspectos psicológicos para lograr alcanzar un beneficio económico a través de técnicas de engaño; por lo anterior, el factor humano es el mayor objetivo del atacante, debido a su falta de conocimiento o exceso de confianza frente a la información que se encuentra a su alcance.

Las organizaciones invierten una gran cantidad de recursos en infraestructura para proteger su información; sin embargo, uno de los eslabones más débiles son los usuarios finales, de los cuales las empresas no dedican el tiempo adecuado y no proyectan recursos financieros para capacitar y culturizar a las personas.

Según estudios realizados por diversas empresas y consultores de seguridad informática y en seguridad de Internet, se evidencian las siguientes estadísticas[1] (Chávez, 2021):

- El 50% de las empresas son y han sido víctimas de la ingeniería social. Los delincuentes han utilizado el phishing y las redes sociales para obtener información de las personas y/o empresas.
- El teléfono y los correos electrónicos buscan engañar y obtener la confianza del destinatario, representan la fuente más común para engañar a los usuarios (47 %).
- Las redes sociales son suministro continuo de personal, familiar, financiera y profesional, (39 %) y los terminales móviles mal asegurados (12 %).

[1] Chávez, J. D. (2021). *Aspectos interesantes sobre la Ingeniería Social*.

- El afán de lucro es la razón más frecuente de los ataques, seguida del deseo a acceder a información confidencial de la persona y/o empresa (46 %), la búsqueda de ventajas competitivas (40 %) y los actos de venganza (14 %).
- Sólo el 34 % de las personas y/o empresas han sido capacitadas y/o concienciadas sobre políticas de seguridad para evitar caer en diferentes tipos de ataques. Los nuevos empleados, y aquellos que no tienen aún la pertinencia de estar en una empresa, con frecuencia son los objetivos más solicitados por los ciberdelincuentes.

Es importante que las empresas trabajen e inviertan en sus modelos de seguridad de la información, de forma que se logren establecer técnicas que involucren al usuario final, con el objetivo de mitigar los riesgos sobre las diferentes amenazas que se presenten, debido a que los empresarios usualmente fijan presupuestos para robustecer sus plataformas a nivel de seguridad, dejando en segundo plano al personal que diariamente presta sus servicios sobre toda su infraestructura.

2. MARCO DE REFERENCIA DE SEGURIDAD

Dentro de esté proceso de investigación se revisa el modelo de seguridad aprobado por las MINTIC "*Ministerio de Tecnologías de la Información y las Comunicaciones*"; este documento, se encuentra alineado con diferentes marcos de referencias como por ejemplo la ISO27001:2013, adicional cuenta con una serie de guías que permiten la gestión de riesgos y controles sobre las empresas públicas, normalmente estás guías son tomadas por las entidades privadas como un prototipo para su implementación y ejecución[2], en esté documento citan, que se debe definir un plan de comunicaciones que se describe a continuación:

- ***Plan de Comunicaciones****:* Todas las organizaciones deben contar con un plan de comunicación, sensibilización y capacitación, su mayor objetivo debe ser preservar el aseguramiento de la información; este documento, debe estar enfocado hacia todos los empleados de la organización y proveedores de forma que se genere conciencia, se creen rutinas y se logre crear una cultura organizacional sobre la seguridad de la información.

Dentro del marco de referencia adoptado por el MINTIC, se definieron 21 guías que apoyan los procesos de seguridad dentro de las diferentes entidades; a continuación, vamos a describir las guías que están relacionadas con las campañas de concientización de seguridad de la información, para que sean tenidas en cuenta como material de apoyo en las oportunidades de mejora sobre esta investigación:

- ***Guía 1*** – *Metodologías y pruebas de efectividad*: este documento tiene como objetivo realizar algunas pruebas que permitan identificar algunas brechas que se puedan presentar dentro del modelo de seguridad, en su proceso de ejecución una de sus etapas es identificar el comportamiento de los empleados con respecto a los ataques de ingeniería social, debido a que las personas son consideradas como una de las mayores amenazas frente a los activos de la información.[3]
- ***Guía 14*** – *Plan de Comunicación, sensibilización y capacitación:* a través de

[2] MINTIC, Modelo de Seguridad y Privacidad de la Información, 2016
[3] MINTIC, Guía Metodológica de Pruebas de Efectividad, 2016

diferentes fases, está guía tiene como finalidad difundir una serie de pautas que se encuentran formalizadas a través de un documento o políticas de seguridad; el equipo de sensibilización y comunicaciones, debe buscar estrategias innovadoras que permitan que el usuario final adquiera el conocimiento, permanezca atento y se encuentre actualizado, del cómo debe actuar ante un posible evento de seguridad que se presente.[4].

Como se dijo al inicio de este apartado, la norma ISO27001:2013 es uno de los marcos de referencia que se tiene en cuenta para el aseguramiento de la información; a continuación, detallamos el control que relaciona los planes de concientización y sensibilización de seguridad de la información, según documento:[5].

- ***"Control A.7.2.2**: Concientización, educación y formación en Seguridad de la Información: Todos los empleados de la Organización y en donde sea pertinente, los contratistas deben recibir formación adecuada en concientización y actualizaciones regulares en políticas y procedimientos organizacionales, pertinentes para su formación laboral*. [6]

Dado los diferentes marcos de referencia, es importante que COMTEC busque idear e implementar planes de sensibilización que les permita asegurar y proteger la información, de forma que se adopten medios de comunicación que innoven y capten la atención de los empleados que les permita alcanzar los objetivos con respecto a la Seguridad de la Información de la entidad.

[4] MINTIC, Plan de capacitación, sensibilización y comunicación de Seguridad de la Información, 2016
[5] SGS
[6] SGS, ISO 27001-2013 esta no es la Norma Original, es una Interpretación de SGS Colombia S.A., División S&SC, Pag 32.

3. PLANTEAMIENTO Y FORMULACION DEL PROBLEMA

Tanto en Colombia, como en el mundo, el aseguramiento de la información siempre presentará brechas y vulnerabilidades; ante esta situación, se han desarrollado e implementado varias medidas, como por ejemplo el bloqueo de páginas de internet, deshabilitación de puertos, restricción de accesos, etc., sin que ninguna haya sido infalible siendo el usuario una de las más críticas.

El desarrollo de este documento implicará el conocimiento y capacitación de los usuarios en COMTEC en la seguridad de la información y cómo se desenvuelve cada uno de ellos.

Partimos de la premisa, que las personas no saben que es la seguridad de la información, no entienden y no prestan atención a las capacitaciones, entonces ¿que se debería hacer?

4. QUIEN ES COMTEC

El desarrollo de este trabajo se hizo en una empresa de telecomunicaciones; sin embargo, por temas de confidencialidad no se utiliza directamente la razón social; por lo anterior, en esté proceso de investigación será conocida como COMTEC:
COMTEC nace el 15 de enero de 1990, producto de la necesidad de tener una empresa de comunicaciones en Colombia. Cierra su primer año de operaciones con 100 clientes (empresas de prestación de servicios de telecomunicaciones). En 1995 COMTEC obtiene alianzas con varias universidades nacionales para iniciar la instalación de Internet, hoy se cuenta con el 63,78% de usuarios en categoría ADSL. En 1991 lanza un proyecto que consiste en utilizar la red satelital para conectar a los habitantes de los antiguos territorios nacionales. En el 2002, COMTEC se convierte en asociado independiente de América Móvil, gracias a esto, se cubren más 400 poblaciones a nivel nacional.

A partir del 2015, se abre una nueva línea de negocio, la cual es la de seguridad de la información, la cual se ofrece inicialmente a entidades bancarias.

COMTEC, es pionera en la tercerización de telecomunicaciones y seguridad de la información, generando valor agregado a los clientes.

A la fecha COMTEC cuenta con más 1200 usuarios tanto corporativos, como personales, tanto en infraestructura, como seguridad informática; a nivel nacional.

5. OBJETIVOS

5.1. OBJETIVO GENERAL.

Analizar y evaluar la efectividad del plan de capacitación y sensibilización sobre seguridad de la información en las campañas de concientización que tiene establecida COMTEC y proponer lineamientos de forma que cada empleado asegure la integridad, confidencialidad y disponibilidad de la información.

5.2. OBJETIVOS ESPECÍFICOS.

- Validar el conocimiento de los empleados sobre seguridad de la información en COMTEC, mediante encuestas que permitan identificar cuáles son las necesidades sobre las capacitaciones en la entidad.
- Evaluar, medir y cuantificar los resultados obtenidos de las encuestas realizadas, de forma que permita valorar la eficacia en la ejecución de programas de concientización de la entidad.
- Con base a los resultados estadísticos, se aportarán opciones de mejora al plan de capacitación que permitan optimizar la respuesta de los usuarios, frente a los diferentes eventos de seguridad.

6. CAPITULO I

En este apartado se describe la metodología empleada para la recolección de la información en COMTEC. La información obtenida proviene de la ejecución de una encuesta realiza a un grupo de funcionarios que hacen parte de la organización, mediante la aplicación de una serie de preguntas relacionadas con el ámbito de Seguridad de la Información.

6.1 FICHA TÉCNICA

- **Ámbito:** Se realizo a nivel nacional.
- **Universo:**
  - 1200 trabajadores pertenecientes a la Empresa COMTEC que desempeñan sus funciones en diferentes áreas de la entidad.
  - Se realizó la dispersión a nivel nacional, de los cuales 14 ciudades respondieron; a continuación, se relacionan:

Tabla 1: Descripción de Ciudades

Ciudades principales	
Popayán	
Bogotá	Medellín
Otras ciudades	
Arauca	Huila
Zipaquirá	Santa Marta
Barranquilla	Villavicencio
Valledupar	Pasto
Manizales	Cúcuta
Armenia	

Fuente: Elaboración propia

- **Muestra:** Se realizo sobre ciento veinte ocho (128) trabajadores de la organización, todos mayores de edad, teniendo en cuenta su antigüedad en la empresa; así como el área en donde prestan sus servicios:

Tabla 2: Áreas de trabajo en COMTEC

Áreas de trabajo
Administrativo
Auxiliar
Dirección
Operario
Técnico
Tecnología

Fuente: Elaboración propia

- **Técnica de recolección:** Formulario electrónico.
- **Preguntas que se formularon:**
  - ¿Qué es Seguridad de la Información?
  - ¿Un malware es?
  - ¿A través de que medios ha conocido sobre Seguridad de la Información?
  - ¿Phishing es?
  - ¿Cuándo recibes un correo de un remitente desconocido, posiblemente sospechoso que haces?
  - ¿Un virus es?
  - ¿Una contraseña segura es?
  - ¿Cada cuanto se deben cambiar las contraseñas del sistema?
  - ¿Para usted un dispositivo biométrico es?
  - ¿Cuándo usted ingreso a la compañía (COMTEC) recibió instrucciones o lo capacitaron sobre Seguridad de la Información?
- **Fecha de realización:** Entre el 17 de septiembre y el 13 de octubre del año 2021.
- **Diseño y realización:** La encuesta fue diseña y realizada por los ingenieros de Sistemas Carolina Romero, Javier Mauricio Caraballo Leon y Arturo José Bolívar Sánchez, estudiantes de la especialización de Seguridad de la Información de la Fundación Universitaria los Libertadores.

6.2 METODOLOGÍA

Para el desarrollo de este proceso investigativo, se utilizó la siguiente metodología de trabajo:

- Se realizó una encuesta a un grupo representativo correspondiente al 10%
- Luego para el análisis de los resultados se elaboró una matriz de ponderación donde se le asignó un peso numérico a cada pregunta y cada opción de respuesta correcta e incorrecta. Los resultados cualitativos de las encuestas fueron transformados a valores cuantitativos de la siguiente forma.

Tabla 3: Matriz de Ponderación

MATRIZ DE PONDERACION					
Factores		**Alternativas**			
Pregunta	**Peso**	**A**	**B**	**C**	**D**
P1	20	10	5	1	1
P2	8	10	5	1	1
P3	13	10	5	1	1
P4	8	5	10	1	1
P5	8	10	1	5	1
P6	8	10	1	5	1
P7	10	10	1	1	5
P8	7	5	1	10	1
P9	8	10	5	1	1
P10	10	10	1	1	5

Fuente: Elaboración propia

En este proceso al no encontrar resultados representativos, se decide explorar las agrupaciones, en donde se identificaron dos variables, la primera correspondiente a localización geográfica y la segunda por nivel de conocimiento:

- Ciudades principales y otras ciudades
- Mayor conocimiento, conocimiento intermedio y menor conocimiento.

Tabla 4: Matriz de Ponderación NC

RESULTADO PONDERACIÓN NC (NIVEL DE CONOCIMIENTO)	
Mayor conocimiento	439-588
Conocimiento intermedio	289-438
Menos conocimiento	139-288

Fuente: Elaboración propia

7. CAPITULO II

7.1 DESARROLLO

Análisis sobre los resultados obtenidos de las encuestas realizadas:
En este análisis, se parte de que los resultados obtenidos son datos cualitativos, los cuales fueron procesados y tabulados para poder validar el nivel de conocimiento sobre seguridad de la información y así convertirlos en datos cuantitativos. Se tabulo y califico para cuantificar y ponderar la información de forma que permita homologarla.
Una vez homologada la información, se procede a realizar diferentes tipos de agrupaciones, esté tipo de análisis son denominado agrupaciones, en donde se busca revelar patrones de comportamiento que permita generar un análisis sobre los datos obtenidos.

- Resultados que describen el nivel de comprensión en las agrupaciones entre las ciudades y los medios por los cuales ha adquirido el conocimiento sobre seguridad de la información:

Figura 1: Medios de comunicación - nivel de conocimiento - ciudades

Nivel de Con	Ciudades Principales	Otras Ciudades	Total general
Capacitaciones empresariales (charlas, cursos)	**41,49%**	**11,54%**	**35,00%**
Conocimiento Intermedio (*NC 289-438)	13,83%	3,85%	11,67%
Mayor Conocimiento (*NC 439-588)	24,47%	3,85%	20,00%
Menor conocimiento (*NC 139-288)	3,19%	3,85%	3,33%
Campañas redes sociales (públicidad, brochure, otros)	**27,66%**	**57,69%**	**34,17%**
Conocimiento Intermedio (*NC 289-438)	18,09%	38,46%	22,50%
Mayor Conocimiento (*NC 439-588)	9,57%	3,85%	8,33%
Menor conocimiento (*NC 139-288)	0,00%	15,38%	3,33%
Capacitaciones personales (diplomatods, cursos)	**13,83%**	**15,38%**	**14,17%**
Conocimiento Intermedio (*NC 289-438)	1,06%	11,54%	3,33%
Mayor Conocimiento (*NC 439-588)	11,70%	3,85%	10,00%
Menor conocimiento (*NC 139-288)	1,06%	0,00%	0,83%
Campañas empresariales (Periódicos internos, ecard)	**8,51%**	**11,54%**	**9,17%**
Conocimiento Intermedio (*NC 289-438)	7,45%	7,69%	7,50%
Mayor Conocimiento (*NC 439-588)	1,06%	0,00%	0,83%
Menor conocimiento (*NC 139-288)	0,00%	3,85%	0,83%
Otros medios	**8,51%**	**3,85%**	**7,50%**
Total general	**100,00%**	**100,00%**	**100,00%**

Fuente: Elaboración propia

Resultados que describen el nivel de comprensión en las agrupaciones, entre las áreas de trabajo y los medios por los cuales se adquirió el conocimiento sobre

seguridad de la información:

Figura 2: Medios de comunicación - áreas de trabajo - nivel de conocimiento

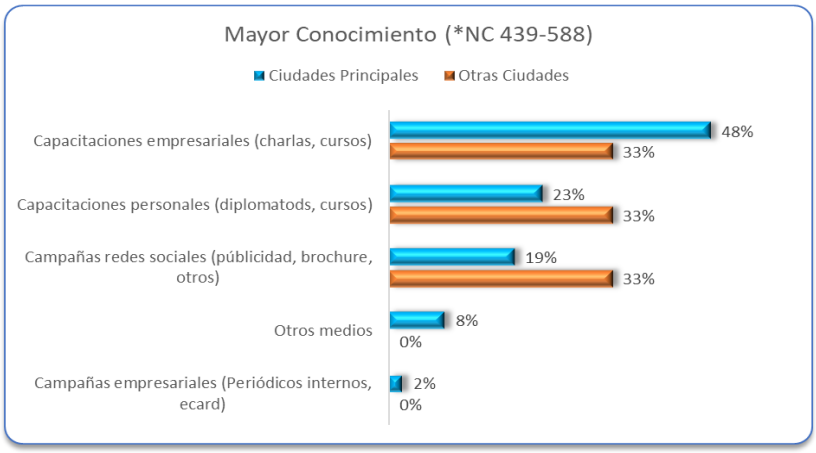
Nivel de Conocimiento SEG INF	Administrativo	Operario	Tecnología	Auxiliar	Dirección	Técnico	Total general
Capacitaciones empresariales (charlas, cursos)	**34,21%**	**48,57%**	**36,36%**	**23,08%**	**9,09%**	**0,00%**	**35,00%**
Mayor Conocimiento (*NC 439-588)	18,42%	20,00%	31,82%	15,38%	9,09%	0,00%	20,00%
Conocimiento Intermedio (*NC 289-438)	13,16%	22,86%	4,55%	0,00%	0,00%	0,00%	11,67%
Menor conocimiento (*NC 139-288)	2,63%	5,71%	0,00%	7,69%	0,00%	0,00%	3,33%
Campañas redes sociales (públicidad, brochure, otros)	**31,58%**	**25,71%**	**31,82%**	**61,54%**	**45,45%**	**0,00%**	**34,17%**
Mayor Conocimiento (*NC 439-588)	0,00%	8,57%	9,09%	38,46%	0,00%	0,00%	8,33%
Conocimiento Intermedio (*NC 289-438)	28,95%	14,29%	13,64%	23,08%	45,45%	0,00%	22,50%
Menor conocimiento (*NC 139-288)	2,63%	2,86%	9,09%	0,00%	0,00%	0,00%	3,33%
Capacitaciones personales (diplomatods, cursos)	**15,79%**	**11,43%**	**22,73%**	**15,38%**	**0,00%**	**0,00%**	**14,17%**
Mayor Conocimiento (*NC 439-588)	10,53%	5,71%	22,73%	7,69%	0,00%	0,00%	10,00%
Conocimiento Intermedio (*NC 289-438)	5,26%	2,86%	0,00%	7,69%	0,00%	0,00%	3,33%
Menor conocimiento (*NC 139-288)	0,00%	2,86%	0,00%	0,00%	0,00%	0,00%	0,83%
Campañas empresariales (Periódicos internos, ecard)	**15,79%**	**2,86%**	**9,09%**	**0,00%**	**9,09%**	**100,00%**	**9,17%**
Mayor Conocimiento (*NC 439-588)	2,63%	0,00%	0,00%	0,00%	0,00%	0,00%	0,83%
Conocimiento Intermedio (*NC 289-438)	13,16%	2,86%	9,09%	0,00%	9,09%	0,00%	7,50%
Menor conocimiento (*NC 139-288)	0,00%	0,00%	0,00%	0,00%	0,00%	100,00%	0,83%
Otros medios	**2,63%**	**11,43%**	**0,00%**	**0,00%**	**36,36%**	**0,00%**	**7,50%**
Total general	**100,00%**	**100,00%**	**100,00%**	**100,00%**	**100,00%**	**100,00%**	**100,00%**

Fuente: Elaboración propia

Por lo anterior recomendamos que se sigan impartiendo capacitaciones empresariales en sala de juntas, cursos a los grupos administrativo, de tecnología y operarios y a la dirección y auxiliares se observa que la mejor técnica para adquirir el conocimiento es a través de las redes sociales y otros.

- En el siguiente clúster se identificó que el 48% de los empleados tienen un mayor conocimiento de seguridad de la información en las ciudades principales y que adquirieron el conocimiento a través de capacitaciones empresariales.

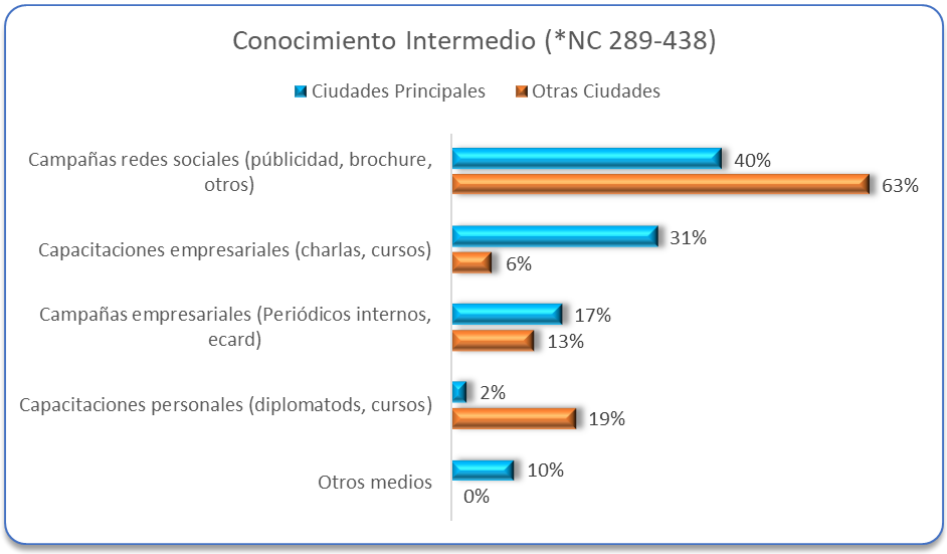
Figura 3: Medios comunicación - ciudades - mayor conocimiento



Fuente: Elaboración propia

- En el siguiente clúster indica que los empleados tienen un conocimiento intermedio del 63% sobre de seguridad de la información en otras ciudades, mencionan que esto fue a través de campañas en redes sociales:

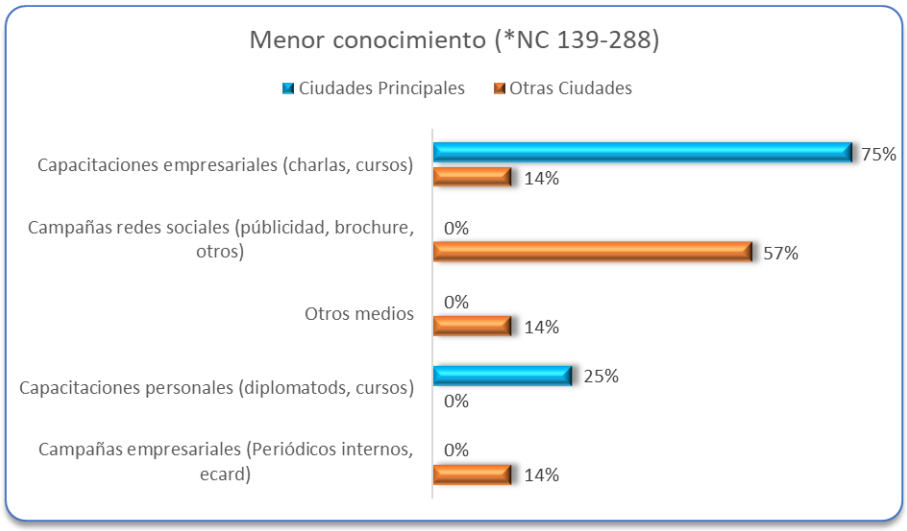
Figura 4: Medios de comunicación – ciudades – conocimiento intermedio



Fuente: Elaboración propia

- El 75% de las agrupaciones de menor conocimiento en ciudades principales, menciona que conoce de seguridad de la información a través de capacitaciones empresariales, en esté grupo analizado predominan empleados con cargo operativo y mayores a 40 años.

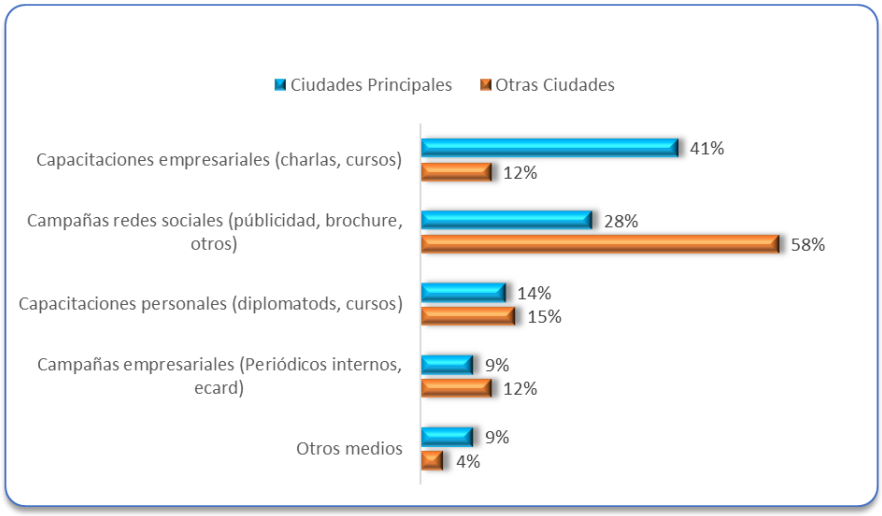
Figura 5:Medios comunicación – ciudades – menor conocimiento



Fuente: Elaboración propia

- Se observa que en las ciudades principales las capacitaciones empresariales tienen un mayor impacto en los empleados (41%) y en las otras ciudades se analiza que las campañas en redes sociales tienen una mejor aceptación (58%).

Figura 6: Medios de comunicación - sobre Seguridad de la Información

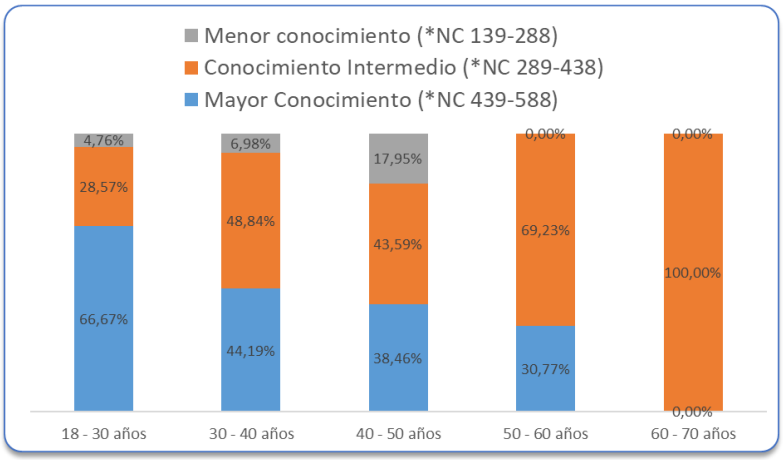


Fuente: Elaboración propia

- Al cruzar el ponderado del nivel de conocimiento, identificamos que a menor edad mayor conocimiento sobre seguridad de la información, de igual manera a mayor edad tienden a tener un conocimiento intermedio sobre seguridad de la

información.

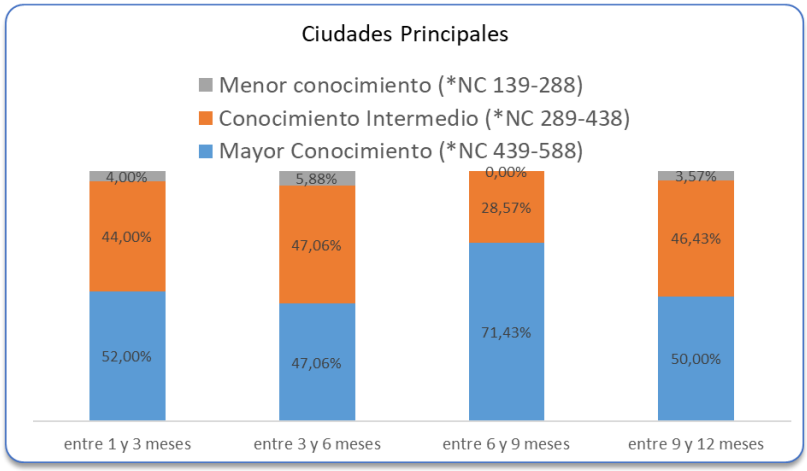
Figura 7: Validación del conocimiento por rango de edad



Fuente: Elaboración propia

- En el siguiente clúster se observa una tendencia a un mayor conocimiento en ciudades principales con respecto a la antigüedad en la empresa:

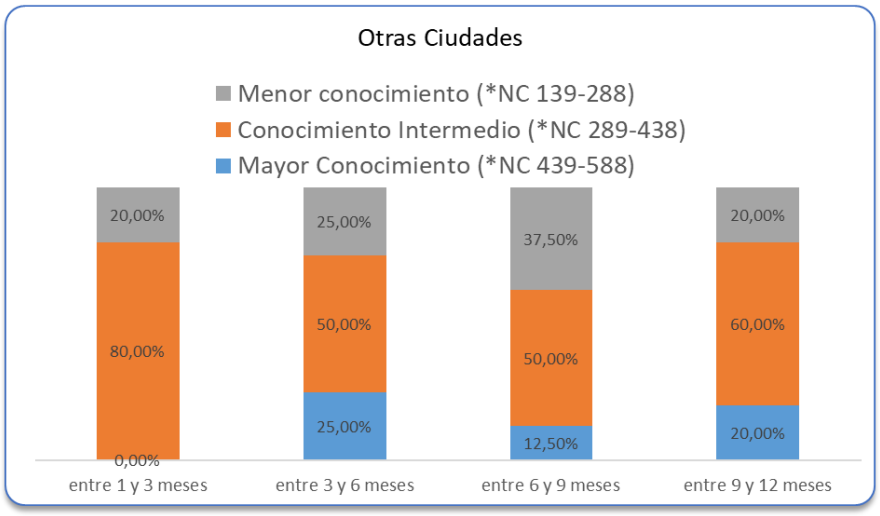
Figura 8: Conocimiento por tiempo de antigüedad en ciudades principales



Fuente: Elaboración propia

- En otras ciudades predomina el conocimiento intermedio en cuanto seguridad de la información y pasados los 3 meses se adquiere mayor conocimiento:

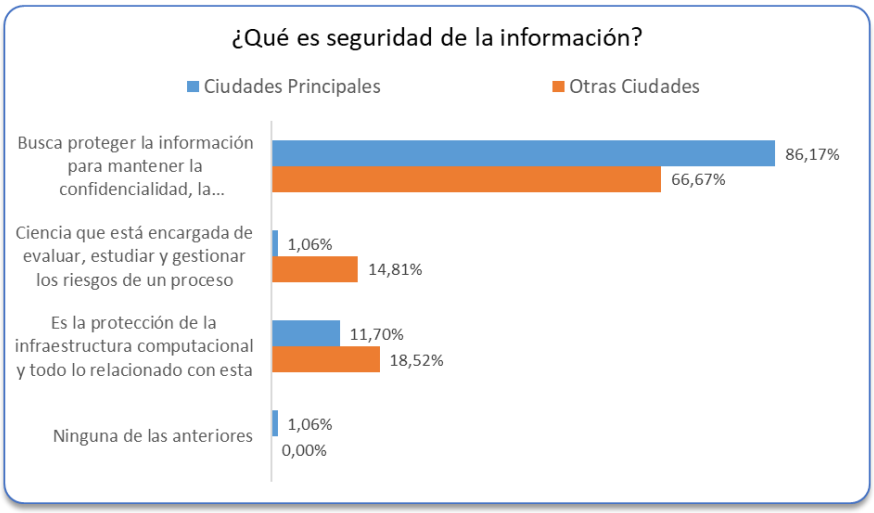
Figura 9: Conocimiento por tiempo de antigüedad en otras ciudades



Fuente: Elaboración propia

- En esta agrupación se observó que en las ciudades principales les fue mejor debido a que acertaron un 86% la respuesta de sobre que es seguridad de la información y en otras ciudades acertaron un 66%:

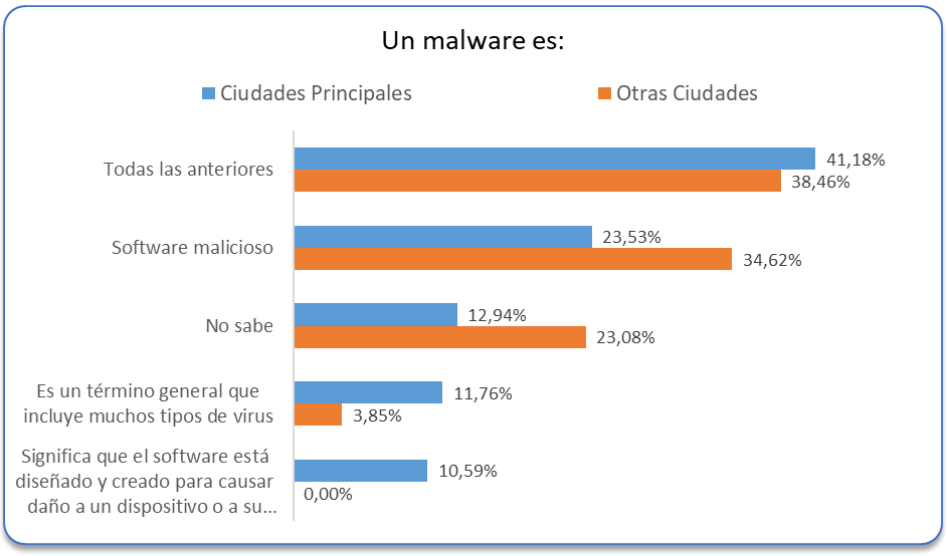
Figura 10: Empleados de COMTEC responden que es Seguridad de la Información



Fuente: Elaboración propia

- En la siguiente agrupación se preguntó ¿qué es un malware?, de forma general las respuestas no fueron acertadas, debido a que soló el 10.59% respondió correctamente en las ciudades principales.

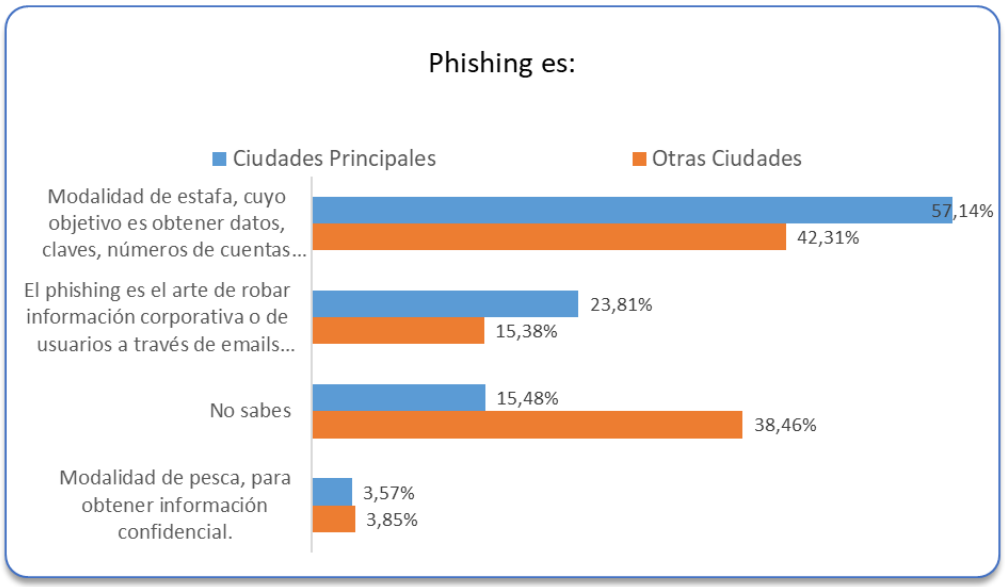
Figura 11: Empleados de COMTEC responden que es un malware



Fuente: Elaboración propia

- En esta agrupación se buscó validar que tanto sabían los empleados sobre phishing y el 15.48% respondió que no sabía en las ciudades principales y en otras ciudades el 38.46%:

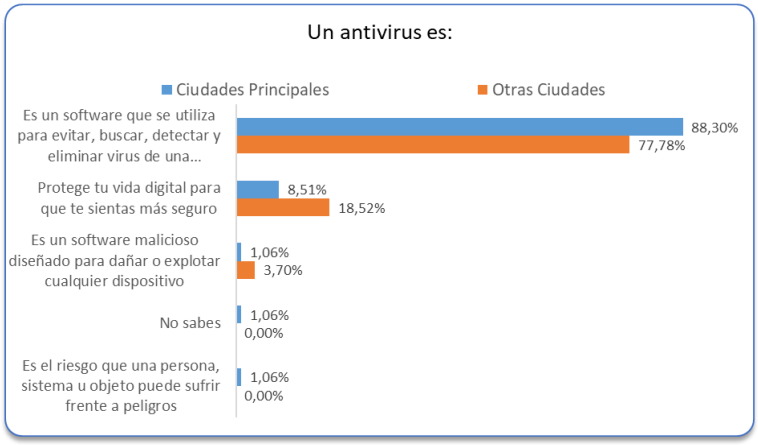
Figura 12: Empleados de COMTEC responden que es un Phishing



Fuente: Elaboración propia

- En esta agrupación, aunque el 88.30% y el 77.78% respondieron de forma acertada en las en las ciudades principales y otras ciudades; se identificó que el 3.18% es una brecha de seguridad que puede poner en riesgo la información debido a que el resultado no fue el acertado.

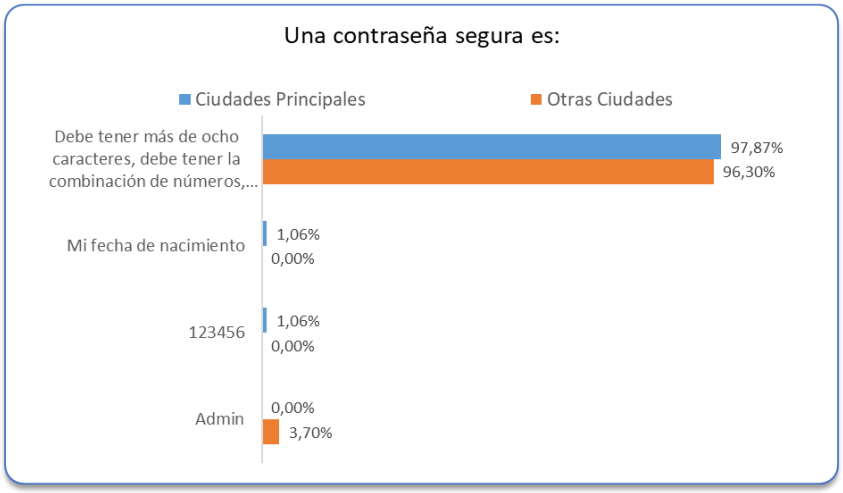
Figura 13: Empleados de COMTEC responden que es un antivirus



Fuente: Elaboración propia

- En la siguiente agrupación se identificó que el 97.87% y el 96.30% en las en las ciudades principales y otras respectivamente tienen el conocimiento para establecer una contraseña segura; sin embargo, con él 5.82% se debe reforzar el conocimiento.

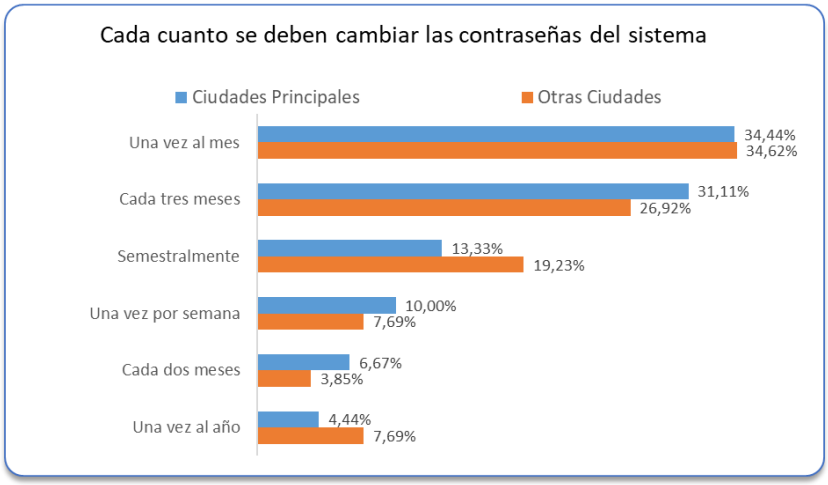
Figura 14: Empleados de COMTEC responden que es una contraseña segura



Fuente: Elaboración propia

- En esta pregunta se buscó determinar el nivel de conocimiento sobre los lineamientos y políticas de COMTEC; sin embargo, la siguiente agrupación respondió que el 34.44% y 34.62% consideran que la contraseña se debe cambiar una vez al mes.

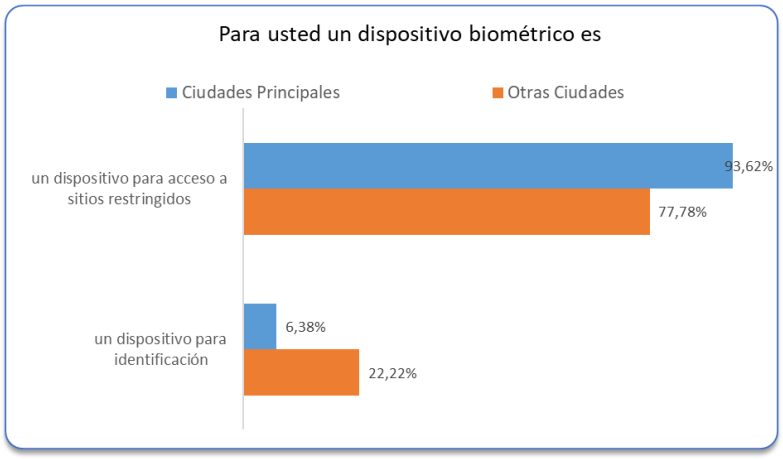
Figura 15: Empleados de COMTEC periodicidad cambio de contraseña



Fuente: Elaboración propia

- En esté agrupación se observó que el 93.62% correspondiente a ciudades principales y el 77,78% en otras ciudades, respondieron acertadamente con respecto a que es un dispositivo biométrico.

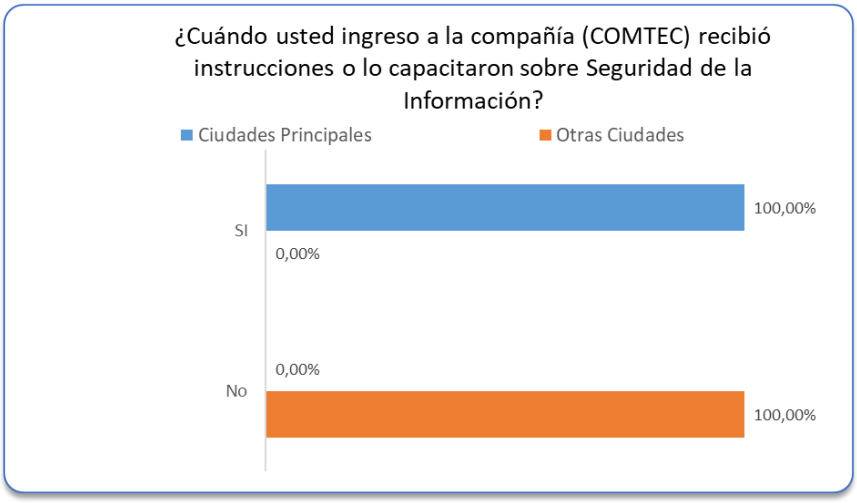
Figura 16:Empleados de COMTEC responden sobre un dispositivo biométrico



Fuente: Elaboración propia

- Según la siguiente agrupación se concluye que en la etapa de inducción se generaron capacitaciones sobre seguridad de la información al 100% en las ciudades principales y en otras ciudades se observó que el 100% no lo está realizando.

Figura 17: Empleados de COMTEC - capacitación al ingresar a la compañía



Fuente: Elaboración propia

8. CONCLUSIONES

- Inicialmente se esperaba que el proceso de encuestas se diera como resultado, un bajo conocimiento sobre seguridad de la información; sin embargo, en él desarrollo se ha encontrado que en diferentes grupos focales su nivel de conocimiento es medio y alto.
- Se sugiere a COMTEC evaluar los procesos de comunicación hacia los empleados de forma eficiente y eficaz para que se cumplan los objetivos establecidos en la política de seguridad de la información.
- Los rangos de edades entre 18 y 30 años tienen un mayor conocimiento en seguridad de la información; por lo cual, se pueden aprovechar las redes sociales para fortalecer los pilares de la información.
- Para personas mayores a 30 años, es importante trabajar a través de capacitaciones presenciales y/o virtuales de forma que se logre captar la atención del usuario final y fortalecer su conocimiento sobre seguridad de la información.
- Garantizar a los nuevos empleados dentro de su proceso de inducción, capacitaciones sobre las políticas, procesos y procedimientos de seguridad de la información.
- Es importante trabajar, como los usuarios entrenan su mente, para saber enfrentar un evento de seguridad, de un tema que ya se conoce; para esto, se sugiere realizar prácticas en ambientes controlados.

9. RECOMENDACIONES

1. Disponer de un plan de capacitación, en donde se recomienda considerar los siguientes aspectos:
   - **a.** Definir una periodicidad (una vez a la semana)
   - **b.** Hay que precisar que siempre sea el mismo día a la semana
   - **c.** Es importante que la información impartida no sea extenuante, larga o pesada para que su retención sea más eficiente.
   - **d.** Establecer una imagen o logo de seguridad de la información, en donde siempre debe visualizarse como parte de la campaña.
   - **e.** Definir temas semanales como, por ejemplo: Riesgos, política de seguridad, recomendaciones preventivas, conceptos de seguridad entre otros.

2. Evaluar los planes de entrenamiento que utiliza seguridad de la información para identificar si están enmarcados de forma globalizada y segmentar las capacitaciones dentro de las áreas de trabajo.

10. GLOSARIO

- **Ataque:** Es una práctica asociada a un software malicioso o persona que busca causar daños a la infraestructura y/o la información.
- **Campaña:** Es una serie de mecanismos y estrategias que busca comunicar o transferir determinada información.
- **Ingeniería Social:** Acciones que utilizan personas para obtener información de terceros y está puede ser utilizada con fines maliciosos.
- **Incidente:** Es un evento que puede afectar los pilares de seguridad de la información.
- **Muestra:** Es un grupo de datos, perteneciente a un universo de información.
- **Seguridad de la Información:** Busca proteger los pilares de la información.
- **Usuario Final:** Persona que utiliza la información de la entidad a través de diferentes medios.
- **Vulnerabilidad:** Brecha de seguridad que puede ser utilizada para realizar un ataque.

11.BIBLIOGRAFÍA

Chávez, J. D. (2021). *Aspectos interesantes sobre la Ingeniería Social*.

Cúbides, L. A. (21 de Septiembre de 2021). Que piensa sobre la protección de la información. (C. Romero, Entrevistador)

MINTIC. (5 de junio de 2016). *Guía Metodológica de Pruebas de Efectividad.* Obtenido de Seguridad y Privacidad de la Información: https://mintic.gov.co/gestionti/615/articles-5482_G1_Metodologia_pruebas_efectividad.pdf

MINTIC. (2016). *Módelo de Seguridad de TI.* Obtenido de Seguridad de TI: https://mintic.gov.co/gestion-ti/Seguridad-TI/Modelo-de-Seguridad/

MINTIC. (29 de 07 de 2016). *Modelo de Seguridad y Privacidad de la Información.* Obtenido de https://mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf

MINTIC. (17 de Marzo de 2016). *Plan de capacitación, sensibilización y comunicación de Seguridad de la Información.* Obtenido de Seguridad y Privacidad de la Información: https://mintic.gov.co/gestionti/615/articles-5482_G14_Plan_comunicacion_sensibilizacion.pdf

Poggi, N. (19 de Mayo de 2021). *The Missing Report*. Obtenido de Prey Project: https://preyproject.com/blog/es/30-estadisticas-seguridad-informatica/

SGS, I. 2.-2. (s.f.). TECNOLOGÍA DE LA INFORMACIÓN. TÉCNICAS DE SEGURIDAD. SISTEMAS DE GESTIÓN DE LA. *VISIÓN GENERAL – ISO 27001:2013*. Esta no es la Norma Original, es una Interpretación de SGS Colombia S.A., División S&SC.