ANÁLISIS DEL RIESGO DE ATAQUES DE INGENIERÍA SOCIAL EN LA SECRETARIA DE EDUCACIÓN DEL DEPARTAMENTO DE NARIÑO, PARA LA IDENTIFICACIÓN DE NECESIDADES DE FORMACIÓN DEL PERSONAL Y ASÍ REDUCIR SU IMPACTO

MARLODY GÓMEZ URBANO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
CEAD PASTO JULIO DE 2020

ANÁLISIS DEL RIESGO DE ATAQUES DE INGENIERÍA SOCIAL EN LA SECRETARIA DE EDUCACIÓN DEL DEPARTAMENTO DE NARIÑO, PARA LA IDENTIFICACIÓN DE NECESIDADES DE FORMACIÓN DEL PERSONAL Y ASÍ REDUCIR SU IMPACTO

MARLODY GÓMEZ URBANO

Monografía para optar el título de Especialista en Seguridad Informática

Directora
Ing. Yenny Stella Nuñez Alvarez

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
CEAD PASTO JULIO DE 2020

Nota de Aceptación

_____

_____

_____

_____

_____

Firma del presidente del Jurado

_____

_____

Firma del Jurado

_____

Firma del Jurado

Pasto Nariño, 2019

RESUMEN

A continuación se presenta un análisis del riesgo de ataques de ingeniería social en la Secretaria de Educación del Departamento de Nariño, para la identificación de necesidades de formación del personal y así reducir su impacto, con el cual se busca recabar información pertinente para lograr la identificación de las amenazas, debilidades y técnicas de ataques de la ingeniería social, sé pretende que quede entendido la gravedad de esta vulnerabilidad en esta entidad y evaluar el nivel de seguridad; esta entidad se limita a sus propias políticas de seguridad al nivel tecnológico como corta fuegos, antivirus, autenticación biométrica, pero no tiene en cuenta que esta vulnerabilidad puede obtener la información confidencial que maneja esta Secretaria.

El método de estos ataques se basa en la manipulación psicológica, los cibercriminales los usan para engañar a los usuarios y lograr que proporcionen datos importantes y así obtener información confidencial de la entidad o personal y luego hacer uso de esta para beneficio propio; esta práctica se ha convertido en una de las principales herramientas para que los ciberdelincuentes a causa de las nuevas tecnologías que actualmente invade la realidad, sean aprovechadas para realizar los diferentes fraudes u crímenes tecnológicos. Por lo expuesto anteriormente, debe informar a que riesgos se está más vulnerable, la manera de prevenirlos y que medidas de seguridad permiten reducir esos riesgos y poderlo aplicar en esta entidad de educación.

.

.

ABSTRACT

Below is an analysis of the risk of social engineering attacks in the Secretary of Education of the Department of Nariño, for the identification of training needs of the staff and thus reduce their impact, with which it seeks to gather relevant information to achieve the identification of the threats, weaknesses and techniques of attacks of social engineering, I know aims to ensure that the seriousness of this vulnerability in this entity is understood and to evaluate the level of security; this entity is limited to its own security policies at the technological level such as fire cuts, antivirus, biometric authentication, but does not take into account that this vulnerability can obtain the confiden-cial information handled by this Secretary.

The method of these attacks is based on psychological manipulation, cybercriminals use them to deceive users into providing important data and thus obtaining confidential information from the entity or personnel and then making use of it for their own benefit; this practice has become one of the main tools for cybercriminals because of the new technologies that currently invade reality, are used to carry out the different frauds or technological crimes. Therefore, it should be reported that risks are most vulnerable, how to prevent them and that security measures allow to reduce those risks and be able to apply it in this educational body.

TABLA DE CONTENIDO

Pág.

LISTA DE TABLAS

pág.

LISTA DE GRAFICAS

pág.

LISTA DE ANEXOS

1 INTRODUCCIÓN

En la actualidad la seguridad de la información es una de las características que priman en el entorno de cualquier organización ya sea pública o privada y de personas naturales, el uso de las tecnologías de la información a traído consigo mismo mayores riesgos, y de igual manera la gran necesidad de protegerse de las amenazas, ataques y de toda vulnerabilidad; es necesario tener en claro que la información su totalidad es el activo más importante y está en riesgo por lo tanto es de vital importancia tomar reglas y medidas que tengan como finalidad proteger y resguardar la información y no exponga su integridad, disponibilidad y confidencialidad

Para llevar a cabo este proceso, es necesario la sensibilización, la formación y cultura del personal de cada organización; el desconocimiento de los ataques y técnicas para obtener información de los sistemas por si, solo abre una brecha de inseguridad en los mismos, donde los vándalos informáticos que se dedican a buscar debilidades en los sistemas de información para logran obtener datos y entrar de manera ilegal a ellos, y obtener su propio beneficio; estos sistemas se pueden implementar con herramientas idóneas para llevar un buen proceso, para así evitar ser víctima de las técnicas que utilizan los delincuentes informáticos que exploran las debilidades de cada una de las organizaciones o entidades.

Con el objetivo de mitigar este tipo de riesgo, las organizaciones o entidades como es el caso de la Secretaria de Educación Departamental de Nariño se mira la gran necesidad de que todo el personal se forme y se concientice sobre los problemas y riesgos que existen, como las vulnerabilidades, tipos de ataques y amenazas informáticas, donde por falta de conocimiento involucran y provocan un alto riesgo de llegar a ser víctimas de todos los delitos informáticos a los que se está expuesto

ya que no se cuenta con medias o esquemas de seguridad necesarias para mitigar el riesgo y evitar comprometer datos de tipo sensible y confidencial de esta entidad

Las personas son vulnerables a la manipulación y engaño, y más cuando desconocen ciertas terminologías y conceptos, que utilizan los vándalos informáticos para aprovecharse de la falta de conocimiento del usuario, y así poder realizar un ataque a su sistema de información. Desafortunadamente la mayoría de los usuarios, no tienen la suficiente capacitación y formación para identificar un ataque como es la INGENIERÍA SOCIAL.

Para llevar a cabo este peligroso ataque sólo se necesitan dos cosas indispensables: Un Sistema de Información y una víctima, todos los incidentes de seguridad conllevan un error humano donde los ciberdelincuentes aprovechan la debilidad humana para atraer diferentes miembros de organizaciones, logrando de esta forma identificar los puntos fuertes y débiles de personas externas para que incautamente les suministren acceso de información delicada, en conclusión la ingeniería social es el empleo de técnicas y acciones premeditadas que permitan manipular las acciones de las personas para lograr que realicen tareas que naturalmente no harían.

Teniendo en cuenta que la Ingeniería social es el ataque informático más peligroso es necesario que las entidades, como ha dicho anteriormente se concienticen y generen cultura de formación sobre el uso correcto que se debe dar a las tecnologías de la información, logrando así que todo el personal coadyude a neutralizar o contrarrestar los delitos que se ejecutan por medio de ataques correspondiente a ingeniera social y evitando que atacantes cumplan su objetivo

2 TÍTULO

ANÁLISIS DEL RIESGO DE ATAQUES DE INGENIERÍA SOCIAL EN LA SECRETARIA DE EDUCACIÓN DEL DEPARTAMENTO DE NARIÑO, PARA LA IDENTIFICACIÓN DE NECESIDADES DE FORMACIÓN DEL PERSONAL Y ASÍ REDUCIR SU IMPACTO.

3 DEFINICIÓN DEL PROBLEMA

3.1 PLANTEAMIENTO DEL PROBLEMA

En todas las organizaciones se maneja información importante ya sea la de los usuarios o de las personas que hacen parte de la entidad, o como es el caso de la Secretaria de Educación Departamental de Nariño , las cuales dependen una u otra manera de las tecnologías de la información, como una de las herramientas más esenciales para lograr sus objetivos y el desarrollo de las actividades en su vida cotidiana; donde al mismo tiempo todos tienen que enfrentarse con una amplia gama de amenazas y vulnerabilidades asociadas a los entornos informáticos de hoy.

Para los múltiples tipos de vulnerabilidades a los que se está expuesto se debe tomar medidas preventivas y reactivas en las organizaciones, junto con el recurso humano y los sistemas tecnológicos; se le debe brindar la protección necesaria y pertinente para mantener, resguardada y protegida la información, buscando mantener la confidencialidad, la disponibilidad e integridad de datos y de la misma manera asegurando su precisión y confiabilidad.

Cada día son más comunes los ataques informáticos, y la gran mayoría enfocados a la Ingeniería Social que con sus diferentes técnicas toman control del objetivo de ataque, con fines delictivos ya sea para tomar el control de la información robo o suplantación de identidad, entre otros.

Por ello es de vital importancia que en la Secretaria de Educación del Departamento de Nariño se tenga en cuenta que la Ingeniería Social es un problema que afecta a todos, sus distintos métodos y técnicas, la falta de información, divulgación y

capacitación hace que la entidad este corriendo riesgo de su información; para proteger esa información de todos los procesos y los medios que las contienen la mejor protección es el conocimiento a la seguridad a través de la educación, el único camino verdadero para reducir el efecto de estos ataques es saber que existen, para conocer cómo es su naturaleza para entender el proceso de pensamiento y de la mentalidad de las personas que hacen tales cosas, y así poder mantener esa actitud de precaución y alerta en su cotidianidad laboral porque los empleados son la última barrera del sistema de defensa de la seguridad de las organizaciones u entidades.

3.2 FORMULACIÓN DEL PROBLEMA

¿Como puede reducir el impacto de la ingeniera social en las organizaciones, implementado planes de capacitación al personal de la Secretaria de Educación Departamental de Nariño?

4 JUSTIFICACIÓN

Con respecto a Seguridad Informática ,la ingeniería social se ha convertido en una de las técnicas más utilizadas en diferentes acciones para vulnerar la seguridad y obtener información confidencial a través de la manipulación de usuarios legítimos, como investigadores privados, criminales, o delincuentes informáticos, para obtener información, acceso o privilegios en sistemas de información que les permitan realizar algún acto que perjudique o exponga a personas, empresas u organizaciones comprometido a riesgo o abusos de ataque cibernético, y vender la idea a identificar.

Por lo anterior expuesto es de gran importancia realizar una investigación monográfica la necesidad de formación para el personal de la Secretaria de Educación del Departamento de Nariño en Seguridad Informática y ejecución de las diferentes técnicas, modalidades y métodos enmarcados dentro de llamada Ingeniería Social; donde se evidencia que esta entidad no capacitan a su personal de esta gran vulnerabilidad de seguridad informática y a un más teniendo en cuenta que la Ingeniería Social es el ataque informático más peligro en la actualidad, donde existen constantes amenazas de personas que quieren hacer uso de la información. Este tipo de fraude manipula psicológicamente a personas para que compartan información de mayor confidencialidad o hagan acciones inseguras; en muchas ocasiones, los ataques delictivos se realizan por medio de correos electrónicos y telefónicamente, con el fin de convencer a la víctima y sacar información sensible de la organización u entidad.

Como es un tema más humano, y teniendo encueta que las herramientas tecnológicas que implementan las compañías no pueden prevenir los diferentes ataques a los que está expuesto, por tal razón los atacantes recurren a este tipo de tácticas para vulnerar sistemas muy seguros y complejos que cada entidad posee.

Los vándalos informáticos llamados “CRACKERS” que se dedican a buscar debilidades en los sistemas de información para obtener datos que le ayuden a entrar de manera ilegal en ellos y obtener beneficio de estos.

Mirando las constantes amenazas de personas que quieren hacer uso de la información para su beneficio, se bebe tomar medidas de prevención y seguridad que nos permitan reducir esos riesgos de la seguridad informática, dirigido esta entidad que se brinde la formación funcionarios y eduquen en las diferentes técnicas de la ingeniería social para lograr identificar y mitigar sus riesgo, amenazas y todas las vulnerabilidades que se presenten a raíz de estas técnicas que buscan instrucciones a los datos o información sensible; siendo la información el activo más importante de las entidades u organizaciones y el cual necesita protección para lo cual se establecen diferentes tipos de controles para asegurar al máximo, por las anteriores razones es en este punto donde se debe preparar el personal y estar capacitados con medidas necesarias para proteger privilegio de la información y sensibilizar de que la seguridad debe ser la prioridad.

5 OBJETIVOS

5.1 OBJETIVO GENERAL

Realizar un análisis de formación en la actualidad de Ingeniería Social para generar propuestas de capacitación

5.2 OBJETIVOS ESPECÍFICOS

- ✓ Realizar un estudio sobre la ingeniería social y su desarrollo en la actualidad.
- ✓ Realizar un estudio sobre estrategias desarrolladas por instituciones relacionadas con capacitación en seguridad e ingeniería social.
- ✓ Realizar un análisis de brecha para identificar el nivel de conocimiento en cuestión de seguridad de la información por parte del personal de la secretaria de educación de Nariño.
- ✓ Diseñar una propuesta de plan de capacitación en seguridad de la información que permita reducir los riesgos de ataques en ingeniería social en la secretaria de educación de Nariño.

6 DELIMITACIONES

6.1 DELIMITACIÓN GEOGRÁFICA.

La secretaria de Educación Departamental de Nariño se encuentra situada en la Carrera 42B N.º 18º A-45, Barrio Pandiaco Municipio de Pasto, capital del Departamento de Nariño _ Colombia.

6.2 DELIMITACIÓN CONCEPTUAL

Esta monografía tiene como principal objetivo realizar un análisis de Seguridad Informática e ingeniería social en La Secretaria de Educación Departamental de Nariño; con el propósito de saber el grado de conocimiento en Seguridad Informática, para llevar a cabo este propósito se indagara a los funcionarios de esta entidad para evaluar el nivel de conocimiento, después de culminar esta labor investigativa y observando las debilidades encontradas se pretende que la Secretaria de Educación Departamental de Nariño busque implementar estrategias de protección y de la información y se concienticen en la importancia la formación y la capacitación en debilidades y los diferentes temas vulnerables encontrados.

7 MARCO REFERENCIAL

El contenido de este marco de referencia se basa en la recuperación y análisis documental que permitirán un entendimiento de los conceptos de Seguridad Informática y su aplicabilidad como pertinencia en dependencias gubernamentales.

7.1 MARCO TEÓRICO

Durante esta nueva era se han realizado grandes avances en las tecnologías de la información y Comunicación, donde las organizaciones o entidades han mirado la necesitada de tomar estas herramientas para el desarrollo organizacional de cada entidad, donde diariamente se miran amenazadas por delincuentes informáticos que aprovechan toda clase de vulnerabilidades en los sistemas de información, representando daños económicos y a su vez la confiabilidad o imagen institucional y gubernamental. Para ellos es muy importante entender y comprender los diferentes conceptos de seguridad para lograr combatir y protegerse de posibles ataques a la información como es la ingeniera social.

Las instituciones o entidades no son ajenas a este tipo de flagelo, en tanto que sus sistemas informáticos contienen recursos de alto valor estratégico para la seguridad y defensa, tales como: Información financiera, datos personales, datos administrativos, datos jurídicos entre otros, por lo que se hace necesario la identificación, individualización y generación estrategias, políticas y medidas de contención de las posibles amenazas a las cuales se ven enfrentadas todo el tiempo.

Así mismo, estos grandes avances en las tecnologías de la información y comunicación vienen acompañados por una evolución en la sofisticación y complejidad de los ataques a los que se ven sometidos, lo cual se ha visto evidenciado en un aumento sustancial en la cantidad y tipos de ataques informáticos

a nivel mundial de los últimos años, así como el nivel de impacto que estos generan, a saber, algunos de ellos:

7.1.1 Ingeniería Social

Muchas de estas técnicas que se utilizan para obtener la información de forma ilegal tienden a considerar la utilización de herramientas, equipos y mecanismos y con amplios conocimientos técnicos y con una gran experiencia para que los ataques sean efectivos, a pesar de que la que hoy en día, "Según Flor Angel, Hernadez la llamada Ingeniera social ataca directamente al principal dominio como es considerado eslabón más débil dentro de la seguridad informática: el usuario o personal de la entidad u organización"[1]

Teniendo en cuenta que las nuevas tecnologías han permitido que la brecha entre usuarios y máquinas sea cada vez menor también se han visto en la gran necesidad en el desarrollo de crear mecanismos para el intercambio de la información de maneras rápidas, sencillas y fáciles conllevando al personal mayor confiabilidad.

7.1.2 Tipos de ingeniería social

Básicamente, se conocen dos tipos de ingeniería social. La primera basa sus técnicas en la interacción humana para aprovechar debilidades y obtener a través de ella la información deseada. La segunda se basa en los dispositivos y el uso del Internet. computadoras e intenta obtener información a través de programas informáticos.

7.1.3 Ingeniería social basada en personas

Esta ingeniería social "según INCIBE se basa en personas con el fin de explorar,

1. Hernández, Pérez, Flor Ángel, and Zaldívar, Pedro M Ricardo. Glosario de Términos Informáticos, edited by Flores, Miguel (ed.) Sosa, El Cid Editor, 2006. Disponible en, http://ebookcentral.proquest.com/lib/unadsp/detail.action?docID=3167493.

conocer y la información que necesitan utilizando tácticas de manipulación de emociones, aplican teorías psicológicas y promover sentimientos y/ o necesidades del diario vivir y lograr conseguir su objetivo final baje la guardia o sus defensas y den paso a acceder a la información sin darse cuenta alguna"[2]

Los delincuentes informáticos que utilizan que utilizan los ingenieros basas en personas son conocedores que todos como humanos tenemos miedos, necesidades y debilidades las cuáles son reflejadas inevitablemente.

7.1.4 Ingeniería social basada en la web

Esta clase de Ingeniería social se base en la Web," hace uso de sitios web o correos electrónicos ilegales obteniendo así datos confidenciales y sensibles, logrando imitar las características de comunicación institucional la perfección de actuación de los piratas o delincuentes informáticos engañan por completo a los usuarios o personal legitimo obteniendo los datos sensibles de la organización."[3]

La ingeniería social independientemente del método a utilizar su principal objetivo es de atraer y convencer a la persona por medio de cualquier forma de manipulación aprovechando el desconocimiento de los usuarios o personal que tiene con respecto a la seguridad de la información

7.1.5 Técnicas de Ingeniería Social en la Seguridad Informática

En la figura siguiente, se presenta una clasificación de las "técnicas usadas en

[2] INCIBE. (12 de 05 de 2014). La ingeniería social en la empresa: aprovechando la naturaleza humana. Obtenido de https://www.incibe.es/protege-tu-empresa/blog/ingenieria-social-en-empresas

[3] Roa, Buendía, José Fabián. Seguridad informática, McGraw-Hill España, 2013. disponible en, http://ebookcentral.proquest.com/lib/unadsp/detail.action?docID=3211239.

ingeniería social, identificar las técnicas de la Ingeniería Social nos ofrecen la ventaja de aprender aquellas habilidades para lograr comprender, verificar y analizar la forma en que los atacantes o criminales informáticos lleven a cabo su objetivo y tener lo máximo de claridad que es fundamental que el personal de la organización o entidad se concientice. No tan sólo en el cumplimiento de las políticas que se hayan implantado, sino también teniendo una actitud de precaución y vigilar en el uso frecuente de los sistemas de información, tanto en lo personal como en lo laboral. Los Empleados que labora n en una entidad es la última barrera del sistema de defensa de la seguridad, por tal razón eso los ciberdelincuentes diseñan su sistema de ataque enfocado y orientado a el eslabón más importante de la entidad como es el personal quien son los más vulnerables de robo de la información."[4]

[4] Pandasecurity.com. (15 de 09 de 2015). Técnicas de ingeniería social: ¿cuáles son y cómo evitarlas en las empresas? Obtenido de https://www.pandasecurity.com/spain/mediacenter/seguridad/ingenieria-social-empresas/

Grafica 1 Técnicas de Ingeniería Social

Fuente: https://deepwebiupsm.files.wordpress.com/2016/06/deepweb11.jpg

7.1.6 Tácticas de la ingeniería social

"Son muchos los riegos que existen a consecuencia de las tácticas de la ingeniería social en una entidad u organización debido a que cada una de ellas ingeniosamente manipula de una manera mañosa con el principal objetivo de robo de la información haciendo que las victimas realicen ciertas acciones que divulguen información personal o de una entidad muchas de ellas con fines lucrativos.[5]

- ✓ **Bombas Lógicas**: Estas son aplicaciones o programas que se activan en momento predeterminado utilizados por los atacantes informáticos para la destrucción de sistemas; este permanece oculto hasta cumplir una o más condiciones pre programadas y ejecutar la acción delictiva, este ataque pude activar en un momento especifico y en varios equipos al mismo tiempo, entre

[5] Yulienth,R. R. (Junio de 2018). Reposorio. Obtenido de http://openaccess.uoc.edu/webapps/o2/bitstream/10609/81255/6/jrodriguezrinTFM0618memoria.pdf

una de las acciones más maliciosas que este ataque puede realizar están: eliminar información del disco duro, expandiendo virus en el PC que se aloja y en las que estén conectadas a la misma red y ser víctimas de las diferentes vulnerabilidades que deja este ataque.

- ✓ **Backdoors:** "son una de las herramientas con una secuencia especial dentro del código de programación que permiten al atacante tener acceso al sistema controlándolo y permitiendo hacer lo que desee con él con sus fines maliciosos y de espionaje, utilizándolos como medio de conexión al momento de ser ejecutado convirtiéndose en peligrosa vulnerabilidad dentro de una infraestructura informática."[6]

- ✓ **Troyanos: "**es un tipo de programa malicioso que se camufla con el fin de engañar al usuario disfrazándose de programas como software o archivos legítimos con el objeto de causar daño irreversible destruyendo la información del PC o robar o captura de datos y renviar información confidencial y personal a una dirección externa. Estos ciberdelincuentes utilizan estas herramientas para robar datos bancarios, nombres de usuarios y contraseñas y otros".[7]
- ✓ **Botnets:** "es una red de ordenadores y dispositivos conectados entre sí controlados por un o grupo atacantes o piratas informáticos que son utilizados para él envió de SPAM, para crear o difundir ataques como denegación de servicios e instalar cualquier programa maligno en la red teniendo en cuenta que estos se ejecutan de manera autónoma y automática

---

[6] HERNANDEZ P , F. A. (2006). *Glosario de terminos Informaticos*. Obtenido de http://ebookcentral.proquest.com/lib/unadsp/detail.action?docID=3167493

[7] Latam.kaspersky.com. (s.f.). *Qué es un virus troyano.* Obtenido de https://latam.kaspersky.com/resource-center/threats/trojans

los ciberdelincuentes pueden administrar de manera remota y causar daños irreparables."[8]

- ✓ **Ransomware:** "Es un software malicioso que restringe el acceso a determinadas parte de la información o archivos del sistema operativo infectado es decir realiza una especie de secuestro de la información de la víctima y pide rescate a cambio de quitar la restricción o el acceso a ella".[9]

Una vez que el ransomware está alojado en el equipo, comienza a encriptar los archivos que el usuario comúnmente utiliza para realizar sus actividades diarias: archivos pdf, doc, xls, jpg y similares, generando un cifrado de tipo asíncrono, donde se genera una llave privada y una llave pública. Una de estas llaves tiene la capacidad de encriptar los archivos y la otra de desencriptarlos, por lo que, el atacante, almacena la llave que se utilizará para desencriptar los archivos, en un servidor externo, no accesible para la víctima. Una vez que el pago se haya realizado, según el atacante, se le entregará la llave de desencriptación a la víctima para que recupere sus archivos. Existe un plazo de tiempo para realizar el pago del rescate, de excederse el tiempo, el atacante amenaza con eliminar la llave de desencriptación, que, de suceder, será imposible eliminar el algoritmo de cifrado aplicado a los archivos. A finales del 2014 e inicios del 2015, este ataque se hizo común, afectando mayormente a México en el área

---

[8] *CIBERSEGURIDAD. RETOS Y AMENAZAS A LA SEGURIDAD NACIONAL EN EL CIBERESPACIO.* (Diciembre de 2010). Obtenido de http://www.ieee.es/Galerias/fichero/cuadernos/CE_149_Ciberseguridad.pdf

[9] INCIBE_PTE_AproxEmpresario. (2017). 〉 Ransomware: una guía de aproximación para el empresario. *Press Star INSERT BITCOIN_007_Ransomware-2017-v1*, 25.

latinoamericana."[10]

7.1.7 Metodología de la Ingeniería Social

"La ingeniería social cumple con unas fases o estructuras que permiten que el ataque sea exitoso, a consecuencia involucra la privacidad, protección de la información y comunicación de una organización de una entidad y también la personal, haciendo uso de sofisticadas técnicas de la Ingeniera Social para manipular y persuadir a las personas para que accedan a sitios de información restringidos y robar la información.

A relación a esto se presenta las fases o pasos de un ataque informático.

- ✓ **Paso 1. Identificar a la víctima**: el atacante planea su objetivo y promueve la estima de las diferentes probabilidades de éxito del ataque al ser ejecutado ya sea una organización, entidad o ataque personal

- ✓ **Paso 2. Reconocimiento:** después de tener presente el blanco del ataque el atacante inicia en busca de la información o en busca del anzuelo de datos de su objetivo que pueda utilizar para su ataque. Esta información la puede obtener por medio de teléfono, redes sociales, en la basura de la víctima entre otros.

- ✓ **Paso 3. Crear el escenario:** para dar este paso depende del ingenio del atacante y mirando la clase de seguridad existente del objetivo de ataque donde quieres ingresar.

- ✓ **Paso 4. Realizar el ataque:** para este paso el delincuente informático coloca

[10] RedUSERS. (04 de diciembre de 2015). Ingeniería Social y cuáles son sus tipos de ataque. Obtenido de http://www.re-dusers.com/noticias/ingenieria-social-cuales-son-los-tipos-de-ataque/

en práctica las diferentes técnicas de la ingeniería social para hacerse amigo de la víctima y ganarse la confianza.

- ✓ **Paso 5. Obtener la información:** teniendo ya su control o el acceso al objetivo, el ingeniero social procede a hacer su uso de la información que necesitaría utilizando los diferentes medios de almacenamiento y hacer el control que requiera el atacante.
- ✓ **Paso 6. Salir:** después de llevar a cabo su meta, el delincuente informático procede a dar por cumplido objetivo."[11]

7.2 MARCO CONCEPTUAL

7.2.1 Seguridad Informática

"La falta de control y deficiencia de una política de seguridad informática son un atractivo para los cibercriminales. Las entidades públicas como privadas y en este caso la entidad en mención, mantienen depósitos de datos sensibles de todos los procesos que lo constituyen. La falta de personal capacitado, la falta de inversión en seguridad y la no adecuada implementación de soluciones de seguridad coloca en riesgo los datos confidenciales que se maneja pueden ser objeto a diversos tipos de amenazas o peligros. Es allí donde la seguridad informática tiene sus raíces, ya que esta disciplina busca la protección tanto física como lógica de todo tipo de información almacenada, para garantizar su disponibilidad, confiabilidad e integralidad.

Con el desarrollo de las tecnologías de la información, los datos económicos, tecnológicos o de prácticamente cualquier área pueden ser indexados y explotados

[11] JIMÉNEZ, R. M. (04 de 06 de 2019). Estudio de metodologías de Ingeniería Social. Obtenido de http://openaccess.uoc.edu/webapps/o2/bitstream/10609/81271/6/rmarinjTFM0618memoria.pdf

por sistemas de informáticos, donde al estar interconectados en la red informática "[12]

7.2.2 Seguridad Física

La plataforma base de todo sistema informático está en su hardware, el cual permite realizar el almacenamiento e interacción transaccional de los datos contenidos en él con otros sistemas informáticos o simplemente con un usuario final, por lo cual se hace necesario tomar las medidas preventivas tanto pasivas como activas para asegurar la disponibilidad de este activo como de sus contenidos.

Estas medidas deben evaluar y mitigar el riesgo generado por el entorno de los componentes físicos del sistema, tales como; Instalaciones, condiciones atmosféricas, Electricidad, personal autorizado, entre otros. [13]

7.2.2.1 Seguridad Lógica

"El Software y/o la información almacenada en un sistema informático no solamente requiere una protección física que asegure el medio de almacenamiento, sino que también requiere medidas de seguridad que prevengan daños o modificaciones no autorizadas de los registros o datos contenidos, así como de la intrusión no consentida a ellos."[14]

Este tipo de seguridad tiene gran relevancia en la actualidad debido a que la gran mayoría de los sistemas informáticos existentes permiten un acceso no solamente físico en sitio a ellos, sino que también un acceso remoto a través de cualquier

---

[12] Escrivá, Gascó, Gema, et al. Seguridad informática, Macmillan Iberia, S.A., 2013. Disponible en, http://ebookcentral.proquest.com/lib/unadsp/detail.action?docID=3217398

[13] GOV.CO, M. (Código: ST-MA-02). MANUAL DE SEGURIDAD INFORMÁTICA. *Versión: 02,* 43. Obtenido de https://www.mineducacion.gov.co/1759/articles-322548_Manual_de_Seguridad_Informatica_.pdf

[14] Baca, Urbina, Gabriel. Introducción a la seguridad informática, Grupo Editorial Patria, 2016. disponible http://ebookcentral.proquest.com/lib/unadsp/detail.action?docID=4849850

terminal conectada a la red mundial ya sea un computador o simplemente un teléfono celular, por lo cual es importante la generación de políticas y procedimientos de accesibilidad a la información.

7.2.3 Características de la Información

"Para cualquier empresa u organización uno de sus activos más importantes, es la información, la cual dependiendo de su razón social tiene unas características especiales, sin embargo, para que cualquier sistema informático sea altamente confiable"[15], su información debe cumplir con las siguientes características:

- ✓ **Integridad: "**la información al ser compuesta por una secuencia de código puede verse modificada o disminuida por una intrusión o falla en el sistema informático, por lo cual este principio exige que la información contenida sea válida, precisa y completa

- ✓ **Disponibilidad:** los sistemas informáticos en una organización permiten la acumulación y análisis de grandes cantidades de información para el negocio, por lo cual no solamente se requiere contar con los recursos físicos de almacenamiento, si no también todos los recursos necesarios para la accesibilidad y explotación de. datos, el principio de disponibilidad busca asegurar el acceso a los datos almacenados en el momento y lugar que requiera la organización". [16]

[15] Cecilia, M. P. (2013). Revista de Ingeniarías. USBMed, Vol.4, N.º 2, Julio-diciembre, 65.

[16] Excellence, B. e. (28 de Mayo de 2018). *Blog especializado en Sistemas de Gestión*. Obtenido de https://www.pmg-ssi.com/2018/02/confidencialidad-integridad-y-disponibilidad/

- ✓ **Eficiencia: “**la acumulación o almacenamiento de grandes cantidades de información requieren de la generación de políticas y procedimientos que permitan el uso eficiente de todos los recursos físicos y lógicos del sistema informático, así logrando tiempos de respuesta cortos y con resultados altamente fieles”.[17]

- ✓ **Efectividad: “**para que el desarrollo de las actividades de cualquier organización sea optimo, es necesario que la información explotada o consultada para la toma de decisiones, tenga todas las características de consistencia y fiabilidad para tal fin”.[18]

- ✓ **Confidencialidad:** el acceso selectivo de la información es un factor para tener en cuenta, dentro y por fuera de las organizaciones. Este acceso selectivo permite mitigar el riesgo de fuga o perdida de información, evitando perdidas de todo tipo.

- ✓ **Apego a los Estándares:** t”eniendo en cuenta que las actividades de toda organización deben estar acorde a las leyes, normatividad vigente y acuerdos contractuales, según sea el caso, así mismo el contenido de sus sistemas informáticos deben cumplir los parámetros definidos en los acuerdos generales, como en cada caso se determine”.[19]

---

17 GONZALEZ, R. H. (2011). *Conocimiento, Innovacion y Desarrollo*. Obtenido de http://www.casatic.org/wp-content/uploads/2015/03/RafaelHerreraCR_conocimiento.pdf

18 Marianela., A. (s.f.). *Planificación Estratégica e Indicadores de Desempeño en el Sector Público*. Obtenido de cepal.org/ilpes/noticias/paginas/5/39255/30_04_MANUAL_COMPLETO_de_Abril.pdf

19 ING., A. A. (2011). *C.V.S.* Obtenido de POLITICAS Y NORMAS DE SEGURIDAD INFORMiTICA : https://www.cvs.gov.co/jupgrade/images/stories/docs/Alertas/Politicas_de_Seguridad_Informatica_CVS_2011-.pdf

- ✓ **Confiabilidad: “**la veracidad de la información tratada o arrojada por un sistema informático permite a las organizaciones la correcta toma de decisiones y la apropiada prestación de servicios a sus consumidores, por lo cual es requerido la generación de prácticas que permitan determinar con exactitud la trazabilidad de datos, que generen confianza al usuario”.[20]

7.2.4 Riesgos

“Los sistemas informáticos permiten el almacenamiento, procesamiento e interacción entre servidores y usuarios, con el fin de realizar las transacciones necesarias, según sea el caso. Estas actividades pueden ser objeto de daño o manipulación por parte de agentes externos como internos, la medida de probabilidad de ocurrencia de estos eventos se le conoce como riesgo.”[21]

La administración del riesgo permite a una organización evaluar las posibles amenazas y vulnerabilidades a las que se verá enfrentados sus sistemas informáticos, y de esta manera tomar las acciones necesarias para su eliminación o mitigación.

7.2.4.1 Tipos de riesgo

“Las amenazas a los sistemas informáticos pueden tener distintas procedencias u orígenes, así mismo diferentes tipos de comportamiento, por lo cual se pueden clasificar de la siguiente manera:

- ✓ **Riesgo Tecnológico**: en el momento de una implantación o actualización tecnológica de un sistema informático, este es susceptible a amenazas

[20] Excellence, B. e. (28 de Mayo de 2018). *Blog especializado en Sistemas de Gestión*. Obtenido de https://www.pmg-ssi.com/2018/02/confidencialidad-integridad-y-disponibilidad/

[21] JARAMILLO, L. C. (s.f.). La Ingeniería Social: Un desafío Investigativo. *Universidad eafiat N 104*, 94.

latentes, toda vez que, en muchas ocasiones por desconocimiento de las nuevas normas y estándares, se puede dejar una puerta abierta a futuros ataques.

- ✓ **Riesgo Externo**: existen riesgos o posibles amenazas a los sistemas informáticos, los cuales están fuera del alcance de administración por parte de las organizaciones y pueden ser de gran impacto organizacional, como los son eventos climáticos, eventos geológicos, problemas de financiación, entre otros, a los riesgos que tienen esta característica son conocidos como riesgos externos

7.2.5 Amenaza

"Una amenaza es considerada como una entidad (persona, organización u objeto), la cual puede producir una vulneración a la seguridad informática, siempre y cuando se den determinadas condiciones que le faciliten su actuar.

7.2.5.1 Tipos de amenazas

"Las amenazas a un sistema informático pueden tener distintas naturalezas y orígenes, que van desde los factores humanos, hasta sofisticadas herramientas lógicas que permiten la intrusión maliciosa[22]", entre ellos:

- ✓ **Personas:** los factores humanos son el mayor riesgo de seguridad para un sistema informático, ya que el accionar intencional o no intencional de una persona puede provocar grandes problemas, dependiendo obviamente el nivel de autorización que tenga u obtenga, así como de su capacidad cognoscitiva referente a la informática como de las herramientas que tenga

[22] T., C. H. (s.f.). *AMENAZAS INFORMÁTICAS Y SEGURIDAD DE LA INFORMACIÓN.* Obtenido de DerecPenalyCriminXXIX.indd.

a su disposición.

- ✓ **Personal:** el activo estratégico para cualquier organización es el talento humano, sin embargo, a pesar de ser la fuerza indispensable para las actividades de esta, es la fuente recurrente de posibles amenazas, ya que por descuido del personal o por un ataque intencionado interno, se puede ver comprometida la seguridad informática, este ataque puede ser considerados de entre los más peligrosos ya que las personas pueden conocer altamente el funcionamiento lógico del sistema.
- ✓ **Ex-empleados:** este tipo de amenaza es considerada una de las más peligrosas, teniendo en cuenta que personal que tiene conocimiento del funcionamiento del sistema informático, puede haber dejado puertas traseras o simplemente algún tipo de código malicioso que se active con un trigger, por lo cual se hace necesario para la organización la generación de políticas y procedimientos que mitiguen esta amenaza, cambiando las configuraciones y accesos una vez se produzca la expulsión de alguno de los administradores del sistema.
- ✓ **Curiosos**: esta amenaza es una de las más habituales en el mundo de la informática, donde una persona con conocimientos mínimos de informática intenta la vulneración de algún sistema lógico, con normalidad se trata de robo de contraseñas personales que no comprometen en gran medida el sistema, si puede ser objeto de una vulneración a la confidencialidad de la información, por lo tanto, debe ser tratada con la máxima rigurosidad del caso.
- ✓ **Hacker:** en el ámbito de la informática, se le conoce como hacker a una persona que, a diferencia de los curiosos, posee un alto conocimiento en procedimientos y procesos informáticos, lo cual lo consolida como una amenaza potencial para cualquier sistema. A pesar de que en la actualidad se asocia con algo negativo el término, la realidad es que muchos de estos denominados hackers no realizan actos criminales, si no por el contrario, colaboran con el mejoramiento de los procesos de seguridad informática en

las organizaciones

- ✓ **Cracker**: un cracker se puede considerar como un hacker o persona especialista y con altos conocimientos en informática, que enfoca todo su esfuerzo para obtener el acceso no autorizado a los recursos informáticos con intenciones criminales.

- ✓ **Intrusos remunerados:** esta amenaza de origen en los factores humanos se puede entender como una persona que conocimientos de informática, y pagos por un tercero para violar la confidencialidad de la información almacenada en un sistema informático

7.2.6 Amenazas lógicas

"Se entiende como amenaza lógica todo tipo de secuencia de código el cual fue desarrollado con o sin intenciones maliciosas, el cual permite con su ejecución dentro del sistema la consolidación de algún riesgo.

- ✓ **Software incorrecto:** en el desarrollo de software o de sistemas informáticos de gran complejidad suelen haber errores de programación, los cuales pueden ser aprovechados o explotados por atacantes con el uso de software malicioso.
- ✓ En algunas ocasiones los usuarios pueden equivocarse con la instalación de programas de acceso libre que consigo pueden contener algún tipo de código troyano.

- ✓ **Herramientas de seguridad:** monitorear y registrar posibles fallos de seguridad informática, las herramientas de seguridad como lo son los antivirus pueden consolidarse como una amenaza, toda vez que pueden ser objeto de manipulación por un atacante, el cual por el medio de esta puede tener conocimiento de las vulnerabilidades encontradas y de esta manera lanzar su ataque informático.

- ✓ **Puertas traseras:** Cuando se desarrolla aplicaciones de gran complejidad es común que los desarrolladores generen códigos “shortcut” que permiten tener acceso rápido a ciertos recursos, los cuales pueden llegar a ser posibles puertas traseras para el ingreso malicioso al sistema.

- ✓ **Bombas lógicas:** Códigos maliciosos pueden ser programados para activarse dentro de un sistema informático mediante un trigger o simplemente con una programación especial, que cuando se den las condiciones ideales, este activara la acción de la denominada bomba lógica.

- ✓ **Canales cubiertos: P**or descuido o por programación intencional, pueden existir lazos de comunicación abiertos en los sistemas informáticos por los cuales se puede sustraer información, violando claramente la confidencialidad de este.

- ✓ **Virus**: un virus se denomina como una secuencia de condigo malicioso, el cual se hospeda dentro un de un archivo ejecutable, de tal forma que cuando este es ejecutado por el anfitrión este virus es activado e insertado en el mismo.

- ✓ **Gusanos:** a diferencia de un virus informático, un gusano es considerado como una un software malicioso capaz de ejecutarse y reproducirse a sí mismo, aprovechando las vulnerabilidades de los sistemas informáticos.
- ✓ “Un gusano que en 1988 causó pérdidas millonarias al infectar y detener más de 6.000 máquinas conectadas a la red”

- ✓ **Caballos de Troya:** se denomina bajo este nombre los códigos maliciosos que se esconden dentro de un software que funciona con el comportamiento esperado, sin embargo, mientras esto sucede el código malicioso se inserta dentro de anfitrión y vulnera la seguridad sin que el usuario detecte la

situación.

- ✓ **Programas conejo o bacterias:** este concepto se les da a los códigos maliciosos que no cumplen ningún procedimiento complejo, sino que solo se programan para copar los recursos de maquina mediante su reproducción masiva.

- ✓ **Amenazas Físicas:** Son aquellas amenazas que producen un daño o error hardware loa cual puede manifestarse y provocar daños como: robos, daños a discos duros, memorias, procesadores es decir todo daño que entorpezca la información o funcionalidad de un sistema". [23]

7.2.7 Vulnerabilidad

Una vulnerabilidad es una debilidad presente en un sistema operativo, software o sistema que al ser expuestos amenazas afectan la confidencialidad disponibilidad e integridad de la información y causan irregularidades en los sistemas, provocando perdida y robo de la información importante y sensible de una organización entidad o empresa.

Estas vulnerabilidades son producto de fallos producido por mal diseño de un software o de las limitaciones propias de la tecnología del diseño, por una codificación deficiente o insegura, por errores en la implementación o por falta de mantenimiento otro caso particular lo constituye un software utilizado masivamente, como por ejemplo las aplicaciones Web, los sistemas operativos y la ofimática, para el cual el tema de las vulnerabilidades constituye además una pérdida de confianza en productos y proveedores

[23] MONTE, d. P. (Marzo de 2010). *SEGURIDAD LÓGICA Y DE SEGURIDAD LÓGICA Y DE ACCESOS Y SU AUDITORÍA* . Obtenido de https://e- archivo.uc3m.es/bitstream/handle/10016/10653/PFC+Seguridad+Logica+y+de+Accesos+y+su+Auditoria.pdf?sequence=1

La seguridad informática busca identificar estas vulnerabilidades para darles una administración que permita sesgar el accionar a las amenazas, sin embargo, no es posible generar una protección de un 100% por la gran cantidad de variables que se ven inmersas.

En el campo de la seguridad de la información, el problema de las vulnerabilidades ha dado lugar a un nuevo escenario. Ya no resultan suficientes las soluciones simples o aisladas, sino que se hace necesario implementar "seguridad en profundidad", que proteja todos los activos de acuerdo con su criticidad, y también contemple la capacitación y la concientización a los empleados sobre las nuevas amenazas.

De todo lo anterior cabe mencionar otro importante aspecto es el de las vulnerabilidades sobre las personas, de las cuales se benefician los malhechores a través de la ingeniería social.[24]

7.2.7.1 Tipos de Vulnerabilidad

"En la actualidad hay muchos tipos de vulnerabilidades por lo tanto se debe tener en cuenta el tipo de vulnerabilidad para actuar, debido a que existen distintas soluciones para enfrentar los problemas encontrados día a día

Existen tres tipos de vulnerabilidades

- ✓ **Vulnerabilidades reconocidas por el desarrollador con generación de corrección.** Estas vulnerabilidades han sido examinadas por el proveedor del producto el cual puede generar una corrección lógica al problema

[24] ORELLA Pazmiño, J. b. (2012). "Propuesta de Best Práctica para el análisis de vulnerabilidades, métodos de protección aplicados a la infraestructura de red del laboratorio de Sistemas". Obtenido de Previa a la obtención de título de Ingenieros en electrónica, telecomunicaciones y Redes: http://dspace.espoch.edu.ec/bitstream/123456789/1943/1/98T00013.pdf

mediante el suministro de un parche.

- ✓ **Vulnerabilidades reconocidas por el desarrollador sin generación de corrección,** Estas vulnerabilidades han sido reconocidas por el proveedor del producto, sin embargo, no ha generado la corrección, por lo cual con normalidad se proporciona una alternativa de corrección temporal se suspende el uso parcial del aplicativo.
- ✓ **Vulnerabilidades no reconocidas por el desarrollador**. Este representa el peor de los casos ya que el sistema informático puede estar comprometido sin que el usuario ni el desarrollador lo conozcan.

En la actualidad el primer tipo es el más habitual puesto que los desarrolladores de la aplicación conocen sus puntos débiles donde a consecuencia se han creado soluciones inmediatas para mitigar dichas vulnerabilidades haciendo uso de parches y actualizaciones que ayudarán a mejorar esos puntos débiles que pueda tener el sistema que hemos instalado[25]".

Clasificación de vulnerabilidad según su gravedad

"Las vulnerabilidades se catalogan según la gravedad de estas teniendo en cuenta que todas no van a tener el mismo impacto negativo dentro del sistema de acuerdo con esto se existen 4 categorías racionadas a continuación.

Gravedad baja

---

[25] UNIVERSIDADVIU.COM. (28 de 04 de 2018). *Vulnerabilidad informática, tipos y debilidades principales*. Obtenido de CIENCIA Y TECNOLOGÍA: https://www.universidadviu.com/vulnerabilidad-informatica-tipos-debilidades-principales/

Esta se trata de la vulnerabilidad más débil que hay y es la que menos afecta y de menos impacto en un sistema informático o ampliación.

Gravedad media moderada

Esta Vulnerabilidad es la más sencilla de combatir y su riesgo se puede disminuir por medio de configuraciones auditorias, su potencial no alcanza a afectar una gran masa de usuarios.

Gravedad de gran importancia

Este tipo de vulnerabilidad es capaz de colocar en riesgo y atacar rápidamente un sistema informático porque su impacto es negativo y colca en riesgo la integridad, confidencialidad, confiabilidad de los datos de los usuarios y todas sus integridades.

Gravedad critica

Esta peor vulnerabilidad que existe puesto a que trae mayores consecuencias negativas para un sistema, esta debilidad propicia fácilmente que se desarrolle y a se expanda por la red, esta no espera que un usuario realice un movimiento dentro del sistema para producir el ataque

Es de vital importancia tener conocimiento de los tipos de vulnerabilidades y sus alcances a los que está expuesto para poder garantizar la seguridad en el entorno de cada organización, empresa u entidad y definir mediadas de seguridad apropiadas para su corrección o prevención[26]".

---

[26] UNIVERSIDADVIU.COM. (28 de 04 de 2018). *Vulnerabilidad informática, tipos y debilidades principales*. Obtenido de CIENCIA Y TECNOLOGÍA: https://www.universidadviu.com/vulnerabilidad-informatica-tipos-debilidades-principales/

7.2.8 Ataque

“Podemos inferir que un ataque informático consiste como un intento de violar la seguridad informática, estos ataques pueden darse de forma intencionada o no intencionada.

- ✓ **Ataque no intencionado**: se considera como un ataque no intencionado, a cualquier hecho o actividad que provoca una vulneración al sistema informático, sin que exista algún tipo de planificación, tales como eventos climatológicos, eventos geológicos, incendios, fallas en el suministro de energía, entre otros.

- ✓ **Ataque intencionado**: cuando se consolida un acceso no autorizado en el sistema, donde el intruso malicioso obtiene acceso a los recursos con fines criminales, es considerado como un ataque intencionado.

- ✓ **Criptografía** durante el desarrollo de todo tipo de conflictos a través de la historia, se ha hecho necesario ocultar las comunicaciones internas del enemigo, por lo cual el hombre desarrollo la criptografía, la cual consiste en escribir mensajes en un código oculto, de tal manera que, si esta comunicación cae en manos del enemigo, este último no estará en capacidad de reconocer la información, a menos que conozca el método para descifrarlo”.[27]

  “La criptografía consiste en tomar el documento original y aplicarle un algoritmo cuyo resultado es un nuevo documento. Ese documento está cifrado: no se puede entender nada al leerlo directamente. Podemos,

[27] MINTIC, C. . (06 de 11 de 2016). *SEGURIDAD Y PRIVACIDAD DE LA IMFORMAION* . Obtenido de Guía para la Implementación de Seguridad de la Información en una MIPYME.: https://www.mintic.gov.co/gestionti/615/articles-5482_Guia_Seguridad_informacion_Mypimes.pdf

tranquilamente, hacerlo llegar hasta el destinatario, que sabrá aplicar el algoritmo para recuperar el documento original".[28]

7.2.9 Administración del riesgo

"La administración del riesgo consiste en tomar las medidas necesarias para la minimizar la probabilidad de un ataque informático. Esta administración se logra inicialmente con la adopción de políticas y procedimientos organizacionales y hasta la adopción de herramientas sofisticadas para este efecto.

Gestión y medidas de incidentes de seguridad

Las medidas que puede adoptar cualquier organización para el manejo de incidentes de seguridad son:

- ✓ **Medidas preventivas**

  Son aquellas medidas o acciones necesarias para prevenir incidentes de seguridad las cuales pueden ocurrir tanto a nivel de hardware y software.

  Medidas de detección

  Son recomendaciones para detectar y controlar cualquier evento de inseguridad y poder tomar medidas necesarias para no dañar nuestro sistema.
- ✓ **Medidas correctivas**

  Son medias de implementación o acciones preventivas y correctivas adecuadas a cada incidente presentado utilizando canales apropiados a cada incidente para evitar que no vuelvan a ocurrir"[29].

---

[28] *Unidad.2 Criptografía* . (02 de 08 de 2016). Obtenido de http://imarbar.blogspot.com/2016/11/criptografia-1.html

[29] Baca, Urbina, Gabriel. Introducción a la seguridad informática, Grupo Editorial Patria, 2016. disponible http://ebookcentral.proquest.com/lib/unadsp/detail.action?docID=4849850

7.3 MARCO LEGAL

Las organizaciones u entidades en Colombia están obligadas a alinearse y dar estricto cumplimiento de las normas, leyes y políticas generadas por sus entes regulatorios para este efecto:

7.3.1 Ley 1273 Congreso de la Republica de Colombia

“por medio de la cual se modifica el código penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"· y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones"

7.3.1.1 Capítulo Primero

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

“Artículo 269A: acceso abusivo a un sistema informático: Se refiere al que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

Artículo 269b: **Obstaculización ilegitima de sistema informático o red de telecomunicación**: Se refiere al que, sin estar facultado para ello, impida u obstaculice el funcionamiento o el acceso normal a un sistema informático, a los datos informáticos allí contenidos, o a una red de telecomunicaciones, incurrirá en

pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con una pena mayor.

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

Artículo 269d: Daño informático: Se refiere al que, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos, o un sistema de tratamiento de información o sus partes o componentes lógicos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

Artículo 269e: Uso de software malicioso: Se refiere al que, sin estar facultado para ello, produzca, trafique, adquiera, distribuya, venda, envíe, introduzca o extraiga del territorio nacional software malicioso u otros programas de computación de efectos dañinos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

Artículo 269f: Violación de datos personales: Se refiere al que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique p emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

Artículo 269g: Suplantación de sitios web para capturar datos personales. "Se refiere al que el que con objeto ilícito y sin estar facultado para ello, diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con pena más grave.

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

La pena señalada en los dos incisos anteriores se agravará de una tercera parte a la mitad, si para consumarlo el agente ha reclutado víctimas en la cadena del delito".[30]

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

1. Sobre redes o sistemas informáticos o de comunicaciones estatales u oficiales o del sector financiero, nacionales o extranjeros.
2. Por servidor público en ejercicio de sus funciones
3. Aprovechando la confianza depositada por el poseedor de la información o por quien tuviere un vínculo contractual con este.
4. Revelando o dando a conocer el contenido de la información en perjuicio de otro.

[30] COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 1581. (12, abril, 2020). Por la cual se dictan disposiciones generales para la protección de datos personales

5. Obteniendo provecho para si o para un tercero.
6. Con fines terroristas o generando riesgo para la seguridad o defensa nacional.
7. Utilizando como instrumento a un tercero de buena fe.
8. Si quien incurre en estas conductas es el responsable de la administración, manejo o control de dicha información, además se le impondrá hasta por tres años, la pena de inhabilitación para el ejercicio de profesión relacionada con sistemas de información procesada con equipos computacionales."[31]

7.3.1.2 Capitulo Segundo

De los atentados informáticos y otras infracciones.

"Artículo 269i: Hurto por medios informáticos y semejantes: Se refiere al que, superando medidas de seguridad informáticas, realice la conducta señalada en el artículo 239 manipulando un sistema informático, una red de sistema electrónico, telemático u otro medio semejante, o suplantando a un usuario ante los sistemas de autenticación y de autorización establecidos, incurrirá en las penas señaladas en el artículo 240 de este Código. [32]

Artículo 269j: Transferencia no consentida de activos: Se refiere al que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consiga la transferencia no consentida de cualquier activo en perjuicio

[31] COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 1341. (12, Abril, 2020). "Por la cual se definen Principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones -TIC-, se crea la Agencia Nacional del Espectro y se dictan otras disposiciones".

[32]

de un tercero, siempre que la conducta no constituya delito sancionado con pena más grave, incurrirá en pena de prisión de cuarenta y ocho (48) a ciento veinte (120) meses y en multa de 200 a 1500 salarios mínimos legales mensuales vigentes. la misma sanción se le impondrá a quien fabrique, introduzca, posea o facilite programa de computador destinado a la comisión del delito descrito en el inciso anterior, o de una estafa. Si la conducta descrita en los dos incisos anteriores tuviere una cuantía superior a 200 salarios mínimos legales mensuales, la sanción allí señalada se incrementará en la mitad."[33]

[33] COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 1273. (12,abril , 2020). Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones. Diario Oficial. Bogotá, D.C.: 2009.

8 ESTUDIO SOBRE LA INGENIERÍA SOCIAL Y SU DESARROLLO EN LA ACTUALIDAD.

8.1 METODOLOGÍA Y TIPOS DE ATAQUE DE LA INGENIERÍA SOCIAL

8.1.1 Ingeniería Social Electoral: la Guerra por el Poder

> "La "ingeniería social" magistralmente trazada por los grupos de poder, consiste en el desarrollo de actos reales, concretos, para que produzcan un cambio de comportamiento en la población, en un hábito determinado, por ejemplo, y para que vayan acompañados de una clínica de masas (o manipulación psicológica) que permita y favorezca la asimilación de los cambios impuestos por el factor de poder que realiza el acto de ingeniería. Evidentemente, existen caracterizaciones que hoy vemos cómo los grupos dominantes, sin el más mínimo pudor, apelan a las más increíbles mentiras para mantener engañado al público. Y, por cierto, lo consiguen con muchísima eficiencia. Para esto influyen los medios de comunicación masiva que posibilita el internet operando (mentiras organizadas) o noticias falsas toda esta manipulación lo único a lo que conlleva es al efecto que se consigue con mensaje, esa proliferación infinita de mentiras ha logrado que los electorados terminen aprobando propuestas falsas según el interés de cada grupo de poder". [34]

8.1.2 Lenguaje corporal y la proyección de mensajes

"Un ingeniero Social experimentado sabe sacar partido del lenguaje corporal y también de la emoción de las personas objetivo, esta es la forma donde el atacante

---

34

ALAINET. (01 de 18 de 2019). *America Latina en Movimiento*. Obtenido de https://www.alainet.org/es/articulo/197642

crea conexiones entre personas de forma que exista confianza armonía suficiente con el fin de sacar información, utilizan tácticas como llegar a los sentimientos de autoestima de las personas [35]“

8.1.3 Situación hostil

“Existen personas que por lograr su objetivo no importa a recurrir llevar a hechos de escándalo como como se da a conocer con lo siguiente:

En la mayoría de los lugares las personas evitan y se retiran al encontrarse con un individuo que parece desequilibrado emocionalmente, que está colérico o es conflictivo. Tener precaución cuando una persona se pone a como si tuviese una acalorada discusión al teléfono, las personas que pasen cerca notaran su presencia y pasaran de largo, evitando tratar con ese tipo. Esta técnica se realiza simulando un enfado contra una situación o alguien al otro lado del teléfono o un canal de comunicación, pero no hacia otra persona presente.

Existen individuos que desean acceder a áreas restringidas junto con otros empleados, pero en zonas donde normalmente no le está permitido estar, podría usar esta técnica para incorporarse junto a un grupo de personas que evitarán cuestionar su presencia al notar su estado colérico, esperando que pase la tempestad

Otra situación donde algunas personas usan esa técnica de ingeniería social es en los pasos de control donde empleados de seguridad chequean bolsas de viaje, maletas y los objetos contenidos, algunos individuos simulan una discusión

---

[35] Seguridad, N. d. (2018). *DIVERSAS METODOLOGÍAS Y TIPOS DE ATAQUES DE INGENIERÍA SOCIAL*. Obtenido de https://noticiasseguridad.com/importantes/divers

y un estado colérico para evitar ser cuestionados en ese momento. Como la mayor parte de las personas no queremos relacionarnos con gente que está de mal humor y grita a los demás, podrían pasar por evitar el más mínimo trato” [36].

8.1.4 Préstamo de música para esperar durante las llamadas

“Para llevar este ataque los estafadores necesitan tres componentes: tiempo, perseverancia y paciencia. Con tal frecuencia, los ciberataques que utilizan la ingeniería social se realizan lenta y metódicamente; no solo se recopilan datos sobre las personas adecuadas, sino también sobre las llamadas "señales sociales". Esto se hace para ganar confianza y rodear el objetivo con el dedo. Por ejemplo, los intrusos pueden convencer a la persona con la que se comunican de que son colegas.

Una de las particularidades de este enfoque es la grabación de la música que la compañía o entidad utiliza durante las llamadas, en el momento en que la persona que llama está esperando una respuesta. El criminal primero espera esa música, luego la anota y luego la usa en su propio interés. Por lo tanto, cuando hay un diálogo directo con la víctima, los intrusos en algún momento dicen: "Espere un minuto, llame a la otra línea". Luego, la víctima escucha música familiar y no tiene dudas de que la persona que llama representa a cierta compañía. De hecho, este es solo un truco psicológico competente[37]”.

---

36 Gb-advisors.com. (27 de 02 de 2018). *Conoce los riesgos y amenazas de la ingeniería social sobre tus activos y datos sensibles*. Obtenido de https://www.gb-advisors.com/es/riesgos-y-amenazas-de-la-ingenieria-social/

37 Seguridad, N. d. (2018). *DIVERSAS METODOLOGÍAS Y TIPOS DE ATAQUES DE INGENIERÍA SOCIAL*. Obtenido de https://noticiasseguridad.com/importantes/divers

8.1.5 Obtener una entrevista y un trabajo

"Los hackers siempre tienen un objetivo, en el caso de las organizaciones con una gran cantidad de datos valiosos dedican una mayor inversión de tiempo y energía, incluso hasta el punto de invertir meses o años en la infiltración de una empresa es el caso de un ingeniero social con una agenda ambiciosa podría tener éxito en conseguir un puesto de trabajo, aunque la entrevista por sí solo puede proporcionar suficiente información para proceder al siguiente nivel de ataque para hackear la seguridad perimetral y seguridad lógica.

Una sorprendente cantidad de información confidencial o sensible puede ser intercambiada durante una entrevista, en particular uno con un candidato prometedor. Los ingenieros sociales son expertos en hacer las preguntas correctas tal vez acerca de la tecnología de TI en funcionamiento, y los detalles de un proceso de negocio.

Se establece un nivel de comodidad y familiaridad. El candidato puede incluso manejar la situación para conseguir que el entrevistador inicie sesión en el sistema allí mismo, obteniendo toda la información que necesitan de la entrevista a solas, y nunca tener que mostrarse para un día de "trabajo".

Sin embargo, el entrevistador no puede ser llevado tan fácilmente, en cuyo caso, si la organización de destino es lo suficientemente valiosa, el ingeniero social podría tener éxito en la infiltración de la empresa desde dentro, por conseguir un empleo y la obtención de las credenciales oficiales según experiencia de los consultores de pruebas de penetración".[38]

---

38 *Diversas Metodilogias y tipos de Ataques de Ingenieria Social*. (06 de 08 de 2016). Obtenido de https://medium.com/@Ranjeet70818032/diversas-metodolog%C3%ADas-y-tipos-de-ataques-de-ingenier%C3%ADa-social-abd2db0cb48a

8.1.6 El fraude al CEO se basa en la ingeniería social

"El término CEO corresponde a las siglas de Chief Executive Officer es el significado del administrador o máximo responsable del negocio o en una empresa quienes en la actualidad han sido victimas

Esta práctica consiste en una serie de técnicas que utilizan los cibercriminales para manipular a sus víctimas objetivo con el fin de obtener información confidencial, acceso o privilegios en sistemas de información que les permitan realizar algún acto que perjudique o exponga a las personas, organismo u entidades comprometido a riesgo o abusos.

Cómo se hace

El fraude mediante ingeniería social se basa en engañar al CEO, mediante algún medio de comunicación teléfono, correo electrónico, SMS, etc. Con el fin de que revele información sensible". Asimismo, el director del Centro de Análisis y Prospectiva de la Guardia Civil comenta que "las principales formas de ataque son los sitios webs comprometidos, la simulación de correos electrónicos, la información obtenida por teléfono con técnicas de elicitación, el phishing o el hacking".

El arranque suele ser muy similar a los conocidos ataques de phishing, pero realizados de una forma mucho más profesional. "El ataque comienza con el envío de un correo electrónico de phishing, muy elaborado, que parece llegar del directivo de la empresa y en el que se solicita a un empleado realizar una transferencia o movimiento bancario a una cuenta controlada por los ciberdelincuentes", indica el director general de Kaspersky Lab Iberia. También

podría tratarse de una “simulación de correo electrónico de un proveedor, mediante el que los criminales pueden modificar datos de facturación para desviar pagos a sus propias cuentas”, comenta Blanco. Y Ramírez recuerda que “las víctimas también pueden ser empresas que creen recibir un correo electrónico de su cliente. De esta forma, tanto los empleados de la compañía en la que la identidad del CEO ha sido suplantada como la compañía cliente que realiza la transacción son víctimas de este nuevo fraude”,

El responsable del INCIBE señala que “este tipo de engaños se conoce como whaling ‘pesca de ballenas’-, por tratarse de phishing dirigido a ‘peces gordos’”. Además, insiste en un detalle importante. “Si el empleado abre el correo a través de un dispositivo móvil, no podrá comprobar a simple vista que la dirección del correo de origen no es correcta, salvo que haga clic sobre el nombre del remitente. Esto hace que sea más difícil de detectar. Si no se da cuenta del engaño, podría desvelar datos confidenciales”.

Estos delincuentes aprovechan ocasiones en las que el jefe está ausente o no está accesible lograr perpetrar este tipo de suplantaciones, con el fin de que la víctima no tenga la oportunidad de verificar su autenticidad. Además, comenta que “en casos más sofisticados, pueden haber espiado previamente los correos electrónicos mediante un programa maligno para imitar el estilo de escritura del jefe. También pueden robar previamente las credenciales de acceso del jefe a su cuenta de correo para enviar el email desde esta misma cuenta”.

Quiénes son las víctimas

Sus principales víctimas son organizaciones entidades donde se proponen disponer de la información sensible y utilizan a su personal ya sea proveedores, clientes o empleados para lograr cometer el fraude los cuales son considerados como el eslabón más débil y pueden ser engañados fácilmente y ser víctima de las diferentes técnicas para lograr su objetivo propuesto.

Riesgos corre una empresa

Las víctimas de un ataque de fraude al CEO se exponen a "pérdida de información clave, afectación a patentes o posibles licitaciones, fraude económico, por ejemplo, desvío de pagos, afectación a la marca y reputación de la empresa o procesos de extorsión en base a la información robada, tanto personal a empleados como institucional", dependiendo de la información roba será utilizada para venderla en el mercado negro con diferentes objetivos afectando así la buena reputación de la empresa u organización" [39]

8.1.7 Spam

"Este el término utilizado para referirse a los correos electrónicos no solicitados, que se envían normalmente a un gran número de personas, algunos puntos son similares a otras formas de publicidad, tales como la tarjeta colocada en el buzón, el folleto recibido en la esquina y la llamada telefónica que ofrece productos. Sin embargo, lo que difiere es precisamente lo que lo hace tan atractivo y motivador para cualquier persona que envía (spammer): mientras que en la otra las formas remitentes tienen que hacer algún tipo de inversión, el spammer necesita para invertir muy poco, o incluso nada para alcanzar los mismos objetivos y en una escala mucho mayor.

Esta práctica se ha convertido, tras el desarrollo de Internet y las nuevas aplicaciones y tecnologías. Actualmente, el envío de correo no deseado es una

---

[39] RAMOS, D. (18 de 07 de 2017). *Fraude al CEO: ingeniería social al servicio del cibercrimen*. Obtenido de https://www.silicon.es/a-fondo-fraude-ceo-ingenieria-social-cibercrimen-2346572

práctica que es motivo de preocupación, tanto por el aumento desenfrenado en el volumen de mensajes en la red, tales como la naturaleza y los objetivos de estos mensajes.

Correo no deseado están directamente vinculados a los ataques a la seguridad de Internet y el usuario, siendo en gran parte responsable de la propagación de código malicioso, estafas difusión y venta ilegal de productos.

Algunas de las formas en las que puede verse afectada por los problemas causados por el spam son:

- ✓ **La pérdida de mensajes importantes:** Debido al volumen de correo no deseado recibido, se corre el riesgo de no leer los mensajes importantes, que lean tarde o eliminarlos por error.

- ✓ **Inapropiado u ofensivo:** cuánto del correo no deseado son enviados a los conjuntos aleatorios de direcciones de correo electrónico, es probable que reciba mensajes que contienen contenido considerado inapropiado u ofensivo.

Pérdida innecesaria de tiempo: para cada correo no deseado recibido, es necesario tomar el tiempo para leerlo, identificarlo y eliminarlo de su buzón de correo, lo que puede resultar en pérdida de tiempo innecesaria y pérdida de productividad.

- ✓ **No recibir mensajes de correo electrónico:** si el número de correo no deseado recibido es grande y se utiliza un servicio de correo electrónico que limitan el tamaño del buzón, se corre el riesgo de desplazar su área de correo electrónico y hasta que pueda liberar espacio, quedará impedido de recibir nuevos mensajes.

- ✓ **Mensajes de clasificación errónea:** si se utiliza con sistemas de filtrado de reglas antispam ineficiente, se corre el riesgo de que los mensajes legítimos clasificados como correo no deseado y que, según su configuración, se pueden eliminar, se trasladaron a cuarentena o redirigida a otras carpetas y -mail

Algunos de los problemas relacionados con el correo no deseado que los proveedores y las empresas se enfrentan a menudo son:

- ✓ **Impacto en la banda**: el volumen de tráfico generado por el spam hace que sea necesaria para aumentar la capacidad de los enlaces de conexión a Internet.

- ✓ **El mal uso de los servidores:** la mayor parte de los recursos de los servidores de correo electrónico, tales como el tiempo de procesamiento y espacio en disco que se consumen en el tratamiento de los mensajes no solicitados.

- ✓ **La inclusión en las listas de bloqueo**: un proveedor que tiene miembros que participan en casos de envío de correo no deseado puede tener la red incluida en las listas de bloqueo, lo que podría afectar el envío de correos electrónicos por los otros usuarios y dar lugar a la pérdida de clientes.

- ✓ **Recursos de inversión adicionales**: los problemas causados por el spam causan la necesidad de aumentar las inversiones para la adquisición de equipos y sistemas de filtración y la contratación de más técnicos de su funcionamiento.

Técnicas los spammers para recopilar direcciones de correo electrónico desde la compra de bases de datos para producir sus propias listas, generado a partir de:

- ✓ **Los ataques de diccionario**: consisten en forma de direcciones de correo electrónico de las listas de nombres de personas, palabras que se encuentran en los diccionarios y / o combinación de caracteres alfanuméricos.

- ✓ **El código malicioso:** muchos códigos maliciosos están diseñados para examinar el equipo infectado en busca de direcciones de correo electrónico que se pasan posteriormente a los spammers.

- ✓ **Cosecha**: es recoger direcciones de correo electrónico a través de exploraciones en las páginas Web de las listas de correo y de archivos, entre otros.

Después de efectuar la recolección, los spammers tratan de confirmar la existencia de las direcciones de correo electrónico y, por ello, a menudo utilizando el engaño, tales como:

- ✓ Enviar mensajes a las direcciones recogidos y en base a las respuestas recibidas desde el servidor de correo electrónico.

- ✓ Identificar qué direcciones son válidos y cuáles no lo son

- ✓ Incluir en el correo no deseado de un supuesto mecanismo para eliminar la lista de correos electrónicos, tales como un enlace o una dirección de correo electrónico (cuando el usuario solicita la eliminación de hecho se

confirma al spammer que esta misma dirección de correo electrónico es válida y realmente utilizada)

- ✓ Incluir en el correo no deseado de una imagen del tipo Web bug, diseñado para controlar el acceso a una página web o correo electrónico (cuando el usuario abre el correo no deseado, la Web bug se accede y el spammer recibe la confirmación de que esa dirección de correo electrónico es válida)".[40]

8.1.8 Carbanak.

Es un tipo de campaña APT conocida por sus siglas en inglés como amenaza persistente avanzada) a cargo de un grupo de delincuentes cibernéticos. Este ataque programa maligno, conocido por su éxito mundialmente.

Investigadores de seguridad han descubierto el código fuente completo del programa maligno Carbanak, la campaña APT (amenaza persistente avanzada) más exitosa del mundo a cargo de un grupo de ciberdelincuentes se han ocupado de estafar en gran cantidad a instituciones financieras, hospitales, restaurantes.

Esta organización de ciberdelincuentes comenzó sus actividades lanzando una serie de ataques programa maligno para embestir bancos y redes de cajeros automáticos de todo el mundo con el único objetivo de robar grandes cantidades de dinero.

Los atacantes utilizan técnicas extraídas del arsenal de ataques dirigidos: Esto quiere decir que los usuarios maliciosos roban dinero directamente de los bancos a través de correos electrónicos maliciosos de phishing enviados a empleados en diferentes espacios, esta organización de ciberdelincuentes ha

[40] Costas, Santos, Jesús. Seguridad informática, RA-MA Editorial, 2014., disponible en http://ebookcentral.proquest.com/lib/unadsp/detail.action?docID=3228430

tenido la posibilidad de comprometer e infectar computadoras con programa maligno Carbanak en bancos alrededor del mundo. Al abrir esos correos, se les permitía a los estafadores transferir dinero de los bancos afectados a cuentas falsas o cajeros automáticos monitoreados por ellos. y evitan dirigir sus ataques a usuarios finales.

Estos ciberdelincuentes utilizas las siguientes estrategias para llegar al objetivo:

- ✓ Buscan vulnerabilidades críticas de la víctima.
- ✓ Se infiltran en la red buscando sistemas rotos.
- ✓ Aprovechan para extraer todo el dinero posible.

8.1.9 El baiting

"Es como un **caballo de Troya** de verdad, que usa un medio físico, y se basa en la curiosidad o avaricia de la víctima. Es similar, de varias maneras, a los ataques de phishing. Sin embargo, lo que les distingue de otros tipos de ingeniería social es la promesa de un artículo u objeto que los piratas informáticos usan para atraer a sus víctimas; estos atacantes pueden usar música o descargas gratis de películas, si ofrecen sus credenciales a una determinada página, también ataques no ocurren exclusivamente en internet. Los atacantes también pueden enfocarse en explotar la curiosidad humana mediante medios físicos.

¿Cómo se hace el baiting?

Para saber cómo funciona se coloca como ejemplo; un escenario industrial: con el objetivo último de infiltrar la red de una empresa, el ingeniero social puede distribuir memorias flash infectadas con programa maligno o dispositivos similares a sus empleados, con la esperanza de que este hardware se inserte en ordenadores conectados a redes como medio para diseminar el código malintencionado. Las memorias flash infectadas pueden ser presentadas a los

empleados como regalos promocionales, o como recompensa por participar en una encuesta. Tal vez los dispositivos, en apariencia inofensivos, estén en una cesta de obsequios ubicada en la recepción de la empresa, para que los trabajadores tomen uno al regresar a sus lugares de trabajo. Otra posibilidad sería la colocación estratégica de dispositivos corrompidos para ser tomados por empleados específicos. Si estos dispositivos tienen marcas que digan «Confidencial» o «Información Salarial», los dispositivos podrían resultar demasiado tentadores para algunos trabajadores. Estos empleados podrían simplemente morder el cebo e insertar el dispositivo infectado dentro de los ordenadores de la empresa, ¡y listo!

¿Cómo proteger su sistema contra el Baiting?

La mejor defensa contra el baiting y cualquier otro esquema de ingeniería social es formar a su equipo y a usted mismo. Cada uno de nosotros debe procurarse una robusta cultura de seguridad en nuestros alrededores: el hogar, la oficina, donde cada individuo debe considerar la «seguridad de la empresa» como parte integral de sus responsabilidades individuales. Específicamente en el caso del baiting, cada individuo debe discutir el tema abiertamente con sus familiares, colegas y amigos, y hacerlos conscientes acerca de los peligros que puede entrañar la falta de precaución.

El formarse a sí mismo y a los demás es, de lejos, la defensa más efectiva de la que dispone contra la «Ingeniería Social»”[41].

8.1.10 Ciberacoso

“El ciberacoso es un delito informático muy habitual en los últimos tiempos cometidos a una persona o grupo de personas donde más habitualmente son cometido a menores de edad utilizando como medio las tecnologías de información

[41] Baca, Urbina, Gabriel. Introducción a la seguridad informática, Grupo Editorial Patria, 2016. disponible en http://ebookcentral.proquest.com/lib/unadsp/detail.action?docID=4849850

y la comunicación donde realizan acciones hostiles, repetitivas, deliberadas como la difusión de falsos rumores, fotografías humillantes, creación de perfiles falsos que insultan a la víctima su único fin de herir a otras personas provocándole sentimiento susto, vergüenza, ira, humillación, depresión impotencia llevando al victimario a drásticos casos extremos[42]".

8.1.11 El phishing busca empleo

"Es una popular forma donde los delincuentes informáticos intentan engañar a los a personas aprovechando los lugares físicos e informáticos donde frecuentan las personas. Las ofertas de trabajo falsas las realizan de manera llamativa con grandes expectativas; de esta forma manipula a la víctima y obtener información confidencial, donde el interesado publica o entrega su hoja de vida con sus datos personales proporcionando a los cibercriminales datos confidenciales.

Estos ciberdelincuentes aprovechas cualquier tema que este en la actualidad para atraer la atención de la mayoría de las personas sabiendo que la búsqueda de empleo es una necesidad que urge e interesa a mucha gente haciendo que se crea en este tipo de engaño.

Recomendaciones

---

42 ENTICCONFIO.gov.co. (20 de 09 de 2019). *Ciberacoso, un riesgo al que todos estamos expuestos*. Obtenido de https://www.enticconfio.gov.co/Ciberacoso_un_riesgo_al_que_todos_estamos_expuestos

- ✓ Antes de entregar o publicar su hoja de vida en un sitio donde ofertan empleos, revisar políticas de privacidad.

- ✓ Si la oferta de trabajo la realizan por vía telefónica se recomienda hacer uso de motores de búsqueda para mirar su autenticidad.

- ✓ Tener cuidado con ofertas laborales que haya errores ortográficos y correos donde no se evidencie el nombre se la empresa, es decir datos incompletos.

- ✓ En la documentación de soporte en una nueva oferta de trabajo, se recomienda no colocar sus datos personales como fecha de nacimiento, numero de cedula, numero de cuentas de banco, direcciones.

Es de gran importancia que las organizaciones o entidades estén alertas con estas temáticas; ya siendo conocedores de los de algunas **metodologías y tipos de ataque de la ingeniería social** se puede implementar medidas y controles necesarios para evitar ser víctimas de los diferentes ataques a través de sus diferentes técnicas accediendo y obteniendo información que cause daños irreversibles Teniendo en cuenta que la ingeniería social aprovecha el espacio humano falencias encontradas en la seguridad de la información para aprovecharse en de cualquier sistema informático

En el caso de la Secretaria de Educación Departamental de Nariño no cuenta con profesionales altamente calificados y capacitos en Seguridad de la Información que conformen un equipo técnico para proteger a los sistemas de los ataques a los usuarios finales, los cuales no tienen mayores conocimientos sobre los riesgos por esta razón se realiza algunas recomendaciones del manejo y uso apropiado de información y plasmar algunas políticas recomendadas donde se requiere que se cumplan y también aprovechar todo lo referente al uso seguro del Internet e investigar cada una de estas recomendaciones relacionadas a continuación:

- ✓ Utilizar los navegadores Web
- ✓ Utilizar los programas lectores de e-mails
- ✓ Acceder Webmail
- ✓ Realizar transacciones bancarias y acceder a sitios de Internet Banking
- ✓ Realizar transacciones comerciales y de acceso sitios de comercio electrónico
- ✓ Tipos de conexión o que conexión se debe utilizar

Teniendo en cuenta la gran importancia del tema, debemos concienciarnos e instruirnos cada día en las metodología y técnicas de Ingeniería Social y así poder identificar o detectar los diferentes ataques y así poder actuar de manera más segura y dentro de esta Entidad y en nuestra vida cotidiana[43].

43 Seguridad, N. d. (2018). *DIVERSAS METODOLOGÍAS Y TIPOS DE ATAQUES DE INGENIERÍA SOCIAL*. Obtenido de https://noticiasseguridad.com/importantes/divers

9 ESTRATEGIAS DE ESTUDIO DESARROLLADAS EN LAS INSTITUCIONES RELACIONADAS CON CAPACITACIÓN EN SEGURIDAD INFORMÁTICA E INGENIERÍA SOCIAL.

9.1 ESTRATEGIAS DE ESTUDIO EN SEGURIDAD E INGENIERÍA SOCIAL

9.1.1 Serie 800 del NIST

“Es un programa de capacitación y concientización sobre la seguridad de la tecnología de la información es un conjunto de recomendaciones del Instituto Nacional de Normas y Tecnología sobre cómo configurar el programa de concientización y capacitación sobre seguridad.

Consta de cuatro pasos críticos en el ciclo de vida de un programa de concientización y capacitación en seguridad de TI:

Este documento proporciona pautas para crear y mantener un programa integral de concientización y capacitación, como parte del programa de seguridad de TI de una organización. La guía se presenta en un enfoque de ciclo de vida, que abarca desde:

1. Diseño del programa de concientización y capacitación
2. Desarrollo de material de sensibilización y capacitación
3. . Implementación del programa
4. Post-implementación

Dicho documento establece de manera clara la diferencia entre los tres componentes principales de un programa para desarrollar la cultura en seguridad de la información: concientización, entrenamiento y educación:

- ✓ **Concientización**: Su propósito es enfocar la atención en seguridad de la información para posibilitar que el público objetivo reconozca los temas de interés, estableciendo al inicio qué comportamientos se quieren reforzar, por ejemplo, mantener el escritorio limpio, usar de forma adecuada las contraseñas, elaborar copias de respaldo, usar el correo responsablemente, etcétera.

- ✓ **Entrenamiento**: Se centra en producir habilidades y competencias en seguridad de la información relevantes y requeridas con el fin de que el público objetivo las aprenda y aplique en el día a día.

- ✓ **Educación**: Integra habilidades de seguridad y competencias de las diferentes especialidades funcionales dentro de un cuerpo común de conocimientos, enfocándose en producir especialistas en seguridad. Por ejemplo, capacitación en sistemas de gestión de seguridad de la información o en auditoría interna ISO27001

Incluye orientación sobre cómo los profesionales de seguridad de TI pueden identificar las necesidades de concientización y capacitación, desarrollar un plan de capacitación y obtener la participación de la organización para financiar la concientización y los esfuerzos de los programas de capacitación. Este documento también describe cómo: Seleccionar temas de concientización y capacitación; Encuentra fuentes de conocimiento y material de capacitación; Implementar material de sensibilización y capacitación, utilizando una variedad de métodos; Evaluar la efectividad del programa; y Actualizar y mejorar el enfoque a medida que

cambian las prioridades de la tecnología y la organización. El documento es una publicación complementaria de la Publicación especial 800-16 de NIST, Requisitos de capacitación en seguridad de la tecnología de la información: un modelo basado en roles y desempeño. Las dos publicaciones son complementarias: SP 800-50 funciona a un nivel estratégico más alto, analiza cómo desarrollar un programa de capacitación y concienciación sobre seguridad de TI, mientras que SP 800-16 se encuentra en un nivel táctico más bajo, describiendo un enfoque de la seguridad de TI basada en roles capacitación Descargo de responsabilidad Esta copia no está publicada por el Instituto Nacional de Estándares y Tecnología (NIST), el gobierno de los EE. UU. o el Departamento de Comercio de los EE. UU. La publicación de este documento no debe implicar de ninguna manera ninguna relación o afiliación con las organizaciones y el Gobierno mencionados anteriormente"[44].

9.1.2 Centauri Technologies Corporation

"Es una firma de consultoría en Tecnología de Información con la visión de introducir tecnología avanzada pero apropiada para clientes de valor estratégico en la sociedad de la información que tengan alto potencial de impacto y crecimiento en el mercado y la sociedad.

Combina realidad gerencial y operacional diaria corporativa con su dominio tecnológico para dotar sus clientes de soluciones con resultados medibles en los objetivos de negocio de la organización.

Las soluciones y servicios desarrollados van a la medida, analizando y asesorando, ayudando a proteger información y desarrollando tecnología a la medida para nuestros clientes.

[44] Presidencia, M. d. (2017). Guía de Seguridad de las TIC CCN-STIC 804. Centro Criptológico Nacional, 100.

Centauri Technologies Corporation es una empresa constituida en su versión corporativa actual desde 2001 y es la continuación corporativa de Centauri, que opera internacionalmente desde 1996.

Ofrece.

Capacitación del personal

Requerimientos:

Conocimientos básicos de sistemas y/o auditoría de sistemas.

Entregables:

- ✓ Taller en los puestos de trabajo o en un lugar designado.
- ✓ Si se incluye en el alcance, manual de prácticas, material en CD y herramientas utilizadas.
- ✓ Las personas son la medida de la seguridad de un sistema.
- ✓ Propondremos capacitación a la medida de la situación y objetivos de su personal.
- ✓ Podemos capacitar a personal inicial, a auditores, a especialistas o a gerentes de alto nivel.
- ✓ Diseñaremos pruebas de asimilación de material.

Metodología:

- ✓ Comprender los objetivos tecnológicos y las responsabilidades del personal por capacitar.

- ✓ Proponer y lograr aprobación del material por dominar y las pruebas con las que se demuestra la asimilación.

- ✓ Impartir capacitación en las facilidades pactadas.

- ✓ Evaluar impacto del entrenamiento mediante encuestas, exámenes o pruebas.

Credenciales:

- ✓ Por más de 5 años (2001-2005) Centauri ofreció anualmente uno de los talleres más profundos y aceptados del mercado local de seguridad informática.

- ✓ Nuestro personal combina experiencia en proyectos reales con clientes de gran envergadura, formación académica de alto nivel y certificaciones específicas para la industria de seguridad[45]".

9.1.3 Oydia Satrategic Security

"Es una organización que se encuentra conformada por un grupo de profesionales e investigadores altamente especializados en Seguridad Informática e Infraestructura, dedicados a proveer soluciones para los problemas que afectan la imagen y objetivos de las Organizaciones cuando dicha seguridad se encuentra comprometida.

OYDIA provee asimismo consultoría y servicios en general, para la implementación de mecanismos de detección temprana, prevención y ***capacitación.***

45

Centauri, T. C. (2011). Obtenido de http://centauritech.com/quienes-somos

Los Profesionales que integran OYDIA, vienen desempeñándose en este terreno desde hace más de 15 años, operando siempre sobre entornos reales, y en constante capacitación.

Los servicios incluyen Consultoría, Pruebas y Tests de Seguridad, Auditoria, Normalización, Certificación, Análisis e Implementación, Desarrollo y Asesoría General entre otros. OYDIA brinda soluciones que permiten mantener la confidencialidad, integridad y disponibilidad de la información, disminuyendo en un alto porcentaje el grado de riesgo y exposición de los Sistemas Informáticos de las organizaciones.

Debido a la amplia diversidad de escenarios sobre los cuales OYDIA desarrolla sus servicios, se han elaborado diversas metodologías de trabajo con el objetivo de optimizar tiempos y recursos invertidos. Todas incluyen como denominador común, un intenso trabajo de análisis e investigación y un completo esquema de soporte y asistencia durante todo el periodo de desarrollo del proyecto.

Una vez encontradas las acciones correctivas y el Plan de Trabajo se inicia, es necesario producir un control efectivo sobre las nuevas implementaciones como así también sobre las consecuencias de las acciones correctivas.

Capacitación

Alineados con el concepto de que la mejor defensa es el conocimiento, OYDIA brinda cursos de capacitación en diversos niveles, con el objeto de preparar, inducir y capacitar al personal de las organizaciones y entidades en todos los temas que se relacionan con la Seguridad Informática.

Enfoque educativo

El objetivo pedagógico, es formar a las personas para la "sociedad del conocimiento" aplicado a sus tareas cotidianas, como así también despertar su interés, incentivarlo a continuar su capacitación por sus propios medios, a través de la lectura científica, conocimientos, capacidades y habilidades para convertirse en un "Analista Simbólico", capaz de identificar y resolver problemas. **de Seguridad Informática**, desde el punto de vista GLOBAL, y conjugando la necesaria participación de recursos tanto físicos como humanos, partiendo de al menos dos enfoques, a saber, al torno al tema que actúa cada organización".[46]

9.1.4 Tecnoxxi, Tu seguridad, nuestro compromiso

"Esta estrategia esta enfocada a cada necesidad y seguridad de sus clientes, entrega los mejores servicios como arquitecturas alineadas a cada objetivo solicitado y ofrece sus servicios de acuerdo con el presupuesto y prioridad y cada comprador y de tal forma asegurando su cliente para largo plazo

son un equipo de consultores que desarrolla estrategias de seguridad de la información, para generar ventajas competitivas a nuestros clientes, alineadas a sus objetivos del negocio, a través de una arquitectura de seguridad integral.

Maneja una buena experiencia con mas de 19 años de servicio
Cuenta con los más importate especialización en seguridad de la Información

- ✓ Tenemos más de **19 años de experiencia.**
- ✓ Contamos con especialización en **seguridad de la información.**
- ✓ Es socio con los principales les se seguridad de a TI y sus certificaciones y normativas mas altas

---

[46] OYDIA, S. S. (2020). *Copyright © OYDIA*. Obtenido de https://oydia.com/

- ✓ Brinda un servicio post ventas haciendo su soporte con las nuevas prácticas y también las herramientas ITIL, COBIT y toda la familia ISO.
- ✓ El servicio se presta a diferentes sectores tanto probado, públicos y gubernamentales.

Misión

A través de consultoría y servicios **generar e implementar arquitecturas de seguridad de la información adecuadas** las necesidades de nuestros clientes.

Visión

Brindar servicios confiables de consultoría a través de estrategias integrales de seguridad de la información que **garantice la continuidad y operación de su negocio.**

Como su filosofía es el conocimiento y entendimiento de su entorno, lleva a una transformación constante que **trae lo mejor para el beneficio y seguridad de nuestros clientes.**

Capacitación en Seguridad de la Información

Esta capacitación es de vital importancia ya que la información es el más grande valor que tienen las organizaciones u entidades a tal razón que en ellas no existe capacitación ni concientización respecto a este valioso tema por lo tanto es un peligro latente de sufrir pérdidas información y así afrontar difíciles consecuencias.

Se necesita una capacitación para que el personal este consciente de los riesgos de lo que expuesto y cómo manejarlos, favoreciendo así ser víctima de robo o perdida e información y deliberando ser víctima a causada de desconocimiento ante este importante tema.

¿Cómo realizar una capacitación en seguridad de la información?

Para esta capacitación es necesario cumplir ciertos parámetros

- ✓ Tener incidencias iniciales como mal manejo de información o es decir de mala prácticas de seguridad para luego de ser capacitados hacer comparaciones.
- ✓ Comenzar con **temas de alto impacto** para a empresa u entidad.
- ✓ Introducir temas o conceptos nuevos en la capacitación porque la mayoría del personal no es experto en TI.
- ✓ La capacitación debe ser teórico practica para poder aplicar los conocimientos adquiridos y lograr cumplir el objetivo "[47]

9.1.5 Seguridad y privación de la Información

Este programa tiene como objetivo principal establecer lineamientos lograr construir y mantener un plan de capacitación sensibilización y comunicación de Seguridad Informática, seguridad de la Información logrando así asegurar cubra en su totalidad los funcionarios de la Entidad y que cada uno cumpla con sus roles y responsabilidades de seguridad y privacidad de la información dentro de cada entidad.

Se requiere cumplimiento de todos los que tienen acceso al sistema a razón de esto cualquier incumplimiento de las políticas debe llevar imposición de una sanción siempre y cuando el personal haya sido debidamente capacitado o informado.

Sensibilización

---

47 Tecno XXI, T., (08 de 05 de 2017). *Capacitación en Seguridad de la Información*. Obtenido de https://www.tecnoxxi.com/blog/negocios/capacitacion-en-seguridad-de-la-informacion/

Su principal objetivo es impactar sobre el comportamiento de un individuo o grupo de personas o reforzar buenas prácticas sobre algún tema en particular buscando estrategias con practicidad y simplicidad y el aprendiz pueda captar la información.

Educación formal

Se define como todos los niveles y habilidades de seguridad envueltos en un único cuerpo de conocimiento. EJEMPLO: Programa de estudios de educación superior, postgrados.

Desarrollo profesional (educación no formal)

Busca asegurar que los usuarios desde el más principiante hasta el más experimentado tengan los conocimientos suficientes para desempeñar sus roles. Esto se logra a través de certificaciones, que ofrecen proveedores de plataformas específicas, sistemas operativos o algunas otras relacionadas con conceptos de seguridad informática Esta parte de desarrollo profesional depende de cada institución si requiere de certificaciones para desempeñar bien sus roles o si son motivo para brindar algún tipo de bonificación adicional al empleado por su preparación.

9.1.6 Seguridad y Tecnología. _Siete 24

“Para una organización es muy importante estar protegido ante cualquier riesgo, teniendo en cuenta que la información es de los activos más importantes. Contar con la seguridad adecuada puede convertirse en la herramienta ideal para combatir a los delincuentes.

Existen diferentes herramientas que puede poner en práctica para tener un mayor control frente a la seguridad de datos, como los que presentamos a continuación:

- ✓ **SIG7**: un sistema integral que cuenta con el apoyo de distintas herramientas, como dispositivos Android, una central de procesos, coordinadores de zona,

guardas de seguridad y un área de soporte y sistemas que le permiten controlar y monitorear constantemente cualquier movimiento dentro de una compañía.

- ✓ **Sistemas de geolocalización:** estos le permiten realizar un rastreo exacto de la ubicación tanto de personal, como de activos importantes para su empresa. Funcionan por medio de equipos satelitales y se pueden integrar a otros sistemas.

- ✓ **Apoyo a guardas:** el capital humano también es importante, por eso los guardas deben contar con cámaras de seguridad, alarmas y un control de accesos que le permita reaccionar de forma inmediata y eficaz para resguardar a la compañía de cualquier peligro.

Es esencial, que todo el personal que tenga acceso a equipos tecnológicos reciba capacitación adecuada en la prevención de riesgos, y más aún cuando se trata de ingeniería social, para fortalecer todos los procesos que afecten los activos. Recuerde, ante cualquier eventualidad o movimiento extraño tomar las medidas correspondientes.

Es importante estar siempre pendiente de los enlaces que se reciben a través de los correos electrónicos, evite descargar aplicaciones de páginas web sospechosas o conectar memorias USB desconocidas en sus equipos, estas son acciones preventivas bastante significativas para la seguridad de las organizaciones.

No olvide contar con un buen antivirus, la seguridad y confidencialidad de la información de los clientes es una característica de competitividad y calidad que puede potenciar cualquier organización. Una empresa de seguridad que integre

todas las herramientas tecnológicas y de infraestructura puede convertirse en un gran aliado”.[48]

9.1.7 En TIC confío

“Es una gran estrategia su principal objetivo es de promover el uso apropiado y acciones de seguridad con respecto a la TIC, busca ayudar a la sociedad a la sociedad a desenvolverse e interactuar responsablemente con las tecnologías de la información y las comunicaciones permitiendo así compartir, trasmitir y enviar diferente información.

Este enfoque debe de ser primordialmente dirigido a quienes son más susceptibles de correr riesgos en las redes: los niños y jóvenes que utilizan diariamente estas.

herramientas para enfrentar con seguridad riesgos asociados al uso de las TIC, como el grooming, el sexting, el ciberacoso, la ciber dependencia y el material de abuso sexual infantil y también herramientas para sus actividades de entretenimiento y también educativas

Después de analizar las estrategias de estudio desarrollados en las instituciones relacionadas con **capacitación en seguridad e ingeniería social** es de vital importancia resaltar que la capacitación y formación en una organización o entidad es necesaria porque es habilitar a una persona de que tenga el conocimiento la habilidad de detectar mejor las amenazas, los diferentes tipos de ataques y saber cómo manejarlos, es decir educar en seguridad informática e la ingeniería social.

Debemos concienciarnos que en seguridad el eslabón más débil son las personas para esta técnica de ataque es una vulnerabilidad universal e independiente de la plataforma tecnológica que nada servirá la inversión en tecnología para la seguridad de la organización si es tan vulnerable a la manipulación

[48] SIETE24seguridad y tecnología. SEGURIDAD EN INGENIERÍA SOCIAL [en línea], 25 de abril 2003 [revisado 15 de mayo de 2019]. Disponible en internet: https://blog.siete24.com/ingenieria-social-importancia-contar-personal-seguridad-capacitado

Con este contexto es fundamental que tanto personas como organizaciones se eduquen frente a este tema y se tome conciencia del valor de los activos que se deben resguardar y de la misma manera les permitiría comprender en qué posición se encuentra la organización.

Teniendo en cuenta estas estrategias de estudio se busca que la Secretaria de Educación del Departamento de Nariño, se concientice en capacitar en Seguridad Informática e Ingeniería Social a todos los funcionarios de cada dependencia que la conforman, para poder mantener una actitud de precaución y alerta en el uso diario de los sistemas de información, para su mejora en todos los procesos y desarrollo que mantiene.

Es importante que la secretaria tenga claro que la capacitación no es un gasto si no que, por lo contrario, es una inversión que es más costoso contratar a unas personas capacitadas y con los conocimientos que requiere, a capacitar a los empleados ya pertenecientes a esta entidad".[49]

[49] TIC, M. (s.f.). *En TIC Confio*. Obtenido de https://www.enticconfio.gov.co/ tutoriales, E. (06 de 06 de 2018).

10 ANÁLISIS DE LA SITUACIÓN ACTUAL DE LA SECRETARIA DE EDUCACIÓN DEPARTAMENTAL DE NARIÑO CON RELACIÓN A SU CONOCIMIENTO DE SEGURIDAD INFORMÁTICA

Para la recolección de la información y posterior análisis, se procedió a la aplicación de una encuesta la cual se aplicó satisfactoriamente a 24 funcionarios de la Secretaria de Educación departamental de Nariño con el objetivo de analizar el nivel de conocimiento en Seguridad Informática, con los resultados nos va dar lineamientos necesarios para conocer las fortalezas y debilidades existentes, para de esta forma saber que observaciones, sugerencias y recomendaciones se necesita de acuerdo a los datos encontrados.

Como resultado de la aplicación, se obtuvo las siguientes respuestas.

10.1 CONOCIMIENTO GENERAL DE SEGURIDAD:

Las preguntas que a continuación se relacionan sobre los conocimientos en seguridad se pretende que proporcione la información requerida sobre importante tema e identificar fortalezas o debilidades sobre el conocimiento, políticas de seguridad y en prácticas de seguridad y causas de la inseguridad informática en la Secretaria de Educación Departamental de Nariño para tomar medidas necesarias de acuerdo con el resultado

A la pregunta **N.º 1 ¿Sabe usted que es Seguridad Informática?** Los encuestados respondieron así:

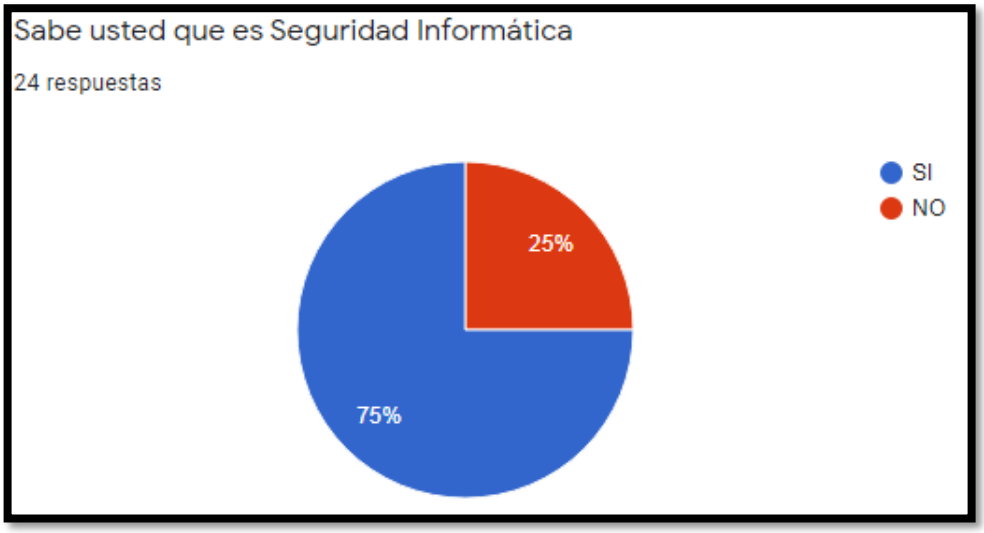
Tabla 1 pregunta 1 en cantidades y porcentaje

¿Sabe usted que es Seguridad Informática?		
Opciones	**Cantidad**	**Porcentaje**
Si	18	75%
No	6	25%
Total	24	100

Fuente: Autor

Grafica reflejo de resultados

Grafica 2 pregunta 1 general porcentajes



Fuente: Autor

Como resultado de las 24 personas encuestadas 18 de ellas dicen que tienen conocimiento en Seguridad Informática para un porcentaje de 75% de los encuestados y 6 de ellas no conocen del tema, para un porcentaje 25% de los encuestados.

Como conclusión demuestra que hay un alto porcentaje donde los funcionarios de la Secretaria de Educación Departamental de Nariño que dicen creer tener conocimiento del término por lo tanto no es un alto índice de desconocimiento del término y abría poca probabilidad de riesgo

A la pregunta N.º 2 **¿Ha recibido usted capacitación sobre seguridad de la información o informática?** Los encuestados respondieron así:

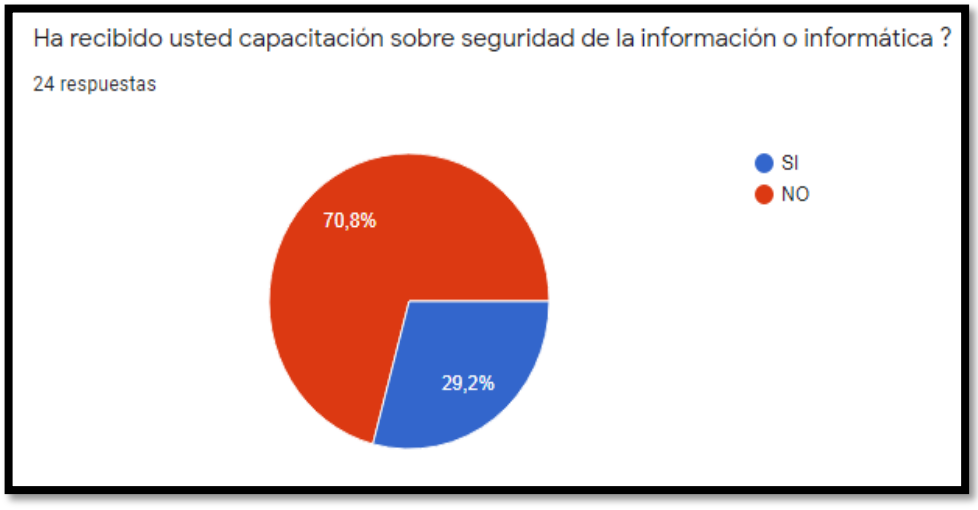
Tabla 2 pregunta 2 general cantidad y porcentaje

¿Ha recibido usted capacitación sobre seguridad de la información o informática?		
Opciones	**Cantidad**	**Porcentaje**
Si	7	29,2%
No	17	70,8%
Total	24	100

Fuente: Autor

Grafica reflejo de resultados

Grafica 3 pregunta 2 general porcentajes



Fuente: Autor

Se puede verificar que de las 24 personas encuestadas 17 de ellas dicen que no han sido capacitadas en seguridad de la información o informática de las personas encuetadas se interpretan que el 77,3% no ha recibido capacitación con respeto a los temas y 7 de ellas afirman lo contrario en un porcentaje de 25%.

Como conclusión esta información no da a conocer que secretaria de Educación Departamental de Nariño no ha tenido interés de capacitar a los funcionarios en este importante tema de la Informática de Hoy, esta inconsistencia se convierte en gran peligro para esta entidad porque por falta de conocimiento muy seguramente haya más probabilidad de convertirse en víctima de los delincuentes informáticos.

A la pregunta N.º 3 ¿**Se le ha presentado a usted o a algún compañero de su organización, algún incidente que haya generado perdida de información?** Los encuestados respondieron así:

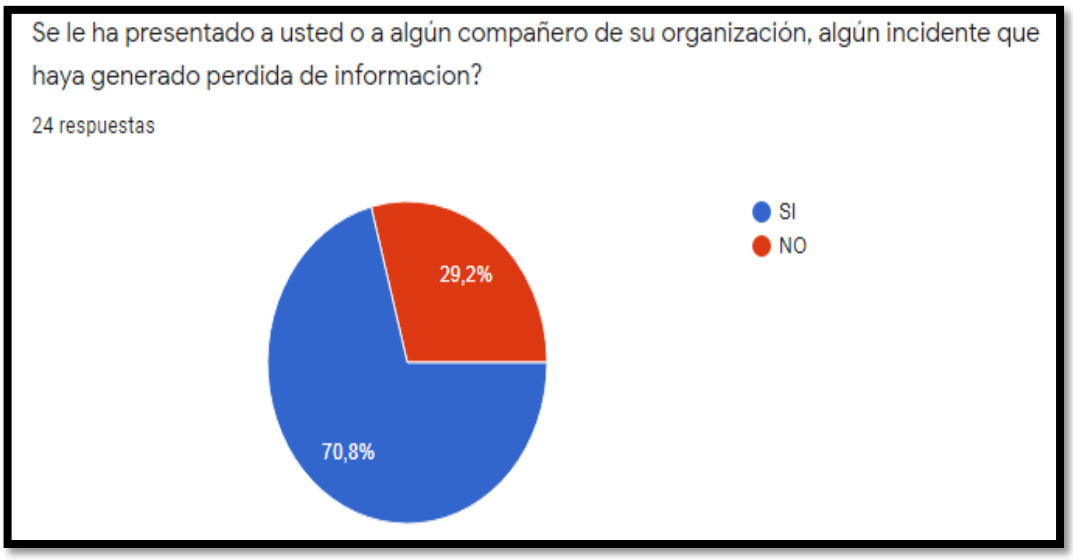
Tabla 3 pregunta 3 general cantidad y porcentaje

¿Se le ha presentado a usted o a algún compañero de su organización, algún incidente que haya generado perdida de información?		
Opciones	**Cantidad**	**Porcentaje**
Si	17	70,8%
No	7	29,2%
Total	24	100

Fuente: Autor

Grafica reflejo de resultados

Grafica 4 pregunta 3 general porcentajes



Fuente: Autor

Según este resultado de las 24 personas encuestadas 17 de ellas afirman sobre la perdida información y de igual manera algunos de sus compañeros de trabajo interpretando en un 70,8% este riesgo y 7 de ellas no son conocedoras de la situación el cual se representa en un 29,2%.

Esta evidencia es preocupante que los funcionarios de esta entidad han sido víctimas de estos incidentes informáticos que a causa desconocimiento hayan perdido información importante de su trabajo y que la entidad no instruya sus funcionarias los posibles riesgos a lo que están expuestos

A la pregunta N.º 4 **¿Sabe si su organización cuenta con políticas para la seguridad de la información?** *Los encuestados respondieron así:*

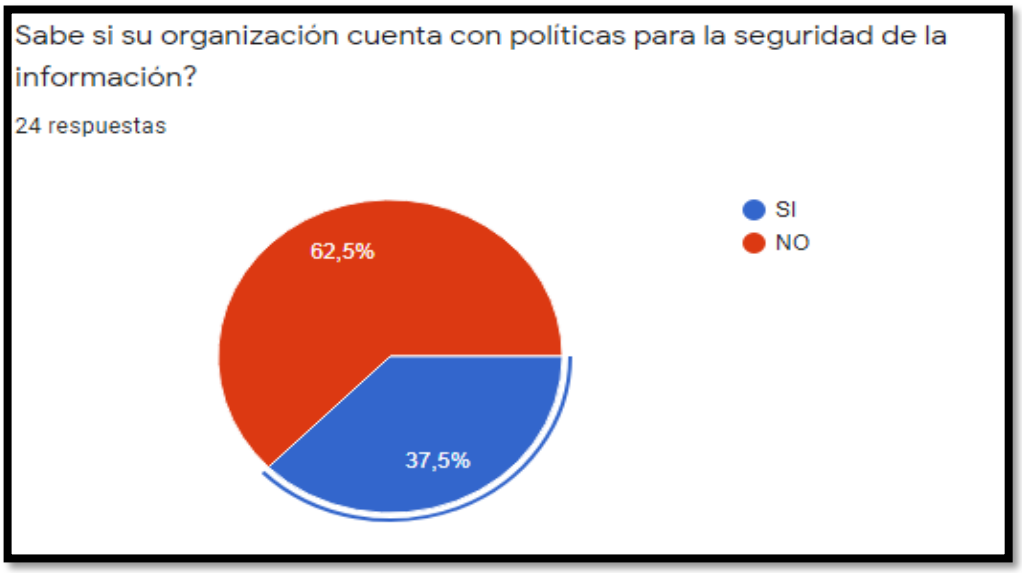
Tabla 4 pregunta 4 general cantidad y porcentaje

¿Sabe si su organización cuenta con políticas para la seguridad de la información?		
Opciones	**Cantidad**	**Porcentaje**
Si	*9*	*37,5%*
No	*15*	*62,5%*
Total	*24*	*100*

Fuente: Autor

Grafica reflejo de resultados

Grafica 5 pregunta 4 general porcentajes



Fuente: Autor

Como resultado de las 24 personas encuetadas 9 de ellas afirman la existencia en esta entidad políticas de seguridad de la Información para equivalencia de un

37,5% de la población y 15 de ellas no tienen conocimiento alguno del tema y su equivalencia es de 62,5% de la población.

Esta interpretación es de gran preocupación que los funcionarios no tengan en claro o definido la existencia de las políticas de Seguridad de la información, esto deja como evidencia que en la en la secretaria de educción Departamental de Nariño no tiene trasparencia en estas directrices. y es imposible ayudar a controlar los riesgos que puedan afectar esta entidad.

A la pregunta N.º **5 ¿En caso de que la pregunta anterior sea afirmativa, usted las conoce y aplica en sus actividades?** Los encuestados respondieron así:

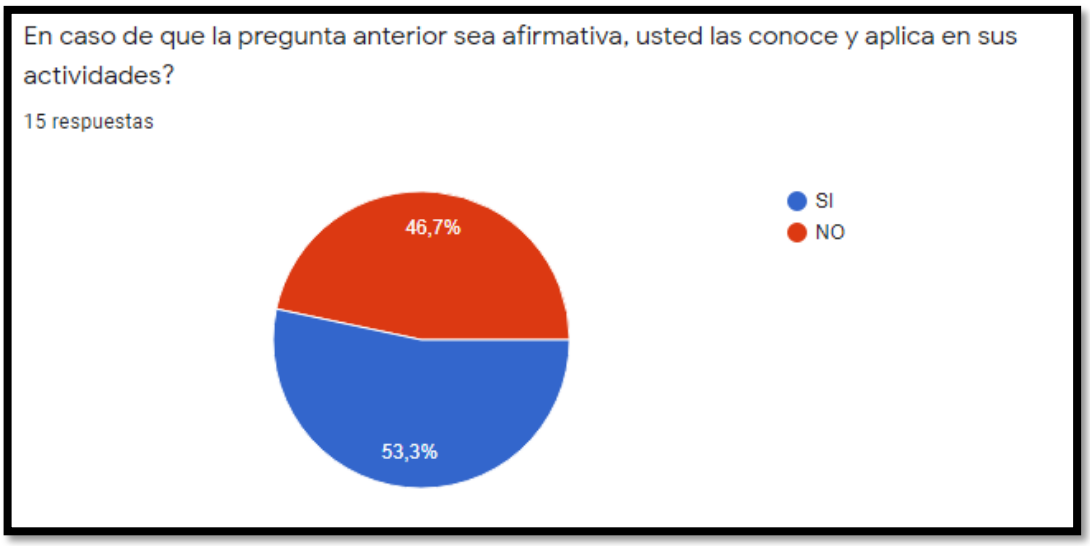
Tabla 5 pregunta 5 general cantidad y porcentaje

¿En caso de que la pregunta anterior sea afirmativa, usted las conoce y aplica en sus actividades?		
Opciones	**Cantidad**	**Porcentaje**
Si	8	53,3%
No	7	46,7%
Total	15	100

Fuente: Autor

Grafica reflejo de resultados

Grafica 6 pregunta 5 general porcentajes



Fuente: Autor

Con este resultado de las 24 personas encuestadas 8 de ellas respondieron que conocen y aplican estas políticas para un porcentaje de 53,3% de la población y 7 de ellas no tienen conocimiento sobre el tema para una equivalencia del al de 46,7% los encuestados

Esta pregunta refleja que en la secretaria de Educación Departamental de Nariño no existe claridad con respeto a estas políticas de seguridad de la información por la tanto se mira la necesidad en realidad de la trasparencia en estas directrices para los funcionarios de esta entidad.

A la pregunta N.º 6 **¿Conoce la ruta para identificar y reportar algún incidente de seguridad?** Los encuestados respondieron así:

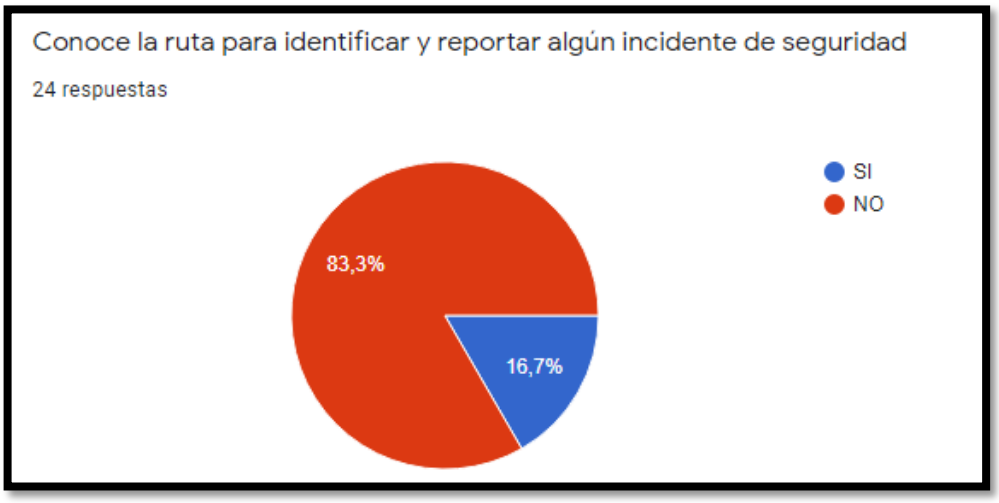
Tabla 6 pregunta 6 general en cantidad y porcentaje

¿Conoce la ruta para identificar y reportar algún incidente de seguridad?		
Opciones	**Cantidad**	**Porcentaje**
Si	4	16,7%
No	20	83,3%
Total	24	100

Fuente: Autor

Grafica reflejo de resultados

Grafica 6 de pregunta 7 general porcentajes



Fuente: Autor

Como resultado de las 24 personas encuetadas 20 tienen total desconocimiento sobre las rutas para identificar y reportar algún incidente de seguridad, para equivalencia de un 83,3% de la población y 4 de ellas no tienen conocimiento alguno del tema y su equivalencia es de 16,7% de la población

Se puede deducir que de los funcionarios encuestados la mayor parte no son conocedores al el manejo e identificación de estas rutas de reporte de seguridad de la información, este incidente hace de que el personal de la Secretaria de Educación Departamental se vea vulnerable incapaz de manejar adecuadamente los incidentes de seguridad de la información ni de dar un repuesta más eficiente y adecuada.

A la pregunta N.º 7 **¿Cada cuánto cambia sus contraseñas de ingreso a las aplicaciones, correos o plataformas de su trabajo?** Los encuestados respondieron así:

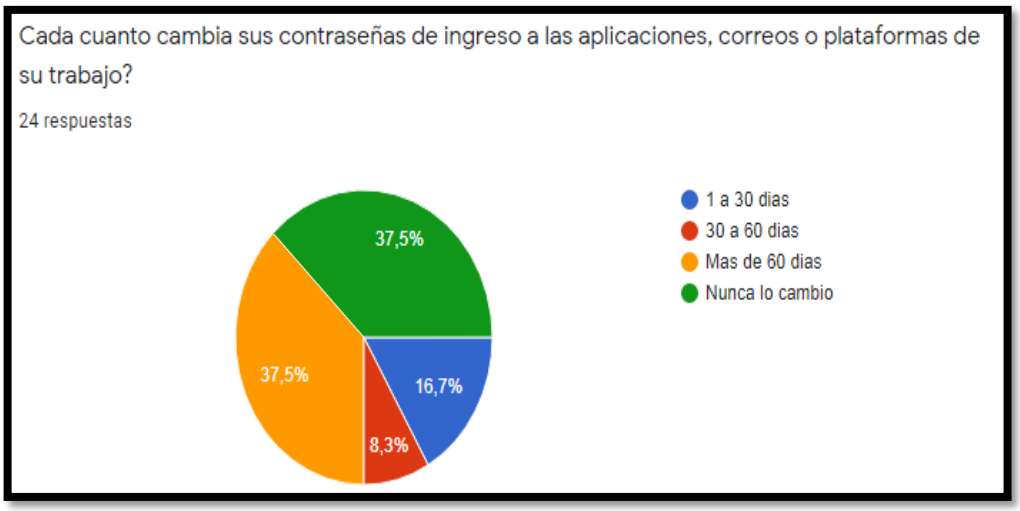
Tabla 7 pregunta 7 general en cantidad y porcentaje

¿Cada cuanto cambia sus contraseñas de ingreso a las aplicaciones, correos o plataformas de su trabajo?		
Opciones	**Cantidad**	**Porcentaje**
1 a 30 días	4	16,7%
30 a 60dias	2	8,3%
Mas de 60 días	9	37,5%
Nunca lo cambio	9	37,5%
Total	*24*	100

Fuente: Autor

Grafica reflejo de resultados

Grafica 8 pregunta 7 general porcentaje



Fuente: Autor

Como resultado de las 24 personas encuestadas con respecto a cada cuanto cambia sus contraseñas de ingreso a las aplicaciones, correos y plataformas de su trabajo, para esta pregunta se tomaron las siguientes opciones donde los encuestado respondieron así:

De la opción 1 a 30 días, 4 de los funcionarios respondieron esta opción
De la opción 30 a 60 días 2 de los funcionarios respondieron esta opción
De la opción más de 60 días, 9 de los funcionarios respondieron esta opción
De la opción nunca la cambio, 9 de los funcionarios respondieron esta opción

Con estos resultados se logra deducir que un gran porcentaje de los funcionarios encuestados no son conscientes del alto riesgo que esto atañe para la seguridad de la información personal y de esta entidad como es la secretaria de Educación Departamental de Nariño y esta forma del manejo de accesos, da la inseguridad de ser víctimas de diferentes prácticas de obtener información como la Ingeniera social.

A la pregunta N.º 8 **¿Usted utiliza contraseñas complejas (Longitud mínima 8, caracteres mayúscula/minúscula, números, caracteres especiales?** Los encuestados respondieron así:

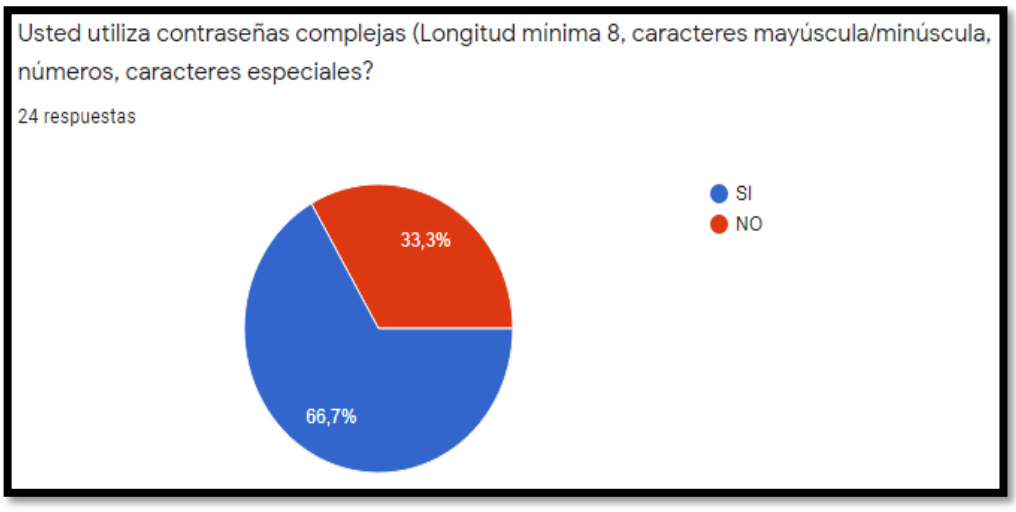
Tabla 8 pregunta 8 general en cantidad y porcentaje

¿Usted utiliza contraseñas complejas (Longitud mínima 8, caracteres mayúscula/minúscula, números, caracteres especiales?		
Opciones	**Cantidad**	**Porcentaje**
Si	16	66,7%
No	8	33,3%
Total	22	100

Fuente: Autor

Grafica reflejo de resultados

Grafica 9 pregunta 8 general porcentaje



Fuente: Autor

Se puede verificar que de las 24 personas encuestadas 16 de ellas utilizan contraseñas complejas, para equivalencia de un 66,7% de la población y 8 de ellas no tienen encuesta estos parámetros de seguridad para un porcentaje de 33,3% de la población.

En conclusión, con estas respuestas según la muestra de la población deja como evidencia que los funcionarios manejan una buena estrategia a la hora de generar una contraseña segura para salvaguardar la información, por lo tanto, hay poca probabilidad de ser víctima de muchos riesgos de quien somos acechados donde pueden acceder a la información robar nuestras contraseñas y suplantar nuestra identidad y estar propensos a que utilicen para algún tipo de fraude.

A la pregunta N.º 9 **¿Considera La información que maneja es vulnerable?** Los encuestados respondieron así:

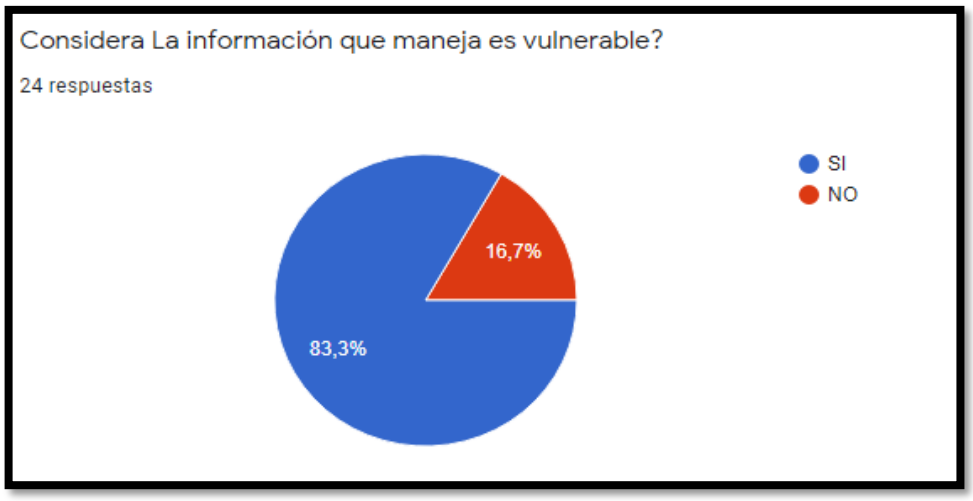
Tabla 9 pregunta 9 general en cantidad y porcentaje

¿Considera La información que maneja es vulnerable?		
Opciones	**Cantidad**	**Porcentaje**
Si	20	83,3%
No	4	16,7%
Total	24	100

Fuente: Autor

Grafica reflejo de resultados

Grafica 10 pregunta 9 general porcentaje



Fuente: Autor

Como resultado de las 24 personas encuetadas 20 de ellas son conscientes de la vulnerabilidad de información que maneja, para equivalencia de un 83,3% de la población y 4 de ellas no le dan la importancia que esta requiere por lo tanto no hay conciencia de su vulnerabilidad que existe en la información para un porcentaje de 16,7%.de población encuestada.

Esta interpretación deja en claro que los funcionarios de la Secretaria de Educación departamental son conscientes del riesgo de la información que ellos manejan por lo tanto es de vital importancia que esta entidad brinde medidas preventivas para mantener a salvo el activo más importante como es la información.

10.2 NAVEGACIÓN EN LA RED:

Esta serie de preguntas tiene como objetivo de recolectar información referida a Navegación en Red como conocimientos, hábitos, preferencias y tendencias a los funcionarios en la secretaria de educación del departamental de Nariño para indagar si saben identificar sitios no seguros o de poca seguridad y también determinar con

que responsabilidad hacen utilización del internet y mejorar su protección en caso de que sea necesario.

A la pregunta N.º 10 **¿Conoce usted como navegar en la red de manera segura?** Los encuestados respondieron así:

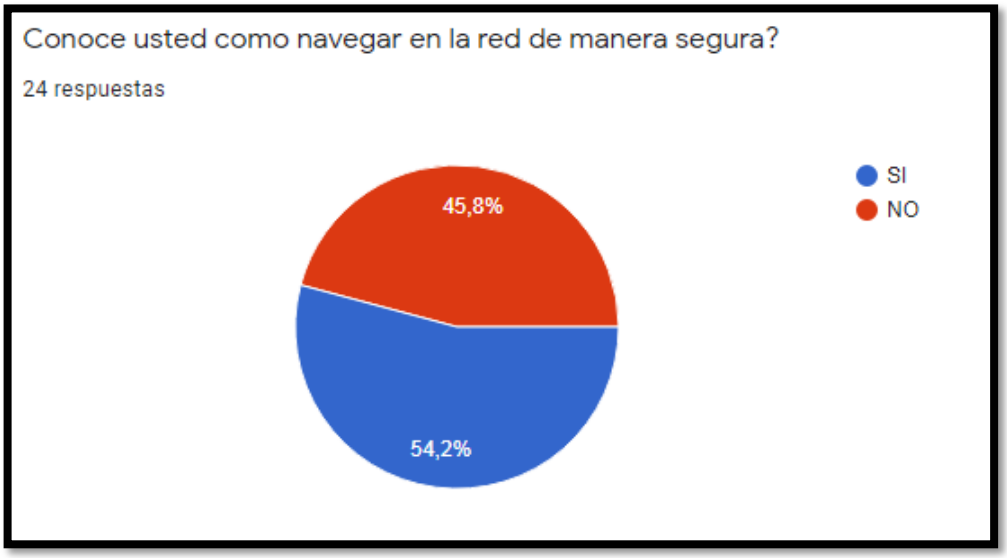
Tabla 10 pregunta 10 general en cantidad y porcentaje

¿Conoce usted como navegar en la red de manera segura?		
Opciones	**Cantidad**	**Porcentaje**
Si	13	54,8%
No	11	45,8%
Total	24	100

Fuente: Autor

Grafica reflejo de resultados

Grafica 11 pregunta 10 general porcentaje



Fuente: Autor

Se puede verificar que de las 24 personas encuestadas 13 de ellas tienen conocimiento como navegar en una red de manera más, para equivalencia de un 54,2% de la población y 11 de ellas desconocen la manera de hacerlos para un porcentaje de 45,8% de la población.

De acuerdo con este estudio se verifica que de las personas encuestadas no hay mucha claridad en la manera de segura de navegación en red ya que la diferencia en los resultados es muy mínima por los tanto es de gran importancia que la Secretaria de Educación del departamento de Nariño capacite a sus funcionarios en como navegar en forma segura en la Red.

A la pregunta N.º 11 **¿Usted utiliza los equipos de su trabajo, para acceder a sitios que no tienen que ver son sus actividades para desarrollar o páginas de interés personal?** Los encuestados respondieron así:

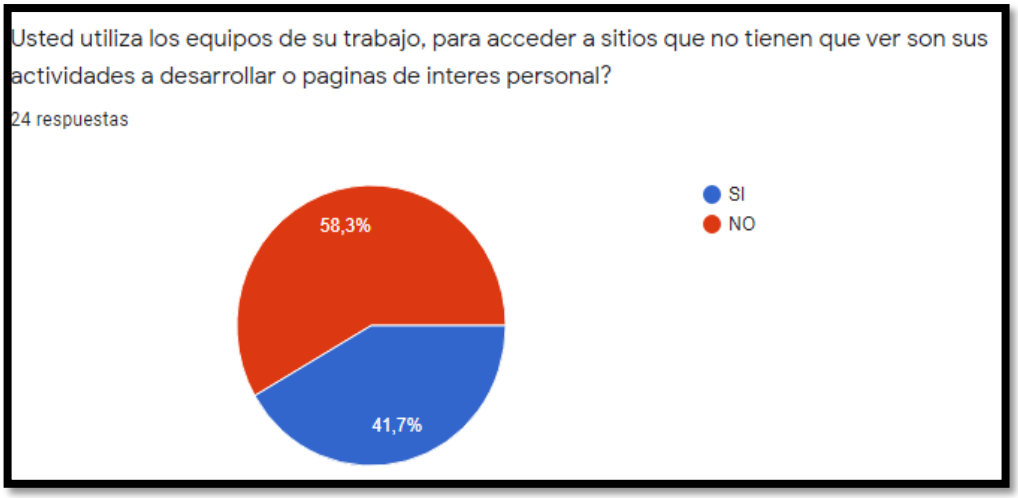
Tabla 11 pregunta 11 general en cantidad y porcentaje

¿Usted utiliza los equipos de su trabajo, para acceder a sitios que no tienen que ver son sus actividades para desarrollar o páginas de interés personal?		
Opciones	**Cantidad**	**Porcentaje**
Si	10	41,7%
No	14	58,3%
Total	24	100

Fuente: Autor

Grafica reflejo de resultados

Grafica 12pregunta 11 general porcentaje



Fuente: Autor

Como resultado de las 24 personas encuestadas 14 de ellas no utilizan los equipos de su trabajo para acceder a sitios o páginas de interés personal, para equivalencia de un 58,3% de la población y 10 de ellas no tienen la precaución necesaria para acceder utilizar y acceder a sitios personales para un porcentaje de 41,7%.de población encuestada.

En conclusión, con estas respuestas según la muestra de la población deja como evidencia que algunos funcionarios no tienen las precauciones necesarias para la utilización de los cómputos de trabajo con fines personales, esta falta de conciencia pone en riesgo directo a toda la clase de información confidencial de la entidad

A la pregunta N.º 12 **¿Hace caso a los mensajes de advertencia que emite los navegadores y soluciones antivirus cuando le alertas que los sitios no son seguros?** Los encuestados respondieron así:

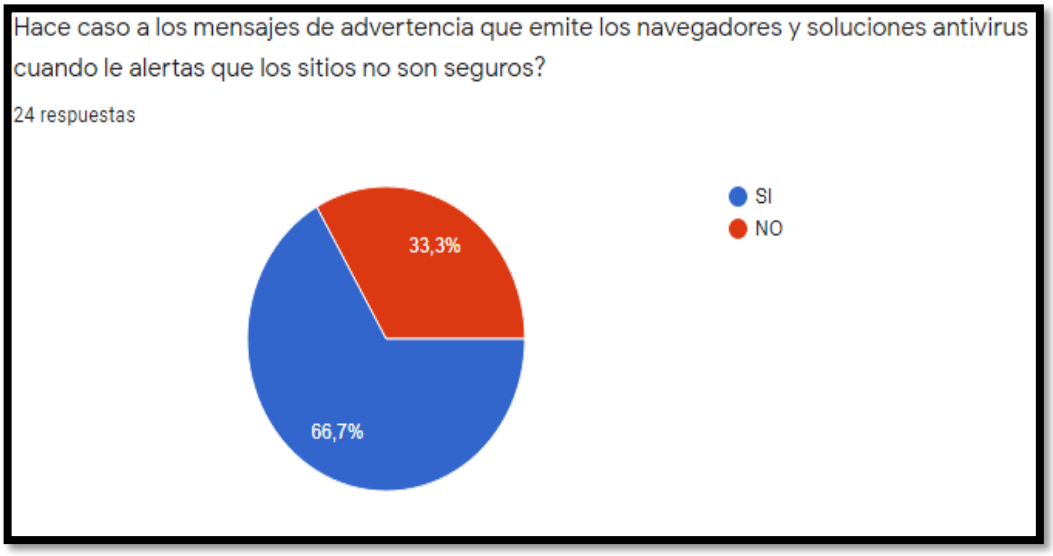
Tabla 12 pregunta 12 general en cantidad y porcentaje

¿Hace caso a los mensajes de advertencia que emite los navegadores y soluciones antivirus cuando le alertas que los sitios no son seguros?		
Opciones	**Cantidad**	**Porcentaje**
Si	16	66,7%
No	8	33,3%
Total	24	100

Fuente: Autor

Grafica reflejo de resultados

Grafica 13 pregunta 12 general porcentaje



Fuente: Autor

Como resultado las 24 personas encuetadas 16 de ellas acatan la advertencia que emiten los navegadores cuando los sito nos son seguros, para un porcentaje de la

población de 66,7% y 8 de ellas no tiene encueta estas advertencias para un porcentaje de 33,3% de población encuestada.

Como conclusión de acuerdo con el resultado algunos de los funcionarios de la Secretaria de Educación Departamental ignoran estas advertencias sin tener en cuenta la veracidad de su procedencia y sin tomar las precauciones necesarias para cada situación.

A la pregunta N.º 13 **¿Usted tiene conectado su teléfono o dispositivo móvil a la red de internet de su trabajo?** Los encuestados respondieron así:

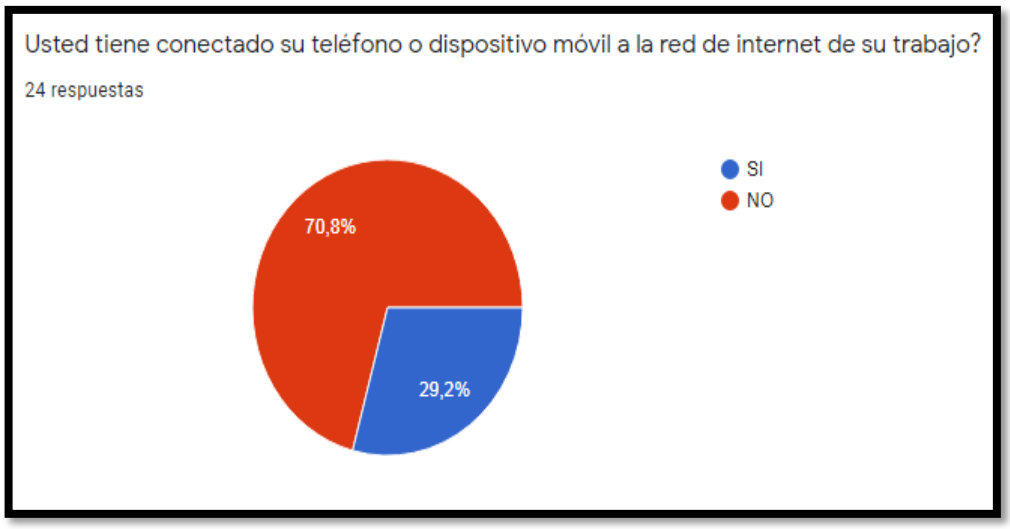
Tabla 13 pregunta 13 general en cantidades y porcentaje

¿Usted tiene conectado su teléfono o dispositivo móvil a la red de internet de su trabajo?		
Opciones	**Cantidad**	**Porcentaje**
Si	7	29,2%
No	17	70,8%
Total	24	100

Fuente: Autor

Grafica reflejo de resultados

Grafica 14 pregunta 13 general porcentaje



Fuente: Autor

Según este resultado de las 24 personas encuestadas 17 de ellas manifiestan que no acceden con sus móviles a red internet de la entidad el cual se interpretada en un 70,8% este riesgo y 7 de ellas hacen uso de la red de internet el cual se representa en un 29,2%.

Esta interpretación deja en claro que los funcionarios de la Secretaria de Educación departamental de Nariño son conscientes de no hacer uso de la Red de internet de su trabajo, por riesgo que esto representa ya sea para sus datos personales y para la Entidad ya que están en la misma condición de la perdida de la información personal y privada que estos manejan

A la pregunta N.º 14 **¿Accedes a servicios bancarios u otros, con tus datos confidenciales en ordenadores públicos o en redes Wi-Fi abiertas sin contraseña?** Los encuestados respondieron así:

Tabla 14 pregunta 14 general cantidad y porcentaje

¿Accedes a servicios bancarios u otros, con tus datos confidenciales en ordenadores públicos o en redes Wi-Fi abiertas sin contraseña?		
Opciones	**Cantidad**	**Porcentaje**
Si	17	70,8%
No	6	29,2%
Total	24	100

Fuente: Autor

Grafica reflejo de resultados

Grafica 15 pregunta 14 general porcentaje

Fuente: Autor

Como resultado de las 24 personas encuetadas 17 de ellas no hacen uso de servicios personales como los bancarios de ordenadores públicos o redes Wifi-abiertas sin, para equivalencia de un 70,8% de la población y 6 de ellas no tienen la

precaución necesaria para acceder desde estos sitios esto a sitios confidenciales, esto equivale un porcentaje de 29,2%.de población encuestada.

En conclusión, a estas respuestas se mira que la mayoría de las personas encuestadas tienen precaución el acceso a servicios confidénciales de ordenadores públicos o redes Wifi-abiertas evitando así perdida de su identidad digital y sus consecuencias.

A la pregunta N.º 15 ¿**Tienes conocimiento que protocolos garantizan que las sesiones de navegación cifradas o seguras?** Los encuestados respondieron así:

Tabla 15 pregunta 15 general cantidad y porcentaje

¿Tienes conocimiento que protocolos garantizan que las sesiones de navegación cifradas o seguras?		
Opciones	**Cantidad**	**Porcentaje**
Si	7	50%
No	5	20,8%
No sabe	12	29,2%
Total	24	100

Fuente: Autor

Grafica reflejo de resultados

Grafica 16 pregunta 15 general porcentaje

Fuente: Autor

Como resultado de las 24 personas encuestadas con respecto a tienes conocimiento que protocolos garantizan que las sesiones de navegación cifradas o seguras; para esta pregunta se tomaron las siguientes opciones donde los encuestado respondieron así:

De la opción Si, 7 de los funcionarios respondieron esta opción

De la opción No 5 de los funcionarios respondieron esta opción

De la opción No Sabe, 12 de los funcionarios respondieron esta opción

Con estos resultados se logra deducir que un gran porcentaje de los funcionarios encuetados no son conocedores de los protocolos que garantizan las navegaciones cifradas o seguras por lo tanto es necesario que la secretaria de educación Departamental de Nariño capacite a los funcionarios en este tema informático para nos para tener todas las garantías en la navegación.

A la pregunta N.º 16 ¿**Usted considera que la información que maneja esta Entidad esta clasifica de acuerdo con al nivel apropiado de protección?** Los encuestados respondieron así:

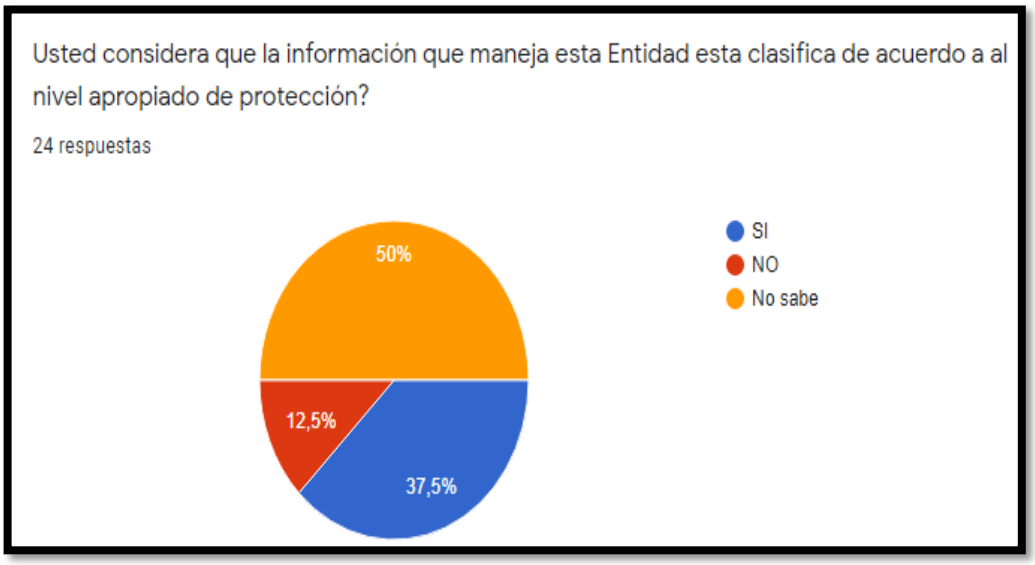
Tabla 16 pregunta 16 general en cantidad y porcentaje

¿Usted considera que la información que maneja esta Entidad esta clasifica de acuerdo con al nivel apropiado de protección?		
Opciones	**Cantidad**	**Porcentaje**
Si	9	37,5%
No	3	12,5%
No sabe	12	50%
Total	24	100

Fuente: Autor

Grafica reflejo de resultados

Grafica 17 pregunta 16 general porcentaje



Fuente: Autor

Como resultado de las 24 personas encuestadas con respecto a tienes conocimiento que protocolos garantizan que las sesiones de navegación cifradas o seguras; para esta pregunta se tomaron las siguientes opciones donde los encuestado respondieron así:

De la opción Si, 9 de los funcionarios respondieron esta opción
De la opción No 3 de los funcionarios respondieron esta opción
De la opción No Sabe, 12 de los funcionarios respondieron esta opción

Con estos resultados se puede apreciar que existe la probabilidad de la que la Secretaria de Educación del Departamento no clasifica de acuerdo con el nivel apropiado de protección la información por los tanto es de vital importancia que tomar medidas organizacionales necesarias para proteger los activos de información de acuerdo con el grado o nivel de protección.

10.3 HERRAMIENTAS Y APLICACIONES PARA LA SEGURIDAD DE LA INFORMACIÓN

Las preguntas que a continuación se relacionan con respecto a las Herramientas y aplicaciones de seguridad de la Información se pretende que proporcione la información necesaria para identificar el nivel de madurez funcionarios en la secretaria de educación del departamental de Nariño en la implementación de herramientas y aplicaciones con el fin de proporcionar las medidas de controles y usos de las mejoras prácticas de seguridad.

A la pregunta N.º 17 **¿Sabe utilizar antivirus?** Los encuestados respondieron así:

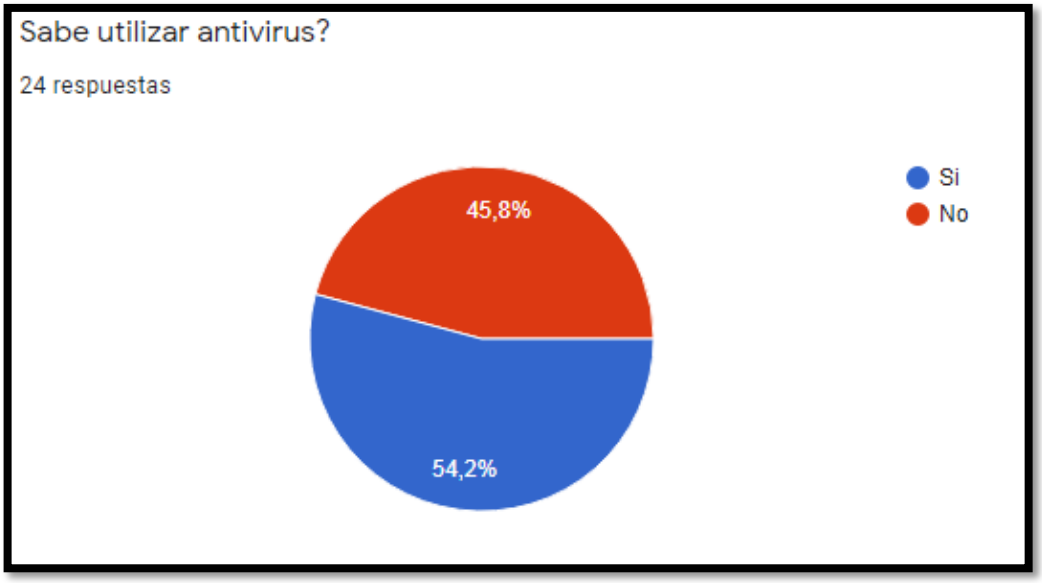
Tabla 17 pregunta 17 general cantidad y porcentaje

¿Sabe utilizar antivirus?		
Opciones	**Cantidad**	**Porcentaje**
Si	13	45,8%
No	11	54,2%
Total	24	100

Fuente: Autor

Grafica reflejo de resultados

Grafica 18 pregunta 17 general porcentaje



Fuente: Autor

Como resultado de las 24 personas encuetadas 13 de ellas saben utilizar antivirus, para equivalencia de un 54,2% de la población y 11 de ellas no saben o no hacen el uso de esta herramienta, esto equivale un porcentaje de 45,8%.de población encuestada.

De acuerdo con este estudio se verifica que de las personas encuestadas no hay mucha claridad en el uso de antivirus ya que la diferencia en los resultados es muy mínima por los tanto es de gran importancia que la Secretaria de Educación del departamento de Nariño estipule políticas de seguridad para el uso de antivirus

A la pregunta N.º ***18 ¿*****Cuenta su computador, teléfono, tables u otro dispositivo algún antivirus instalado?** Los encuestados respondieron así:

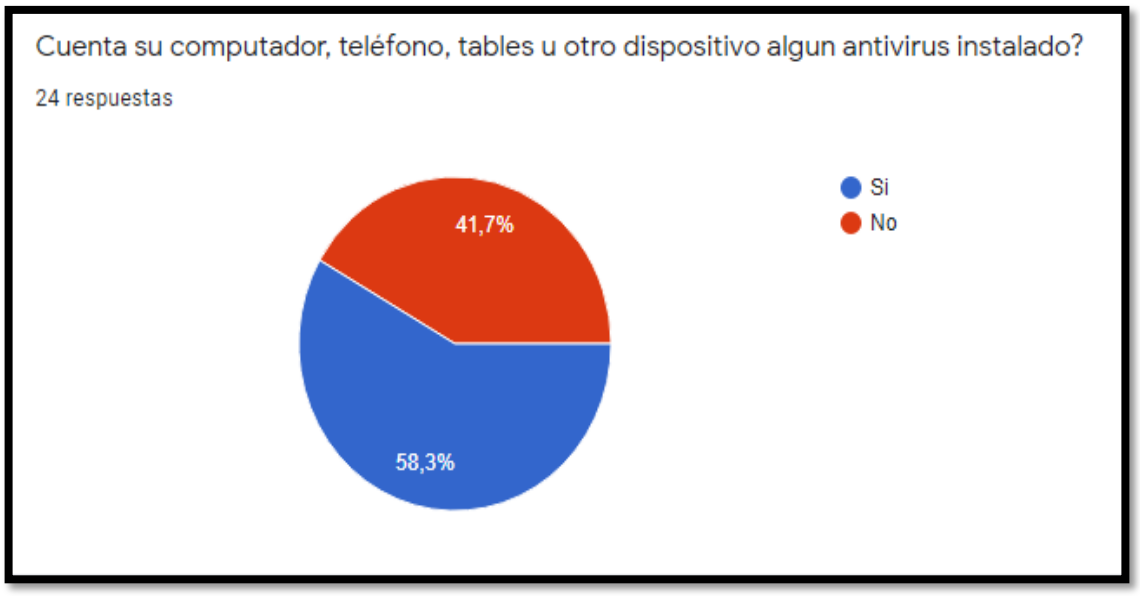
Tabla 18 pregunta 18 general cantidad y porcentaje

¿Cuenta su computador, teléfono, tables u otro dispositivo algún antivirus instalado?		
Opciones	**Cantidad**	**Porcentaje**
Si	14	58,3%
No	10	41,7%
Total	24	100

Fuente: Autor

Grafica reflejo de resultados

Grafica 19 pregunta 18 general porcentaje



Fuente: Autor

Como resultado de las 24 personas encuetadas 14 de ellas hacen uso de antivirus en sus dispositivos de trabajo o personal, para equivalencia de un 58,3% de la población y 10 de ellas no tienen la precaución y no hacen uso de esta herramienta informática, esto equivale un porcentaje de 41,7%.de población encuestada.

En conclusión, con este estudio se verifica que de las personas encuestadas no hay mucha claridad en el uso de antivirus en sus dispositivos de trabajo o personal ya que la diferencia en los resultados es muy mínima y eso deja como evidencia que hay poco interés en el uso de esta herramienta que como consecuencia trae problemas de perdida de información por causa de un virus informático

A la pregunta N.º 19 **¿Realiza copias de seguridad de la Información?** Los encuestados respondieron así:

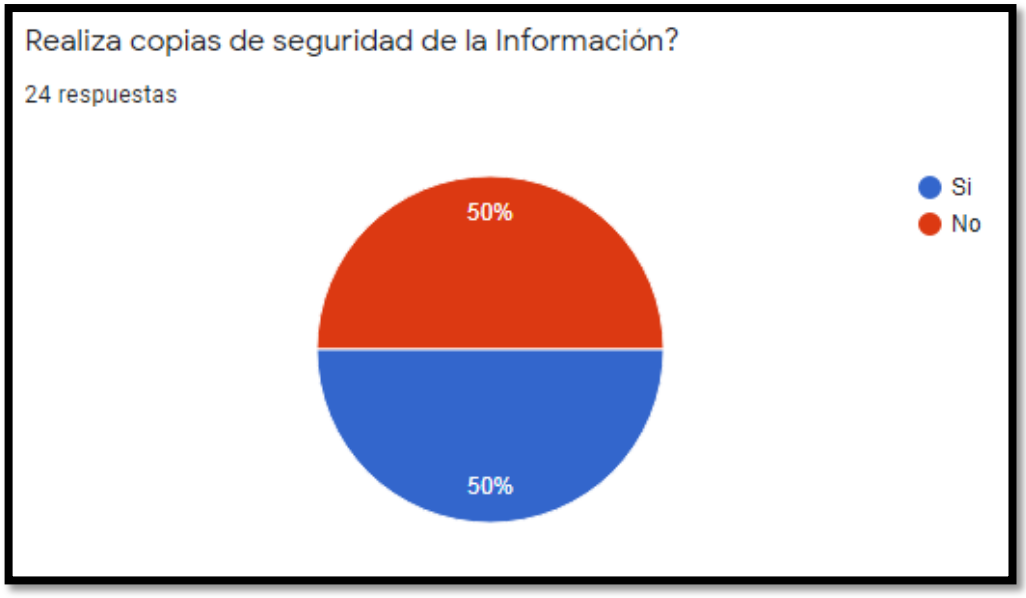
Tabla 19 pregunta 19 general cantidad y porcentaje

¿Realiza copias de seguridad de la Información?		
Opciones	**Cantidad**	**Porcentaje**
Si	12	50%
No	12	50%
Total	24	100

Fuente: Autor

Grafica reflejo de resultados

Grafica 20 pregunta 19 general porcentaje



Fuente: Autor

Como resultado las 24 personas encuetadas 12 de ellas realizan copias de seguridad de la información, para un porcentaje de la población de 50% y 12 de

ellas no tiene encueta o no considera necesaria desarrollar dicha acción para un porcentaje de 50% de población encuestada.

Con esta igualdad respuestas de se evidencia que en la Secretaria de Educación Departamental de Nariño se mira la necesidad de estipular políticas de copias de seguridad para que sean cumplidas y así evitar perdida de la Información.

A la pregunta N.º 20 **¿Sabes qué navegador web utilizas normalmente?** Los encuestados respondieron así:

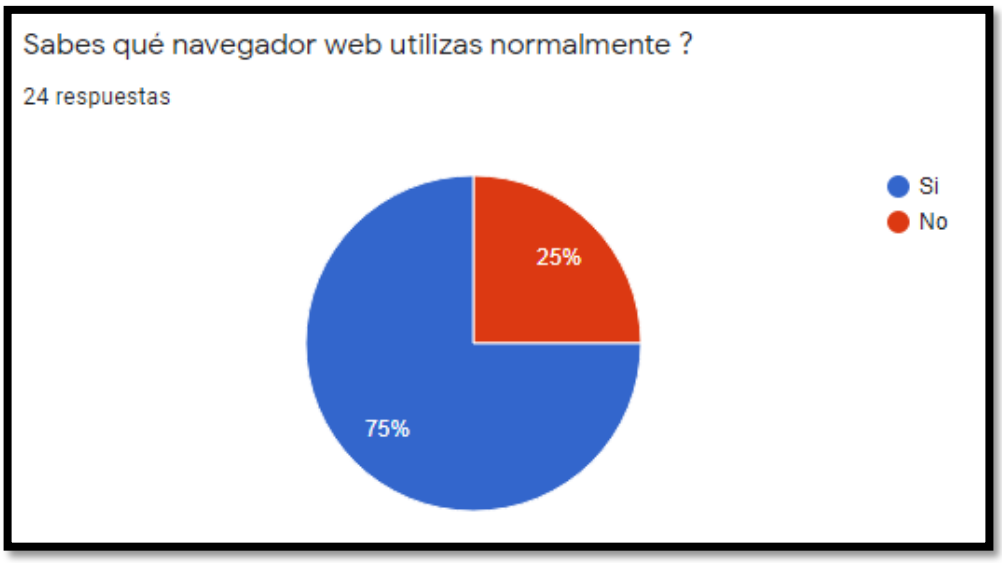
Tabla 20 pregunta 20 general cantidad y porcentaje

¿Sabes qué navegador web utilizas normalmente?		
Opciones	**Cantidad**	**Porcentaje**
Si	18	75%
No	6	25%
Total	24	100

Fuente: Autor

Grafica reflejo de resultados

Grafica 21 pregunta 20 general porcentaje



Fuente: Autor

Como resultado de las 24 personas encuetadas 18 de ellas saben navegador web utilizas, para equivalencia de un 75% de la población y 6 de ellas no tienen conocimiento de que navegador utilizan, para un porcentaje de 41,7%.de población encuestada

En conclusión, con estas respuestas según la muestra de la población deja como evidencia que algunos funcionarios no tienen conocimiento de la versión de navegador web que utiliza y es necesario que ellos lo sepan de la variedad de navegadores disponibles que existen para elegir de acuerdo con cada necesidad.

A la pregunta N.º 21 **¿Tu ordenador tiene actualizado el sistema operativo, programas o aplicaciones?** Los encuestados respondieron así:

Tabla 21 pregunta 21 general cantidad y porcentaje

¿Tu ordenador tiene actualizado el sistema operativo, programas o aplicaciones		
Opciones	**Cantidad**	**Porcentaje**
Si	8	33,3%
No	6	25%
No sabe	10	41.7%
Total	24	100

Fuente: Autor

Grafica reflejo de resultados

Grafica 22 pregunta 21 general porcentaje

Fuente: Autor

Como resultado de las 24 personas encuestadas con respecto a tienes conocimiento que protocolos garantizan que las sesiones de navegación cifradas o

seguras; para esta pregunta se tomaron las siguientes opciones donde los encuestado respondieron así:

De la opción Si, 8 de los funcionarios respondieron esta opción

De la opción No 6 de los funcionarios respondieron esta opción

De la opción No Sabe, 10 de los funcionarios respondieron esta opción

Con estos resultados se puede apreciar que en la Secretaria de Educación del Departamento no está atenta a las actualizaciones necesarias de los equipos de cómputo del personal, colocando en riesgo la seguridad de sus datos

10.4 INGENIERÍA SOCIAL

Siendo un tema tan importante de tratar en esta monografía se mira la necesidad indagar que cuan informados y que buenas prácticas de prevención tienen los funcionarios en la secretaria de educación del departamental de Nariño con respecto a la Ingeniería Social, la información proporcionada es una pieza fundamental como material de estudio con el fin de encontrar fortalezas o debilidades y tomar medidas que correspondan a dar solución a falencias encontradas.

A la pregunta N.º 22 **¿Sabe que es ingeniería social?** Los encuestados respondieron así:

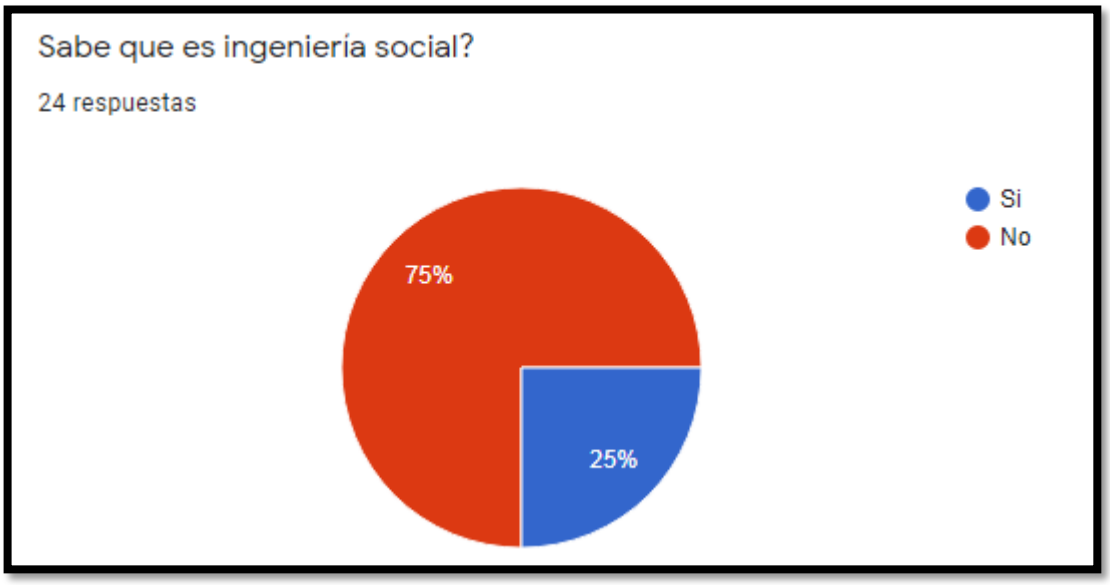
Tabla 22 pregunta 22 general cantidad y porcentaje

¿Sabe que es ingeniería social?		
Opciones	**Cantidad**	**Porcentaje**
Si	6	25%
No	18	75%
Total	22	100

Fuente: Autor

Grafica reflejo de resultados

Grafica 23 pregunta 22 general porcentaje



Fuente: Autor

Como resultado de las 24 personas encuetadas 13 de ellas saben utilizar antivirus, para equivalencia de un 54,2% de la población y 11 de ellas no saben o no hacen

el uso de esta herramienta, esto equivale un porcentaje de 45,8%.de población encuestada.

De acuerdo con este estudio se verifica que de las personas encuestadas no tienen claridad de esta amenaza informática, con este resultado no se puede asegurar que haya atención y protección de la información que maneja la secretaria de educación Departamental de Nariño frente a esta amenaza por tal razón urge que se capacite a los funcionarios sobre esta vulnerabilidad y sus diferentes técnicas.

A la pregunta N.º 23 ¿**En caso de que la pregunta anterior sea afirmativa, usted tiene conocimiento sobre las técnicas que utiliza la ingeniería social?** Los encuestados respondieron así:

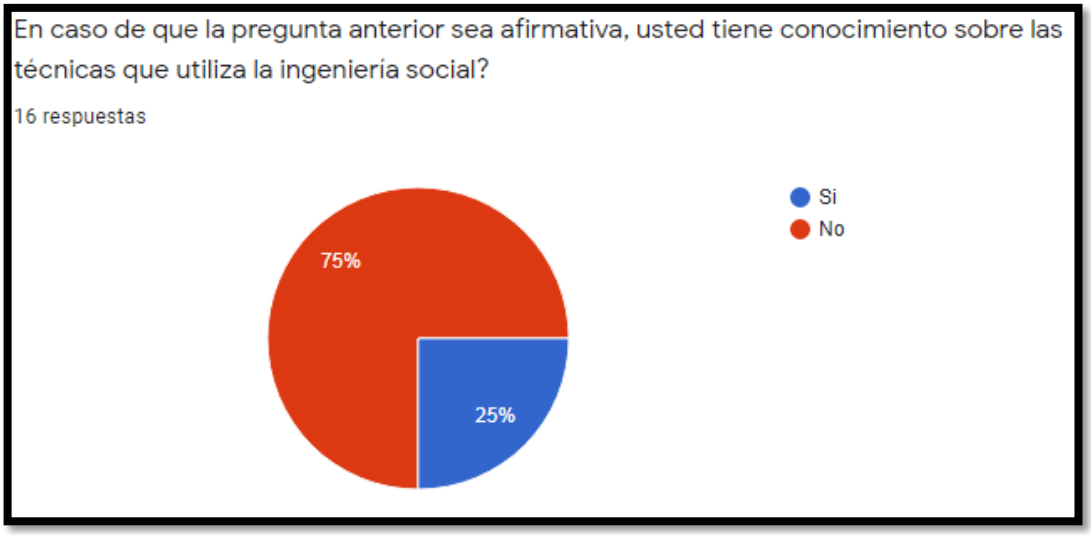
Tabla 23 pregunta 23 general cantidad y porcentaje

¿En caso de que la pregunta anterior sea afirmativa, usted tiene conocimiento sobre las técnicas que utiliza la ingeniería social?		
Opciones	**Cantidad**	**Porcentaje**
Si	12	75%
No	4	25%
Total	16	100%

Fuente: Autor

Grafica reflejo de resultados

Grafica 24 pregunta 23 general porcentaje



Fuente: Autor

Con este resultado de las 24 personas encuestadas 12 de ellas respondieron que no conocen las técnicas de Ingeniería social para un porcentaje del 75% de la población y 4 de ellas no tienen conocimiento sobre el tema para una equivalencia del al 25% de los encuestados

Esta pregunta refleja que los funcionarios de La secretaria de Educación Departamental de Nariño no tienen muy claro el tema en relacionado a la Ingeniera social y sus técnicas y es de gran preocupación que los empleados no tengan el conocimiento que esto requiere ya que ellos son los puntos directos para esta amenaza o ataque.

A la pregunta N.º 24 **¿Lee todos los correos que le llegan a su buzón, sin precaución?** Los encuestados respondieron así:

Tabla 24 pregunta 24 general cantidad y porcentaje

¿Lee todos los correos que le llegan a su buzón, sin precaución?		
Opciones	**Cantidad**	**Porcentaje**
Si	17	70,8%
No	7	29,2%
Total	24	100

Fuente: Autor

Grafica reflejo de resultados

Grafica 25 pregunta 24 general porcentaje

Fuente: Autor

Como resultado de las 24 personas encuetadas 17 de ellas no tiene la precaución necesaria para el acceso a correos que llegan al buzón, para equivalencia de un 70,8% de la población y 7 de ellas tienen la precaución necesaria esto equivale un porcentaje de 29,2%.de población encuestada.

En conclusión, con este estudio se verifica que de los funcionarios encuestados no hay la suficiente precaución para el acceso a estos correos, lo cual pone en riesgo a todos sus activos de información que maneja la Secretaría de educación departamental de Nariño.

A la pregunta N.º 25 **¿Cierra la sección de su sistema cada vez que se levanta se su equipo?** Los encuestados respondieron así:

Tabla 25 pregunta 25 general cantidad y porcentaje

¿Cierra la sección de su sistema cada vez que se levanta se su equipo?		
Opciones	**Cantidad**	**Porcentaje**
Si	16	66,7%
No	8	33,3%
Total	24	100

Fuente: Autor

Grafica reflejo de resultados

Grafica 26 pregunta 25 general porcentaje

Fuente: Autor

Se puede verificar que de las 24 personas encuestadas 16 de ellas tienen en claro la buena práctica de cerrar la sección, para equivalencia de un 54,2% de la población y 8 de ellas no tienen en cuenta, para un porcentaje de 45,8% de la población.

De acuerdo con este estudio se verifica que algunas de las personas encuestadas no son conscientes del riesgo de dejar en vulnerabilidad su equipo y con la mayor probabilidad de ser víctima de las técnicas de la Ingeniería y acceder a la información confidencial.

A la pregunta N.º 26 **¿Guarda información confidencial en su escritorio de la oficina, visible para cualquier persona?** Los encuestados respondieron así:

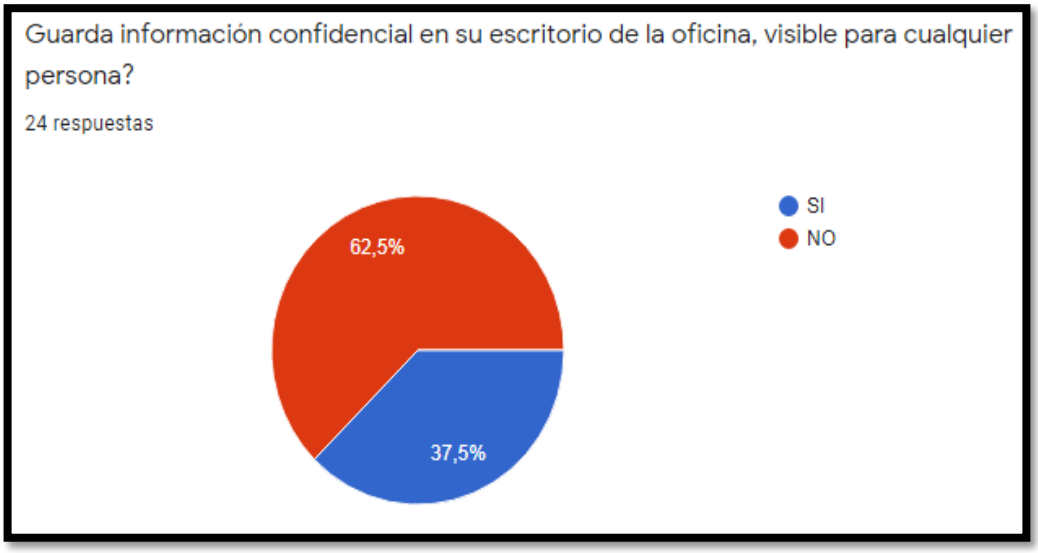
Tabla 26 pregunta 26 general cantidad y porcentaje

¿Guarda información confidencial en su escritorio de la oficina, visible para cualquier persona?		
Opciones	**Cantidad**	**Porcentaje**
Si	9	62,5%
No	15	37,5%
Total	24	100

Fuente: Autor

Grafica reflejo de resultados

Grafica 27 pregunta 26 general porcentaje



Fuente: Autor

Como resultado de las 24 personas encuetadas 9 de ellas guardan información confidencial en escritorio para equivalencia de un 37,5% de la población y 15 de ellas no dejan la información confidencial en el escritorio, su equivalencia es de 62,5% de la población encuestada.

Esta interpretación de los resultados deja en evidencia que algunos funcionarios de la secretaria de educción Departamental de Nariño no tienen la precaución

necesaria y deja la información confidencial visible expuesta a toda vulnerabilidad y dejan riesgos que puedan afectar esta entidad.

A la pregunta N.º 27 **¿Cambia sus contraseñas de ingreso a las aplicaciones, correos o plataformas de su trabajo?** Los encuestados respondieron así:

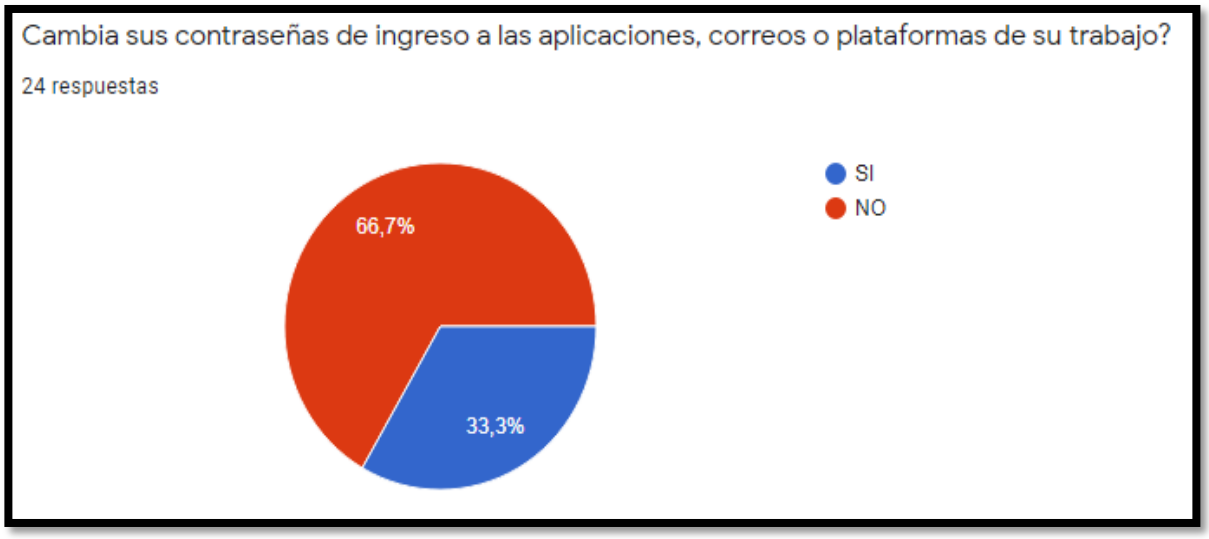
Tabla 27 pregunta 27 general cantidad y porcentaje

¿Cambia sus contraseñas de ingreso a las aplicaciones, correos o plataformas de su trabajo?		
Opciones	**Cantidad**	**Porcentaje**
Si	8	66,7%
No	16	33,3%
Total	24	100

Fuente: Autor

Grafica reflejo de resultados

Grafica 28 pregunta 27 general porcentaje



Fuente: Autor

Se puede verificar que de las 24 personas encuestadas 8 de ellas dicen cambiar contraseñas de ingreso a lo que requiera de su trabajo se interpretan que el 33,3% y 16 de ellas afirman lo contrario en un porcentaje de 66,7%.

Como conclusión esta información no da a conocer que los funcionarios de la secretaria de Educación Departamental de Nariño no tienen las precauciones necesarias del acceso o ingreso como es el cambio de contraseñas, por lo tanto, esta inconsistencia se convierte en gran peligro para esta entidad que seguramente haya más probabilidad de convertirse en víctima de los delincuentes informáticos.

A la pregunta N.º 28 **¿Es necesario la implementación de tecnologías de la seguridad informática?** Los encuestados respondieron así:

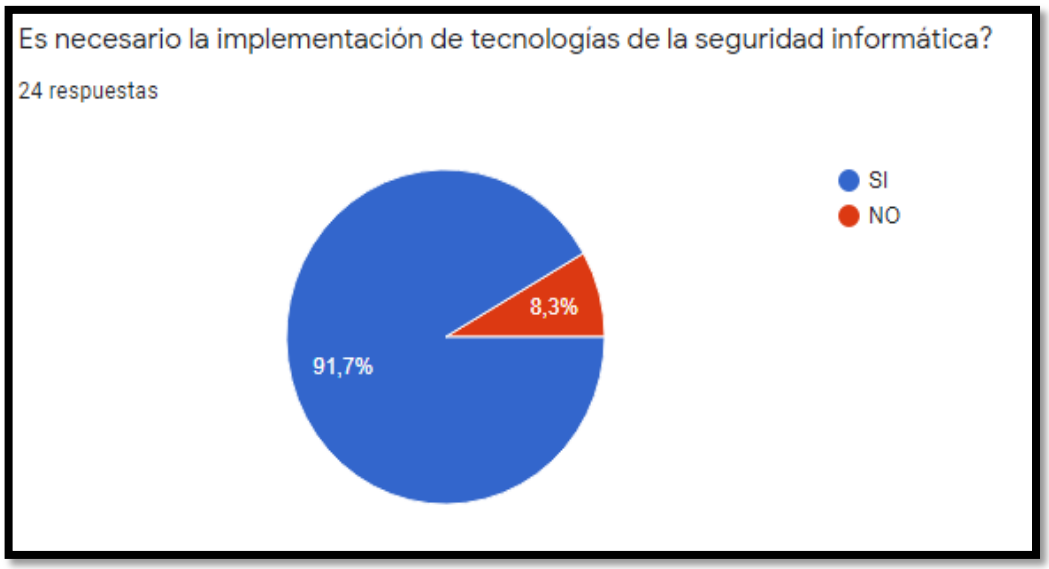
Tabla 28 pregunta 28 general cantidad y porcentaje

¿Es necesario la implementación de tecnologías de la seguridad informática?		
Opciones	**Cantidad**	**Porcentaje**
Si	22	91,7%
No	2	8,3%
Total	24	100

Fuente: Autor

Grafica reflejo de resultados

Grafica 29 pregunta 28 general porcentaje



Fuente: Autor

Como resultado de las 24 personas encuetadas 22 de ellas afirman la necesidad de la implantación de tecnologías de la seguridad informática, para equivalencia de un 8,3% de la población y 2 de ellas no tienen ningún interés, su equivalencia es de 62,5% de la población.

Esta interpretación deja en claro que para los funcionarios de la Secretaria de Educación Departamental de Nariño es gran importancia la implementación de tecnologías de la seguridad de la información esta es una de las buenas alternativas para conservación, protección, control adecuado de la información para ayudar a controlar los riesgos que puedan afectar esta entidad.

A la pregunta N.º 29 **¿Tiene conocimiento de las amenazas lógicas de los sistemas informáticos?** Los encuestados respondieron así:

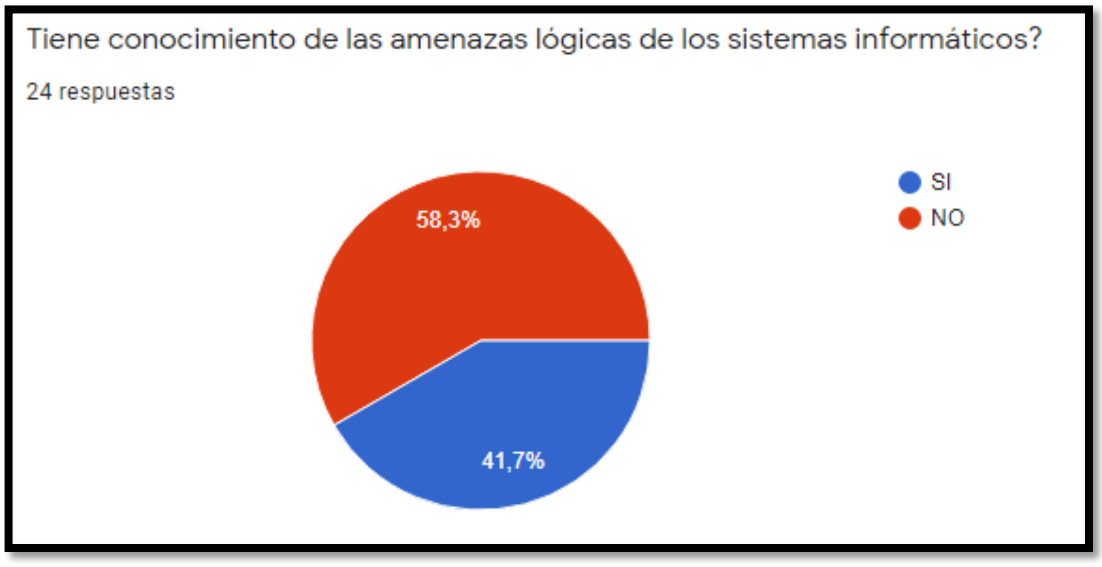
Tabla 29 pregunta 29 general cantidad y porcentaje

¿Tiene conocimiento de las amenazas lógicas de los sistemas informáticos?		
Opciones	**Cantidad**	**Porcentaje**
Si	10	58,3%
No	14	41,7%
Total	24	100

Fuente: Autor

Grafica reflejo de resultados

Grafica 30 pregunta 29 general porcentaje



Fuente: Autor

Como resultado las 24 personas encuetadas 10 de ellas tienen el conocimiento de las amenazas lógicas de los sistemas informáticos acatan la advertencia que emiten

los navegadores, para un porcentaje de la población de 41,7% y 14 de ellas no tiene conocimiento para un porcentaje de 58,3% de población encuestada.

Como conclusión de acuerdo con el resultado, algunos los funcionarios de la Secretaria de Educación Departamental de Nariño ignoran a este tipo amenazas por lo cual están propensos a accesos no autorizados y a todo tipo de fraude colocando en riesgo toda la información confidencial

A la pregunta N.º 30 ¿**Usted ha recibido llamadas sospechosas pidiendo información que comprometa esta Entidad?** Los encuestados respondieron así:

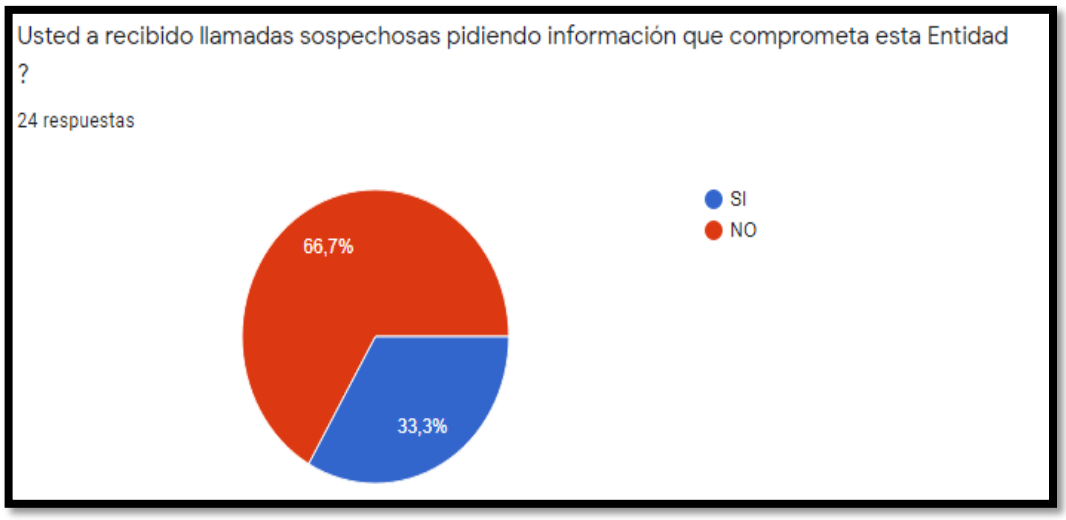
Tabla 30 pregunta 30 general cantidad y porcentaje

¿Usted ha recibido llamadas sospechosas pidiendo información que comprometa esta Entidad?		
Opciones	**Cantidad**	**Porcentaje**
Si	8	33,3%
No	16	66,7%
Total	24	100

Fuente: Autor

Grafica reflejo de resultados

Grafica 31 pregunta 3o general porcentaje



Fuente: Autor

Con este resultado de las 24 personas encuestadas 8 de ellas respondieron que han recibido llamadas sospechosas pidiendo información que comprometen a esta Entidad un porcentaje del 33,3% de la población y 16 de ellas no ha recibido llamadas para una equivalencia del 25% de los encuestados

Esta pregunta refleja que los funcionarios de La secretaria de Educación Departamental de Nariño también son víctimas de técnicas de Ingeniería Social y por falta de conocimiento eta en riesgo toda información que esta entidad maneja ya que son los puntos directos para esta amenaza o ataque.

10.5 RECOLECCIÓN DE DATOS DE LA ENCUESTA

Tabla 31- Recolección de datos de la Encuesta

Nº	Pregunta	Respuesta	Cant.	100%
1	¿Sabe usted que es Seguridad Informática?	Si	19	75%
		No	5	25%
		Total	**24**	**100%**
2	¿Ha recibido usted capacitación sobre seguridad de la información o informática?	Si	***7***	29,2%
		No	***17***	70,8%
		Total	**24**	**100%**
3	¿Se le ha presentado a usted o a algún compañero de su organización, algún incidente que haya generado perdida de información?	Si	**17**	70,8%
		No	7	29,2%
		Total	**24**	**100%**
4	¿Sabe si su organización cuenta con políticas para la seguridad de la información?	Si	10	37,5%
		No	**14**	62%
		Total	**24**	**100%**
5	¿En caso de que la pregunta anterior sea afirmativa, usted las conoce y aplica en sus actividades?	Si	7	53,3%
		No	8	46,7%
		Total	**15**	**100%**
6	¿Conoce la ruta para identificar y reportar algún incidente de seguridad?	Si	4	16,7%
		No	**20**	83,3%
		Total	**24**	**100%**
7	¿Cada cuanto cambia sus contraseñas de ingreso a las aplicaciones, correos o plataformas de su trabajo?	1 a 30 días	**4**	16,7%
		30 a 60 días	**2**	8,3%
		Mas de 60 Días	**9**	37,5%

		Nunca la cambio	**9**	37,5%
		Total	**24**	**100%**
8	¿Usted utiliza contraseñas complejas (Longitud mínima 8, caracteres mayúscula/minúscula, números, caracteres especiales?	Si	16	66,7%
		No	8	33,3%
		Total	**24**	**100%**
9	¿Considera La información que maneja es vulnerable?	Si	17	87,3%
		No	7	16,7%
		Total	**24**	**100%**
10	¿Conoce usted como navegar en la red de manera segura?	Si	14	45,8%
		No	10	54,2%
		Total	**24**	**100%**
11	¿Usted utiliza los equipos de su trabajo, para acceder a sitios que no tienen que ver son sus actividades por desarrollar o páginas de interés personal?	Si	10	41,7%
		No	14	58,3%
		Total	**24**	**100%**
12	¿Hace caso a los mensajes de advertencia que emite los navegadores y soluciones antivirus cuando le alertas que los sitios no son seguros?	Si	17	66,7%
		No	7	33,3%
		Total	**24**	**100%**
13	¿Usted tiene conectado su teléfono o dispositivo móvil a la red de internet de su trabajo?	Si	7	29,2%
		No	17	70,8%
		Total	**24**	**100%**
14	¿Accedes a servicios bancarios u otros, con tus datos confidenciales en ordenadores públicos o en redes Wi-Fi abiertas sin contraseña?	**Si**	**17**	29,2,8%
		No	7	70,8%
		Total	**24**	**100%**
15		Si	7	**29,2%**
		No	5	**20,8%**

	¿Tienes conocimiento que protocolos garantizan que las sesiones de navegación cifradas o seguras?	No sabe	**12**	**50%**
		Total	**24**	**100%**
16	¿Usted considera que la información que maneja esta Entidad esta clasifica de acuerdo a al nivel apropiado de protección?	Si	9	37,5%
		No	**2**	12,5%
		No sabe	**12**	50%
		Total	**24**	**100%**
17	¿Sabe utilizar antivirus?	Si	13	54,2%
		No	11	45,8%
		Total	**24**	**100%**
18	¿Cuenta su computador, teléfono, tables u otro dispositivo algún antivirus instalado?	Si	13	58,3%
		No	11	41,7%
		Total	**24**	**100%**
19	¿Realiza copias de seguridad de la Información?	Si	12	50%
		No	12	50%
		Total	**24**	**100%**
20	¿Tu ordenador tiene actualizado el sistema operativo, programas o aplicaciones?	Si	9	33,3%
		No	**6**	25%
		No lo sabe	**9**	41,7%
		Total	**24**	**100%**
21	¿Sabes qué navegador web utilizas normalmente?	Si	8	25%
		No	**18**	75%
		Total	24	100%
22	¿Sabe que es ingeniería social?	Si	6	25%
		No	**18**	75%
		Total	**24**	**100%**
23	¿En caso de que la pregunta anterior sea afirmativa, usted tiene conocimiento sobre las técnicas que utiliza la ingeniería social?	Si	4	25%
		No	13	75%
		Total	**17**	**100%**

24	¿Lee todos los correos que le llegan a su buzón, sin precaución?	Si	7	70,8%
		No	17	29,2%
		Total	**24**	100%
25	¿Cierra la sección de su sistema cada vez que se levanta se su equipo?	Si	17	66,7%
		No	7	33,3%
		Total	**24**	**100%**
26	¿Guarda información confidencial en su escritorio de la oficina, visible para cualquier persona?	Si	9	37,5%
		No	15	62,5%
		Total	**17**	**100%**
27	¿Cambia sus contraseñas de ingreso a las aplicaciones, correos o plataformas de su trabajo?	Si	9	33,3%
		No	**15**	66,7%
28	¿Es necesario la implementación de tecnologías de la seguridad informática?	Si	**22**	91,7%
		No	2	8,3%
		Total	**24**	**100%**
29	¿Tiene conocimiento de las amenazas lógicas de los sistemas informáticos?	Si	11	58,3%
		No	**13**	41,7%
		Total	**17**	**100%**
30	¿Usted ha recibido llamadas sospechosas pidiendo información que comprometa esta Entidad?	Si	8	33,3,8%
		No	16	66,7,2%
		Total	24	100%

Fuente: Autor

10.6 ANÁLISIS DE LA ENCUESTA

Mediante los datos recolectados de la encuesta realizada a los funcionarios de la Secretaria de Educación Departamental de Nariño y luego de la interpretación de cada gráfica, de acuerdo con las respuestas dadas por los funcionarios se logra evidenciar que el personal de esta entidad de educación tiene mucho desconocimiento en todo lo relacionado a Seguridad Informática y Seguridad de la Información, lo cual conlleva a poner en riesgo tecnológico y especialmente al manejo de la información.

A continuación, se relacionan los puntos más críticos que se logró determinar con la anterior encuesta

Tabla 32_ Analís de la Encuesta

Puntos Críticos	Rta. Individual	Total Respuestas
✓ Desconocimiento términos de seguridad ✓ Perdida de información personal, de la entidad por falta de asesoramiento	17 17	34
✓ Falta de claridad y trasparencia en políticas de seguridad de la información ✓ No se manejan ni identifican rutas para reportar algún incidente de seguridad.	14 20	34
✓ Falta de conciencia en uso de correos y el manejo de sus contraseñas de aplicaciones correos y plataformas.	18 15 17	50

✓ Falta de conocimiento en protocolos que garanticen las secciones de Navegación cifradas y seguras. Y de las amenazas lógicas de los sistemas informáticos	12 13	25
✓ No hay claridad en actualizaciones informáticas y navegadores ✓ No hay clasificación de la información de acuerdo con la protección que ella amerita	15 18	33
✓ Los funcionarios no están familiarizados con la ingeniería social ✓ Ni sus técnicas.	18 13	31
✓ Usted considera que la información que maneja esta Entidad esta clasifica de acuerdo a al nivel apropiado de protección.	14	14
✓ ¿Es necesario la implementación de tecnologías de la seguridad informática?	22	22

Fuente: Autor

La tabla anterior N.º 32, presenta los puntos más críticos encontrados en la encuesta realizada, donde evidencia la cantidad de respuestas de cada participante y en totalidad.

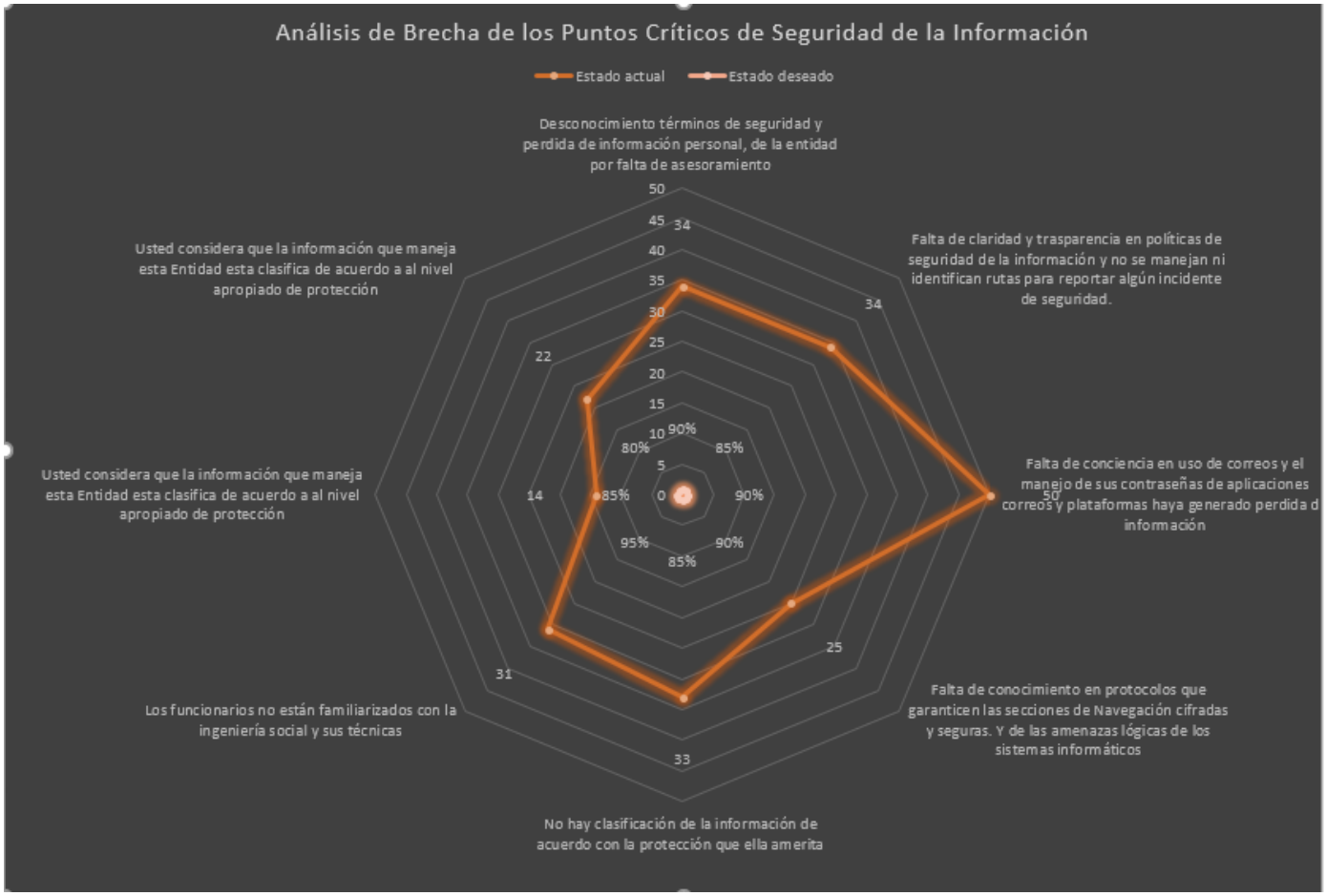
Estos puntos críticos relacionado en a la anterior tabla son de gran importancia para tener una idea mas clara a cerca de la la falta de conocimiento que los funcionarios con respecto a todo lo relacionado con Seguridad Informática y Seguridad de la información, ya que con los datos recolectados se puede determinar qué mayoría de ellos no tiene familiaridad en el manejo, en la identificación y no existe claridad en todo lo relacionado que ayude salvaguardar la información requerida; ya que

por desconocimiento y falta asesoramiento a base de los datos recogidos, se evidencia que existe las siguientes dificultades: como en el manejo términos de seguridad, en el riesgo que se corre de perder información, en la existencia de políticas de seguridad de la información, en rutas para reportar algún incidente de seguridad, en dar un buen manejo a las contraseñas de aplicaciones correos y plataformas, en la clasificación de la información de acuerdo con la protección que ella amerita, en la existencia de protocolos que garanticen las secciones de Navegación cifradas, en no estar familiarizados con la ingeniería social y sus técnicas.

Se aprecia un notorio grado de desconocimiento en Seguridad Informática, Seguridad de la información e ingeniería social de los funcionarios de la Secretaria de Educación Departamental de Nariño

Vale la pena resaltar que se mira un gran el interés del personal de que se implementen tecnologías de la seguridad informática lo cual se debería considerar la implementación de ellas.

Grafica 32 Análisis de Brecha



Fuente: Autor

La grafica Nº 32, ilustra el análisis de brecha de los puntos críticos encontrados bajo el estudio de la encuesta realizada a los funcionarios de la Secretaria de Educación Departamental de Nariño, donde se evidencia según la valoración de acuerdo a la escala del 5 al 50 se corrobora que los puntos de menor conocimiento se ubican hacia centro de la gráfica y los demás puntos críticos se van ubicando hacia el exterior según al grado de conocimiento y el porcentaje que la encuesta arrojo.

Con lo anterior se puede constar, que existe desconocimiento en Seguridad Informática, Seguridad de la información e ingeniería social; donde se pretende disminuir en un 95 % de este alto índice de riesgo de seguridad, luego de ejecutar

los programas o planes de capacitación y por lo tanto poder encaminar en forma adecuada y así lograr disminuir el nivel de riesgo de seguridad que esta entidad está expuesta.

Teniendo cuenta en los anteriores análisis de los puntos críticos identificados; se procede a continuación diseñar una propuesta de plan de capacitación en seguridad de la información que permita reducir los riesgos de ataques en ingeniería social en la secretaria de educación de Nariño, cuya intención es promover elementos de seguridad de cómo protegerla y de cómo usar la de la información.

Esta última parte sobre el análisis de brecha para identificar el nivel de conocimiento en cuestión de seguridad de la información por parte del personal de la secretaria de educación de Nariño se debe profundizar, enfocándose en los puntos críticos identificados, qué puede pasar si nos son mitigados o tratados y qué pueden causar respecto a la seguridad informática en la Secretaria de Educación Departamental de Nariño.

Es importante tener en cuenta que si estos puntos críticos no son mitigados o tratados en la Secretaria de Educación Departamental de Nariño podría acarrear con pérdida valiosa de información, perdida financiera y ataques a la privacidad de la entidad, usuarios y funcionarios que por falta de conocimiento y concientización en Seguridad de la Información , a consecuencia se esté expuesto a ataques la seguridad privada o ataques a su infraestructura computacional, rompiendo la seguridad total de esta entidad

11 ESTRUCTURA PLAN DE TRABAJO DE CAPACITACIÓN Y SENSIBILIZACIÓN

Teniendo en cuenta la información recolectada en la anterior encuesta y luego de realizar el respectivo análisis se propone un programa de capacitación y sensibilización está orientado a los funcionarios de la Secretaria de Educación del Departamento de Nariño con el propósito de preparar y sensibilizar al personal de esta entidad a consecuencia de los riesgos identificados en anterioridad con respecto a las amenazas en seguridad informática e ingeniería social reflejado en la falta de conocimiento en diferentes medidas preventivas de la seguridad de la Información digital

En vista de esta necesidad se procede a estructurar un plan de capacitación y sensibilización orientado a los funcionarios de la Secretaria de Educación Departamental de Nariño para que identifiquen las amenazas que lleve a disminuir las malas prácticas de seguridad de la información que ellos custodian y que por falta de conocimiento no saben cómo protegerla y como usarla.

Consideraciones previas

Para este diseño se han tenido en cuenta los siguientes detalles relacionados así:

Esta estrategia nace dentro de las organizaciones por la necesidad de promover el conocimiento TIC en seguridad de la información, fortaleciendo a los funcionarios con este aprendizaje.

El desconocimiento generalizado de los funcionarios hace de que sean vulnerables con facilidad, propensos a ser víctimas de los delincuentes informáticos y caer en sus estrategias de o tipos de ataque

Para el diseño de plan de capacitación y sensibilización se tienen en cuenta temas relacionados a Seguridad informática, seguridad de información e Ingeniería social orientado a disminuir los incidentes en seguridad digital.

Objetivos

- Capacitar y sensibilizar a los funcionarios de la Secretaria de Educación departamental de Nariño en seguridad informática, seguridad de la información e ingeniería social y reducir el riesgo generado por el desconocimiento en las diferentes vulnerabilidades que afectan la Seguridad de la información Digital.
- Establecer lineamientos en la implementación del plan de capacitación y sensibilización que genere confianza durante la toma de decisiones frente a las amenazas de seguridad.

Alcance

El plan de capacitación está dirigido a 130 funcionarios de planta de la secretaria de educación departamental de Nariño quienes producen, administran, custodian o tienen acceso a la información y están expuestos ante los diferentes vulnerabilidades y factores de riegos relacionados a la seguridad informática.

Temas de sensibilización identificados

Teniendo en cuenta los puntos críticos del análisis de la encueta los temas que capacitación y sensibilización son los siguientes:

- ✓ Análisis de las políticas de seguridad
- ✓ Uso del correo electrónico E identificación de correos sospechosos.
- ✓ Clasificación de información para su propia protección
- ✓ Protocolos de cifrado y seguras.
- ✓ Perdida de información y sus causas

- ✓ Uso de contraseñas Seguras
- ✓ Ingeniería social y sus técnicas
- ✓ Políticas de escritorio limpio.
- ✓ Uso apropiado de internet
- ✓ Seguridad en el puesto de trabajo
- ✓ Amenazas y vulnerabilidades comunes

Consideraciones preliminares para el desarrollo de las capacitaciones.

Para la implantación de la capacitación a los funcionarios de la Secretaria de Educación Departamental de Nariño se hará campañas de sensibilización de seguridad de la información tanto como para los directivos líderes de proceso de cada Dependencia y cada uno de sus funcionarios que la conforman, teniendo como objetivo principal crear conciencia y dejando en claro, primeramente que capacitar no es gastar recursos ni gastar tiempo , que no es un costo si no una inversión, que como resultado haya personas capaces prevenir, gestionar y accionar a incidentes de seguridad y además coadyuvar a mitigar diferentes ataques que afecten la seguridad de la información, con sentido de pertenencia y compromiso a esta Entidad de Educación.

Teniendo en cuenta lo mencionado anteriormente se busca que se la persona nominadora de la Secretaria Departamental de Nariño se comprometa a financiar y realizar las gestiones pertinentes en buscar ayuda acorde a las necesidades que esta entidad necesita tomando como antecedentes los puntos críticos identificados en los hallazgos de la encuesta realizada.

Se propone que esta Entidad al establecer el compromiso considere que la Capacitación orientada a los funcionarios de esta secretaria, **sea dirigido por organizaciones, Instituciones u programas reconocidos, expertos y comprometidos en Seguridad Informática e Ingeniería Social o de lo contrario hacer solicitudes**

de capacitación a la secretaria TIC, Innovación de Gobierno Abierto de la gobernación de Nariño.

Donde como resultado después de recibir sus capacitaciones u accesorias ya de logre crear conciencia a esta nueva cultura de seguridad informática y seguridad de la información y ya se genere tranquilidad y confianza para cumplir con los objetivos misionales con altos estándares de seguridad y de calidad de un buen servicio

A continuación, se relacionan los **roles involucrados** para el desarrollo de estas capacitaciones.

Directivos:

Los niveles directivos de la Secretaria de Educación Departamental de Nariño apoyaran este plan de capacitación en seguridad de seguridad informática, seguridad de la información mediante las siguientes acciones:

- ✓ Conseguir las instalaciones y todo lo pertinente óptimas condiciones para el desarrollo de las actividades de los programas o planes de capacitación si se los requiere.
- ✓ Apoyar con el material necesario para el desarrollo del programa o plan de capacitación como: publicidad, incentivos, posters etc., si se lo requiere.
- ✓ Autorizar a sus funcionarios bajo su responsabilidad para participen en las capacitaciones en toda su vigencia.
- ✓ Fomentar la aplicación de las buenas prácticas se seguridad que divulgara en el desarrollo de la capacitación.
- ✓ Participar de acuerdo con su disponibilidad en las actividades propuestas en los diferentes planes de capacitación.
- ✓ Propiciar el cumplimiento de las recomendaciones e instrucciones en materia de seguridad de la información que se divulguen dentro del marco de capacitación en seguridad informática y en seguridad e la información.

- ✓ Autorizar el medio de divulgación de la información de acuerdo con cada procedimiento.
- ✓ Participar en la elaboración del cronograma de actividades y horarios, generando un mejor respaldo a las diferentes actividades propuestas para el desarrollo de los programas o planes de capacitación y poder garantizar un mejor un mejor cumplimiento en esta entidad.

Líderes de Proceso:

- ✓ Coordinar al interior de sus procesos la participación de los funcionarios en las actividades del plan de capacitación.
- ✓ Participar de acuerdo con su disponibilidad en las actividades propuestas en los diferentes planes de capacitación.
- ✓ Velar por que las actividades de sus procesos apliquen la recomendación en materia de seguridad informática y en seguridad e la información bajo el plan de capacitación.
- ✓ Medir la eficacia o resultados de las diferentes actividades en desarrollo de los planes de capacitación en los que participan los funcionarios de esta entidad.
- ✓ Identificar las necesidades particulares en materia de de seguridad informática y en seguridad e la información para su proceso funcionarios o la entidad.
- ✓ Participar en la elaboración del cronograma de actividades y horarios propuestos para el desarrollo de los programas o planes de capacitación

Responsables de la información

- ✓ Diseñar un plan de sensibilización en seguridad informática y seguridad e la información teniendo presente la misión y visión de la la Secretaria de Educación Departamental de Nariño.

- ✓ Identificar las necesidades prioritarias de riesgo en seguridad Informática y seguridad de la información que esta Entidad posea.
- ✓ Colaborar y participar en la implementación del programa de capacitación.
- ✓ Consolidar los resultados de las diferentes actividades en desarrollo de los planes de capitación en los que participan los funcionarios de esta entidad.
- ✓ Aplicar evoluciones del programa de capacitación e identificar oportunidades de mejora para el plan de capacitación.
- ✓ Participar en el cumplimento del cronograma de actividades y horarios propuestos para el desarrollo de los programas o planes de capacitación

Administradores de los sistemas de información.

- ✓ Participar de acuerdo con su disponibilidad y directrices de los responsables del proceso en esta Entidad, en las actividades propuestas en los diferentes planes de capacitación.
- ✓ Identificar los mecanismos que permitan implementar las recomendaciones y buenas prácticas de los planes de capacitaciones.
- ✓ Difundir de acuerdo con la disponibilidad a los funcionarios o usuarios del sistema de información la adopción e implementación de las diferentes buenas prácticas de Seguridad de la Informática y seguridad de la información.
- ✓ Evaluar en conjunto con los responsables de cada proceso los resultados de las actividades de los programas de capacitación.
- ✓ Participar en el cumplimento del cronograma de actividades actividades y horarios propuestos para el desarrollo de los programas o planes de capacitación

Funcionarios Secretaria Departamental de Nariño

- ✓ Participar en las diferentes actividades de los programas o planes de capacitación de acuerdo con la coordinación que realice el líder del cada proceso.
- ✓ Identificar e implementar en sus actividades diarias las buenas prácticas y recomendaciones del programa de capacitación.
- ✓ Evaluar la calidad, impacto y efectividad las actividades propuestas en el programa de capacitación.
- ✓ Proponer actividades y temas a tratar para el mejoramiento de futuros programas de capacitación.
- ✓ Participar en el cumplimento del cronograma de actividades y horarios propuestos para el desarrollo de los programas o planes de capacitación

Propuesta de Temáticas del Plan o Programa de Capacitación

Teniendo en cuenta los puntos críticos encontrados en la anterior encuesta se propone el desarrollo de un plan o programa de capacitación en seguridad informática e ingeniería social y seguridad de la información a los funcionarios de la Secretaria de Educación departamental de Nariño, además de los puntos críticos relacionados anteriormente se propone las siguientes temáticas en seguridad, la metodología para su aplican y desarrollo será de acuerdo a lo pactado entre el ente nominador y la institución o programa responsable de la capacitación .

- ✓ Conocimientos fundamentales en **seguridad Informática e ingeniería social y seguridad de la Información**
- ✓ Políticas organizacionales en seguridad de la información y su aplicación.
- ✓ Procedimientos principales de seguridad de la información, como acceder a áreas seguras, clasificación y etiquetado de la información
- ✓ Diferentes tipos de amenazas y vulnerabilidades informáticas
- ✓ Ley de trasparencia y acceso a la información

- ✓ Como resolver incidentes de seguridad de la información, como reportar y que puedo reportar
- ✓ Conocimiento en las buenas prácticas de la seguridad de la información.
- ✓ Backups y recuperación de la información
- ✓ Formas comunes de ataque informático
- ✓ Protección de información en el puesto de trabajo.
- ✓ Uso de técnicas de cifrado de datos para proteger la trasmisión de información reservada y clasificada.

Población Beneficiaria

Este plan o programa de capacitación en Seguridad informática e ingeniería social y seguridad de Información serán beneficiados todo el Personal como directivos, líderes de Proceso y demás funcionarios de la Secretaria de Educación Departamental de Nariño.

Financiamiento del plan o programa de capacitación

Este plan de capacitación será financiado con recursos propios presupuestados por la Secretaria de Educación Departamental de Nariño o del contrario será financiado por la gobernación de Nariño.

Planificación de la capacitación

Las capacitaciones se realizarán cada año y se tendrá en cuenta los tiempos necesarios para la implementación de cada temática de Seguridad de la Información

CONCLUSIONES

Con el desarrollo de la presente monografía se logro:

Se realizo un estudio sobre la Ingeniería Social y su desarrollo en la actualidad donde se logró identificar las metodologías y tipos de ataques con el fin de dar a conocer al personal la forma o temas de presentación el fin de tener información confidencial accesos o privilegios en los sistemas de información perjudicando y exponiendo a un organismo u entidad en este caso como es la secretaria de Educación departamental de Nariño.

Con los los datos recolectados de encueta realizada se obtuvo información clave para lograr identificar que esta entidad los funcionarios no tienen pleno conocimiento Seguridad Informática Seguridad de la Información e ingeniera social; según el análisis de las gráficas reflejan altos índices de riesgo por falta de manejo o conocimiento en estos temas en relación donde requieren gran importancia por ser una de las medidas que ayuden para garantizar menos riesgos en perdida o manipulación de la información preservando siempre la privacidad y minimizar la vulnerabilidad de los sistemas, redes o proceso que se maneja en esta entidad.

Al Implementar el análisis de brecha sobre el conocimiento de seguridad de la información a los funcionarios de la Secretaria de Educación del Departamento Nariño se logró identificar la situación actual y puntos críticos de gran relevancia correspondientes al desconocimiento en seguridad Informática e ingeniería social colocando en riesgo los activos información más importantes de esta Entidad.

Acorde a los resultados del análisis de brecha se propone un plan de capacitación y sensibilización dirigido a los funcionarios de esta Entidad teniendo en cuenta que

no existen planes ni programas de capacitación que acrediten el uso y buen manejo de la información física y digital que esta maneja por lo tanto es de vital importancia estructurar estos planes acordes a cada necesidad que quedó reflejada en el análisis de la anterior encuesta y de acuerdo a los hallazgos encontrados y tratar de mitigar de una u otra manera esta y salvaguardar la información requerida.

RECOMENDACIONES

Recomendaciones generales a La Secretaria de Educación Departamental de Nariño.

Es importante que esta Entidad diseñe y aporte un manual de Políticas de seguridad y privacidad de la información y pueda ser implementado a cada una de las Dependencias que la conforman para que resguarde, proteja, garantice y mantenga la integridad, disponibilidad, privacidad de la información.

Se recomienda de manera inmediata la concientización y compromiso de los altos directivos en temas de seguridad de la información y seguridad informática para que implementen controles de seguridad que permitan mitigar cada una de las vulnerabilidades encontradas en el análisis de esta encuesta ya que de una u otra manera se involucra a todos los funcionarios de esta entidad por falta de conocimiento

Tomando en consideración lo anterior es de vital importancia buscar diferentes planes de capacitación, sensibilización y comunicación de la seguridad Informática y seguridad de la información para los funcionarios de la Secretaria de Educación Departamental de Nariño definiendo temas y metodologías para que ayuden a solventar los hallazgos de la encuesta, donde después de llevar a cabo el plan de capacitación la entidad realice periódicamente para una mejor efectividad.

Tener en cuenta que existen diferentes instituciones y programas que capacitan en Seguridad Informática e Ingeniería Social donde cada una ofrece sus planes, estrategias de capacitación, sensibilización adaptándose y solventando a cada necesidad de una organización o entidad, también se recomienda tener en cuenta organizaciones, Instituciones u programas reconocidos, expertos y comprometidos en Se-

guridad Informática e Ingeniería Social o de lo contrario hacer solicitudes de capacitación a la secretaria TIC, Innovación de Gobierno Abierto de la gobernación de Nariño para la capacitación

Se establecieron estrategias desarrolladas por instituciones relacionadas con capacitación que permite orientar que existen organizaciones, instituciones, programas que capacitan y establecen lineamientos que ofrecen varios canales de comunicación donde aplican herramientas poniendo en práctica mayor control frete a la seguridad de datos importantes de una entidad de tal manera protege de riesgos y fortalecer todos los procesos que afecten los activos importantes de información.

BIBLIOGRAFÍA

1. ACOSTA, P. S. (2018). INGENIERÍA SOCIAL EN INSTITUCIONES DE EDUCACIÓN SUPERIOR. *Revista Colombiana de Tecnologías de Avanzada, Vol. 2 N 32*, 10.
2. Americanos, O. d. (s.f.). *Buenas Prácticas para establecer un CSIRT nacional* . Obtenido de ites.oas.org/cyber/Documents/2016%20-%20Buenas%20Practicas%20CSIRT.pdf
3. Arenosa, L. A. (2008). Sobre virus y antivirus... Enfermería Dermatológica, 2(4), 38-41. recuperado de: https://dialnet.unirioja.es/descarga/articulo/4604586.pdf
4. Armas Montesino, L. (2003). Análisis comparativo de los principales sistemas antivirus. Acimed, 11(5), 0-0. Recuperado de. http://scielo.sld.cu/scielo.php?pid=S1024-94352003000500005&script=sci_arttext&tlng=en
5. Baca, Urbina, Gabriel. Introducción a la seguridad informática, Grupo Editorial Patria, 2016. disponible http://ebookcentral.proquest.com/lib/unadsp/detail.action?docID=4849850.
6. Bello Hernández, R. O., & Alfonso Sánchez, I. R. (2003). Elementos teórico-prácticos útiles para conocer los virus informáticos. Acimed, 11(5), 0-0. Recuperado de: http://scielo.sld.cu/scielo.php?pid=S1024-94352003000500004&script=sci_arttext&tlng=pt
7. BENCHIMIL.Daniel. (s.f.). Conozca sus vulnerabilidades y proteja su información. *HACKING DESDE CERO*, 192.
8. Canes Fauces, D. M., Pérez Infante, Y., & Callis Fernández, S. (2011). Acerca de los virus informáticos: una amenaza persistente. Medisan, 15(2), 257-260. Recuperado de: http://scielo.sld.cu/scielo.php?pid=S1029-30192011000200018&script=sci_arttext&tlng=pt

9. Cecilia, M. P. (2013). Revista de Ingeniarías. USBMed, Vol.4, N.º 2, Julio-diciembre, 65.

10. César, V. L. (s.f.). CONCIENCIACIÓN EN SEGURIDAD DE LA INFORMACIÓN. *Universidad Piloto de Colombia*, 10.

11. Chicano, Tejada, Ester. Gestión de incidentes de seguridad informática (MF0488_3), IC Editorial, 2014. Disponible en http://ebookcentral.proquest.com/lib/unadsp/detail.action?docID=4184054.

12. COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 1273. (5, enero, 2009). Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado “de la protección de la información y de los datos”- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones. Diario Oficial. Bogotá, D.C.: 2009. no. 47.223. 2 p.

13. COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 1341. (29, Julio, 2009). "Por la cual se definen Principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones -TIC-, se crea la Agencia Nacional del Espectro y se dictan otras disposiciones".

14. Comunicación, I. d. (s.f.). *Implantación de un SCSI en la empresa.* Obtenido de https://www.incibe.es/extfrontinteco/img/File/intecocert/sgsi/img/Guia_apoyo_SGSI.pdf

15. Costas, Santos, Jesús. Seguridad informática, RA-MA Editorial, 2014. disponible en, http://ebookcentral.proquest.com/lib/unadsp/detail.action?docID=3228430.

16. DURAN, P. L. (2013). INGENIERÍA SOCIAL: Un ataque a la confianza y al servicio en el sector financiero. Revista Digital Apuntes de Investigación l ISSN: 2248-7875, http://apuntesdeinvestigacion.bucaramanga.upb.edu.co/wp-content/uploads/2016/03/6.ESI-Luis-Eduardo-Patin%CC%83o-Dura%CC%81n.pdf.

17. DURAN, P. L. (2013). INGENIERÍA SOCIAL: Un ataque a la confianza y al servicio en el sector financiero. Revista Digital Apuntes de Investigación l ISSN: 2248-7875, http://apuntesdeinvestigacion.bucaramanga.upb.edu.co/wp-content/uploads/2016/03/6.ESI-Luis-Eduardo-Patin%CC%83o-Dura%CC%81n.pdf.
18. ESAMCIENCIA. Navia Marlon, Párraga Jorge, Molina Gustavo, Vidal José. (2014). Loor2EFECTIVIDAD Y EFICIENCIA DE LOS ANTIVIRUS GRATUITOS COMBINADOS FRENTE AL MALWARE recuperado de: http://investigacion.espam.edu.ec/index.php/Revista/article/download/108/86
19. Escrivá, Gascó, Gema, et al. Seguridad informática, Macmillan Iberia, S.A., 2013. Disponible en, http://ebookcentral.proquest.com/lib/unadsp/detail.action?docID=3217398.
20. ESET. Ilya López, 2014. 13. Ingeniería Social: los usuarios como víctimas de la falta de atención, recuperado de: https://www.welivesecurity.com/la-es/2014/05/01/ingenieria-social-los-usuarios-como-victimas-de-la-falta-de-atencion/
21. ESET. Narinder Purba. 2016. Las organizaciones deben capacitar sobre Ingeniería Social, según una especialista, recuperado de: https://www.welivesecurity.com/la-es/2016/10/05/capacitar-sobre-ingenieria-social/
22. Espectador, E. (12 de 05 de 2012). Colombia lidera el ranking de inseguridad informática en América Latina, Obtenido de https://www.elespectador.com/tecnologia/colombia-lidera-el-ranking-de-inseguridad-informatica-a-articulo-374381
23. Espinoza Bucheli, A. M., & Montoya Tapia, D. A. (2016). Diagnóstico de seguridad informática utilizando la metodología de análisis de vulnerabilidades en la red del Banco Nacional de Fomento-casa Matriz, Quito-Ecuador (Bachelor's thesis, Universidad de las Fuerzas Armadas ESPE. Carrera de Ingeniería de Sistemas e Informática.) recuperado de: http://repositorio.espe.edu.ec/handle/21000/11951
24. Ficarra, F. (2002). Los virus informáticos. Revista Latinoamericana de Comunicación CHASQUI, (78). Recuperado de: https://www.redalyc.org/pdf/160/16007810.pdf

25. García-Morales, Elisa. Gestión de documentos en la e-administración, Editorial UOC, 2013. Disponible en, http://ebookcentral.proquest.com/lib/unadsp/detail.action?docID=3214477.
26. GESTIÓN TIC, A. d. (2017). PLAN DE SENSIBILIZACIÓN, COMUNICACIÓN Y CAPACITACIÓN (PSCC). Obtenido de COMPONENTE: SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN: ospatios-nortedesantander.gov.co/Conectividad/InformesGEL/GT-D-03%20PLAN%20DE%20COMUNICACIÓN%20Y%20SENSIBILIZACION.pdf
27. GESTION.ORG. (s.f.). El impacto de la tecnología en la empresa. Obtenido de https://www.gestion.org/el-impacto-de-la-tecnologia-en-la-empresa/
28. González, G. (1989). Virus informáticos. Ra-ma. Recuperado de: http://www.academia.edu/download/40280261/Monografia_virus_informaticos.docx
29. González, J. A., Meana, H. P., & López, P. G. Gusanos informáticos. recuperado de: https://www.amc.edu.mx/revistaciencia/images/revista/66_3/PDF/Gusanos.pdf
30. Guadalupe, G. A. (07 de 10 de 2011). Impacto de las tecnologías de información en las organizaciones. Obtenido de https://www.gestiopolis.com/impacto-tecnologias-informacion-organizaciones/
31. Guadalupe, G. A. (07 de 10 de 2011). Impacto de las tecnologías de información en las organizaciones. Obtenido de https://www.gestiopolis.com/impacto-tecnologias-informacion-organizaciones/
32. Guindel, S. E. (23 de 11 de 2009). *CALIDAD Y SEGURIDAD DE LA INFORMACIÓN Y AUDITORÍA INFORMÁTICA*. Obtenido de h: ttps://e-archivo.uc3m.es/bitstream/handle/10016/8510/proyectoEsmeralda.pdf
33. GUTIÉRREZ, J. M. (02 de 2016). Ingeniera Social, elemento Humano de la seguridad, contra medias y planes de acción para fortalecer la seguridad. Obtenido de http://rd.udb.edu.sv:8080/jspui/bitstream/11715/1182/1/60909%20_tesis.pdf

34. GUTIÉRREZ, J. M. (02 de 2016). Ingeniería Social, El elemento Humano de la seguridad; contramedida y planes de la acción para y planes de Acción para fortalecer la seguridad. Obtenido de http://rd.udb.edu.sv:8080/jspui/bitstream/11715/1182/1/60909%20_tesis.pdf
35. Hernández, Pérez, Flor Ángel, and Zaldívar, Pedro M Ricardo. Glosario de Términos Informáticos, edited by Flores, Miguel (ed.) Sosa, El Cid Editor, 2006. Disponible en, http://ebookcentral.proquest.com/lib/unadsp/detail.action?docID=3167493.
36. HUERTA, D. (2010). Ingeniería Social. *Revista de Derecho Informático*, 43.
37. INCIBE. (12 de 05 de 2014). La ingeniería social en la empresa: aprovechando la naturaleza humana. Obtenido de https://www.incibe.es/protege-tu-empresa/blog/ingenieria-social-en-empresas
38. INCIBE. (12 de 05 de 2014). La ingeniería social en la empresa: aprovechando la naturaleza humana. Obtenido de https://www.incibe.es/protege-tu-empresa/blog/ingenieria-social-en-empresas
39. INCIBE. (12 de 05 de 2014). *La ingeniería Social en una empresa: aprovechando la naturaleza humana*. Obtenido de https://www.incibe.es/protege-tu-empresa/blog/ingenieria-social-en-empresas
40. *Ingeniería social: los 8 métodos más comunes*. Obtenido de https://www.taringa.net/+ebooks_tutoriales/ingenieria-social-los-8-metodos-mas-comunes_16hh9w
41. JARAMILLO, L. C. (s.f.). La Ingeniería Social: Un desafío Investigativo. *Universidad eafiat N 104*, 94.
42. JIMÉNEZ, R. M. (04 de 06 de 2019). Estudio de metodologías de Ingeniería Social. Obtenido de http://openaccess.uoc.edu/webapps/o2/bitstream/10609/81271/6/rmarinjTFM0618memoria.pdf

43. JIMÉNEZ, R. M. (04 de 06 de 2019). Estudio de metodologías de Ingeniería Social. Obtenido de http://openaccess.uoc.edu/webapps/o2/bitstream/10609/81271/6/rmarinjTFM0618memoria.pdf
44. Lic., B. C. (2006). Capacitación y Concientización de Seguridad en Organizaciones. Segun.Info.
45. Línea, G. e. (s.f.). CENTRO DE INFORMACIÓN Y RESPUESTA TÉCNICA A INCIDENTES DE SEGURIDAD INFORMÁTICA DE COLOMBIA. Obtenido de http://programa.gobiernoenlinea.gov.co/apc-aa-files/5854534aee4eee4102f0bd5ca294791f/CIRTISI_COLOMBIA_aprobado_24_de_mayo_de_2007_2.pdf
46. MALDONADO, G. F. (s.f.). La pedagogía como ingeniería social, Revista Educación y pedagogía 14y 15. 335. Obtenido de http://aprendeenlinea.udea.edu.co/revistas/index.php/revistaeyp/article/viewFile/5594/5016
47. MALDONADO, G. F. (s.f.). La pedagogía como ingeniería social, Revista Educación y pedagogía 14y 15. 335. Obtenido de http://aprendeenlinea.udea.edu.co/revistas/index.php/revistaeyp/article/viewFile/5594/5016
48. MEJÍA, A. (2016). Buenas prácticas de seguridad informática en microempresas colombianas. CÍES-ISSN 22116-0167Volumen 7 Numero 1.
49. Mieres, J. (2009). Ataques informáticos. Debilidades de seguridad comúnmente explotadas). Recuperado http://proton. ucting. udg. mx/tutorial/hackers/hacking. pdf.
50. Ministerio de Tecnologías de la Información y las Comunicaciones. SEGURIDAD Y PRIVACIDAD DE LA COMUNICACIÓN [en línea], 29 de julio de 2016 [revisado 15 de mayo de 2019]. Disponible en internet: https://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf
51. NIC, b. (2016). INTERNET SEGURO. Centro de Estudios, Resposta e Tratamiento de Incidentes de Segurança no Brasil.

52. NIÑO, F. (21 de febrero de 2019). Fraude a través de la ingeniería social: el desafío es la prevención. Obtenido de https://www.ambitojuridico.com/noticias/analisis/financiero-cambiario-y-seguros/fraude-traves-de-la-ingenieria-social-el-desafio
53. ORELLA Pazmiño, J. b. (2012). “Propuesta de Best Práctica para el análisis de vulnerabilidades, métodos de protección aplicados a la infraestructura de red del laboratorio de Sistemas”. Obtenido de Previa a la obtención de título de Ingenieros en electrónica, telecomunicaciones y Redes: http://dspace.espoch.edu.ec/bitstream/123456789/1943/1/98T00013.pdf
54. orres Diaz, O. A. (2017). *DISEÑO E IMPLEMENTACIÓN DE UN PLAN DE CONCIENTIZACIÓN FRENTE A LA INGENIERÍA SOCIAL PARA LA EMPRESA PROMOCIONES Y COBRANZAS BETA S.A.* Obtenido de Trabajo de Grado de la Universidad Piloto de Colombia.
55. PabloYglesias. (s.f.). *#Mundo Hacker: Los 6 principios básicos de la ingeniería social*. Obtenido de https://www.pabloyglesias.com/mundohacker-ingenieria-social/
56. Pandasecurity.com. (15 de 09 de 2015). Técnicas de ingeniería social: ¿cuáles son y cómo evitarlas en las empresas? Obtenido de https://www.pandasecurity.com/spain/mediacenter/seguridad/ingenieria-social-empresas/
57. Pandasecurity.com. (15 de 09 de 2015). Técnicas de ingeniería social: ¿cuáles son y cómo evitarlas en las empresas? Obtenido de https://www.pandasecurity.com/spain/mediacenter/seguridad/ingenieria-social-empresas/
58. PATIÑO D, L. E. (2013). INGENIERÍA SOCIAL: Un ataque a la confianza y al servicio en el sector financiero. *Revista Digital Apuntes de Investigación Vol. 7*, 31.
59. Presidencia, M. d. (2017). Guía de Seguridad de las TIC CCN-STIC 804. *Centro Criptológico Nacional,* 100.

60. publicas, M. d. (2012). 126GUÍA/NORMA DE SEGURIDAD DE LAS TIC (CCN-STIC-807). *CRIPTOLOGÍA DE EMPLEO EN EL ESQUEMA NACIONAL DE SEGURIDAD*, 119.
61. PURBA, N. (5 de octubre de 2016). Las organizaciones deben capacitar sobre Ingeniería Social, según una especialista. Obtenido de https://www.welivesecurity.com/la-es/2016/10/05/capacitar-sobre-ingenieria-social/
62. R., A. J. (2011). Seguridad Informática en Colombia Tendencias. Obtenido de http://52.0.140.184/typo43/fileadmin/Revista_119/Investigacion.pdf
63. RAMOS, D. (18 de 07 de 2017). *Fraude al CEO: ingeniería social al servicio del cibercrimen*. Obtenido de https://www.silicon.es/a-fondo-fraude-ceo-ingenieria-social-cibercrimen-2346572
64. Rascagneres, P. (2016). Seguridad informática y Malwares. Recuperado de: https://www.ediciones-eni.com/libros/webs-referencia-das/.8014f35ecd618ffce2bb7c79f7bfe1d5.PDF
65. RedUSERS. (04 de diciembre de 2015). Ingeniería Social y cuáles son sus tipos de ataque. Obtenido de http://www.redusers.com/noticias/ingenieria-social-cuales-son-los-tipos-de-ataque/
66. Revisión de las políticas de seguridad informática de la Facultad de Ingeniería. (2017). 16. Obtenido de http://www.ptolomeo.unam.mx:8080/xmlui/bitstream/handle/132.248.52.100/177/A8.pdf?sequence=8
67. Roa, Buendía, José Fabián. Seguridad informática, McGraw-Hill España, 2013. disponible en, http://ebookcentral.proquest.com/lib/unadsp/detail.action?docID=3211239.
68. RURAL, M. D. (21 de marzo de 2017). Plan de Sensibilización de seguridad de la Información Obtenido de https://www.minagricultura.gov.co/Furag2017/Evidencias/Pregunta%20144/I/PLAN%20DE%20SENSIBILIZACI%C3%93N_2017.pdf

69. SALAZAR, C. (11 de marzo de 2015). Lecciones de Ingeniería Social en una escuela par Hackers, periódico La Nación.
70. SANDOVAL, C. E. (2002). Ingeniera Social corrompiendo a la mente Humana. Revista Seguridad 1251478,1251477, Revista Bimestral.
71. SANDOVAL, C. E. (2002). Ingeniería Social: corrompiendo mente Humana. Revista Seguridad 1251478,1251477, Revista Bimestral.
72. Security, C. (2 de 08 de 2016). *DIVERSAS METODOLOGÍAS Y TIPOS DE ATAQUES DE INGENIERÍA SOCIAL*. Obtenido de https://iicybersecurity.wordpress.com/2016/09/02/diversas-metodologias-y-tipos-de-ataques-de-ingenieria-social/
73. SEGURIDAD. Gómez, Vieites, Álvaro. Auditoría de seguridad informática, RA-MA Editorial, 2014. Disponible en , http://ebookcentral.proquest.com/lib/unadsp/detail.action?docID=3229127.
74. Sena, L., & Tenzer, S. M. (2004). Introducción al riesgo Informático. Facultad de Ciencias Económicas y de Administración. Universidad de la República de Montevideo, Uruguay, 16-17.
75. SIETE24seguridad y tecnología. SEGURIDAD EN INGENIERÍA SOCIAL [en línea], 25 de abril 2003 [revisado 15 de mayo de 2019]. Disponible en internet: https://blog.siete24.com/ingenieria-social-importancia-contar-personal-seguridad-capacitado
76. SOCIAL, C. N. (22 de 01 de 2016). POLÍTICA NACIONAL DE SEGURIDAD DIGITAL. Obtenido de https://www.mintic.gov.co/portal/604/articles-14481_recurso_1.pdf
77. SOUZA, A. (s.f.). May Ingeniería social y los impactos en el medio corporativo. Obtenido de https://ostec.blog/es/generico/ingenieria-social-impactos
78. SOUZA, A. (s.f.). May Ingeniería social y los impactos en el medio corporativo. Obtenido de https://ostec.blog/es/generico/ingenieria-social-impactos

79. Tecno XXI, T., (08 de 05 de 2017). *Capacitación en Seguridad de la Información*. Obtenido de https://www.tecnoxxi.com/blog/negocios/capacitacion-en-seguridad-de-la-informacion/
80. TIC, M. (s.f.). *En TIC Confio*. Obtenido de https://www.enticconfio.gov.co/ tutoriales, E. (06 de 06 de 2018).
81. tutoriales, E. (06 de 06 de 2018). *Ingeniería social: los 8 métodos más comunes*. Obtenido de https://www.taringa.net/+ebooks_tutoriales/ingenieria-social-los-8-metodos-mas-comunes_16hh9w
82. Universidad Tecnológica de Pereira. (2011). Quinto Angelica, Restrepo Arley. Los antivirus y sus tendencias futuras, RECUPERADO DE. http://repositorio.utp.edu.co/dspace/bitstream/11059/2513/1/0058M
83. VELÁZQUEZ, K. (1 de febrero de 2018). Por qué la ingeniería social podría afectar tu esquema de seguridad cibernética. Obtenido de https://marketing4ecommerce.mx/por-que-la-ingenieria-social-podria-afectar-tu-esquema-de-seguridad-cibernetica/
84. VIZCAINO, R. J. (2014). Ingeniería Social. La práctica de obtener información confidencial. *Revista Síntesis Semilleros de Investigación*, 54-57

Anexo A Formato RAE

Fecha de Realización: 3/03/2020
Título: ANÁLISIS DEL RIESGO DE ATAQUES DE INGENIERÍA SOCIAL EN LA SECRETARIA DE EDUCACIÓN DEL DEPARTAMENTO DE NARIÑO, PARA LA IDENTIFICACIÓN DE NECESIDADES DE FORMACIÓN DEL PERSONAL Y ASÍ REDUCIR SU IMPACTO
Autor: GÓMEZ URBANO, MARLODY REGINA
Palabras Claves: Seguridad Informática, Seguridad de la Información e Ingeniería Social.
Descripción: Se realiza esta monografía con el principal objetivo de realizar un análisis de Seguridad Informática e ingeniería social en La Secretaria de Educación Departamental de Nariño; con el propósito de saber el grado de conocimiento en Seguridad Informática, para llevar a cabo este propósito se indagara a los funcionarios de esta entidad para evaluar el nivel de conocimiento, después de culminar esta labor investigativa y observando las debilidades encontradas se pretende que la Secretaria de Educación Departamental de Nariño busque implementar estrategias de protección y de la información y se concienticen en la importancia la formación y la capacitación en debilidades y los diferentes temas vulnerables encontrados.
Fuentes: Fuentes bibliográficas 1. ACOSTA, P. S. (2018). INGENIERÍA SOCIAL EN INSTITUCIONES DE EDUCACIÓN SUPERIOR. *Revista Colombiana de Tecnologías de Avanzada, Vol. 2 N 32*, 10. 2. Americanos, O. d. (s.f.). *Buenas Prácticas para establecer un CSIRT nacional* . Obtenido de ites.oas.org/cyber/Documents/2016%20-%20Buenas%20Practicas%20CSIRT.pdf

3. Arenosa, L. A. (2008). Sobre virus y antivirus... Enfermería Dermatológica, 2(4), 38-41. recuperado de: https://dialnet.unirioja.es/descarga/articulo/4604586.pdf
4. Armas Montesino, L. (2003). Análisis comparativo de los principales sistemas antivirus. Acimed, 11(5), 0-0. Recuperado de. http://scielo.sld.cu/scielo.php?pid=S1024-94352003000500005&script=sci_arttext&tlng=en
5. Baca, Urbina, Gabriel. Introducción a la seguridad informática, Grupo Editorial Patria, 2016. disponible http://ebookcentral.proquest.com/lib/unadsp/detail.action?docID=4849850.
6. Bello Hernández, R. O., & Alfonso Sánchez, I. R. (2003). Elementos teórico-prácticos útiles para conocer los virus informáticos. Acimed, 11(5), 0-0. Recuperado de: http://scielo.sld.cu/scielo.php?pid=S1024-94352003000500004&script=sci_arttext&tlng=pt
7. BENCHIMIL.Daniel. (s.f.). Conozca sus vulnerabilidades y proteja su información. *HACKING DESDE CERO*, 192.
8. Canes Fauces, D. M., Pérez Infante, Y., & Callis Fernández, S. (2011). Acerca de los virus informáticos: una amenaza persistente. Medisan, 15(2), 257-260. Recuperado de: http://scielo.sld.cu/scielo.php?pid=S1029-30192011000200018&script=sci_arttext&tlng=pt
9. Cecilia, M. P. (2013). Revista de Ingeniarías. USBMed, Vol.4, N.º 2, Julio-diciembre, 65.
10. César, V. L. (s.f.). CONCIENCIACIÓN EN SEGURIDAD DE LA INFORMACIÓN. *Universidad Piloto de Colombia*, 10.
11. Chicano, Tejada, Ester. Gestión de incidentes de seguridad informática (MF0488_3), IC Editorial, 2014. Disponible en http://ebookcentral.proquest.com/lib/unadsp/detail.action?docID=4184054.

12. COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 1273. (5, enero, 2009). Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado “de la protección de la información y de los datos”- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones. Diario Oficial. Bogotá, D.C.: 2009. no. 47.223. 2 p.
13. COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 1341. (29, Julio, 2009). "Por la cual se definen Principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones -TIC-, se crea la Agencia Nacional del Espectro y se dictan otras disposiciones".
14. Comunicación, I. d. (s.f.). *Implantación de un SCSI en la empresa.* Obtenido de https://www.incibe.es/extfrontinteco/img/File/inteco-cert/sgsi/img/Guia_apoyo_SGSI.pdf
15. Costas, Santos, Jesús. Seguridad informática, RA-MA Editorial, 2014. disponible en, http://ebookcentral.proquest.com/lib/unadsp/detail.action?docID=3228430.
16. DURAN, P. L. (2013). INGENIERÍA SOCIAL: Un ataque a la confianza y al servicio en el sector financiero. Revista Digital Apuntes de Investigación l ISSN: 2248-7875, http://apuntesdeinvestigacion.bucaramanga.upb.edu.co/wp-content/uploads/2016/03/6.ESI-Luis-Eduardo-Patin%CC%83o-Dura%CC%81n.pdf.
17. DURAN, P. L. (2013). INGENIERÍA SOCIAL: Un ataque a la confianza y al servicio en el sector financiero. Revista Digital Apuntes de Investigación l ISSN: 2248-7875, http://apuntesdeinvestigacion.bucaramanga.upb.edu.co/wp-content/uploads/2016/03/6.ESI-Luis-Eduardo-Patin%CC%83o-Dura%CC%81n.pdf.
18. ESAMCIENCIA. Navia Marlon, Párraga Jorge, Molina Gustavo, Vidal José. (2014). Loor2EFECTIVIDAD Y EFICIENCIA DE LOS ANTIVIRUS

GRATUITOS COMBINADOS FRENTE AL MALWARE recuperado de: http://investigacion.espam.edu.ec/index.php/Revista/article/download/108/86

19. Escrivá, Gascó, Gema, et al. Seguridad informática, Macmillan Iberia, S.A., 2013. Disponible en, http://ebookcentral.proquest.com/lib/unadsp/detail.action?docID=3217398.
20. ESET. Ilya López, 2014. 13. Ingeniería Social: los usuarios como víctimas de la falta de atención, recuperado de: https://www.welivesecurity.com/la-es/2014/05/01/ingenieria-social-los-usuarios-como-victimas-de-la-falta-de-atencion/
21. ESET. Narinder Purba. 2016. Las organizaciones deben capacitar sobre Ingeniería Social, según una especialista, recuperado de: https://www.welivesecurity.com/la-es/2016/10/05/capacitar-sobre-ingenieria-social/
22. Espectador, E. (12 de 05 de 2012). Colombia lidera el ranking de inseguridad informática en América Latina, Obtenido de https://www.elespectador.com/tecnologia/colombia-lidera-el-ranking-de-inseguridad-informatica-a-articulo-374381
23. Espinoza Bucheli, A. M., & Montoya Tapia, D. A. (2016). Diagnóstico de seguridad informática utilizando la metodología de análisis de vulnerabilidades en la red del Banco Nacional de Fomento-casa Matriz, Quito-Ecuador (Bachelor's thesis, Universidad de las Fuerzas Armadas ESPE. Carrera de Ingeniería de Sistemas e Informática.) recuperado de: http://repositorio.espe.edu.ec/handle/21000/11951
24. Ficarra, F. (2002). Los virus informáticos. Revista Latinoamericana de Comunicación CHASQUI, (78). Recuperado de: https://www.redalyc.org/pdf/160/16007810.pdf

25. García-Morales, Elisa. Gestión de documentos en la e-administración, Editorial UOC, 2013. Disponible en, http://ebookcentral.proquest.com/lib/unadsp/detail.action?docID=3214477.
26. GESTIÓN TIC, A. d. (2017). PLAN DE SENSIBILIZACIÓN, COMUNICACIÓN Y CAPACITACIÓN (PSCC). Obtenido de COMPONENTE: SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN: ospatios-nortedesantander.gov.co/Conectividad/InformesGEL/GT-D-03%20PLAN%20DE%20COMUNICACIÓN%20Y%20SENSIBILIZACION.pdf
27. GESTION.ORG. (s.f.). El impacto de la tecnología en la empresa. Obtenido de https://www.gestion.org/el-impacto-de-la-tecnologia-en-la-empresa/
28. González, G. (1989). Virus informáticos. Ra-ma. Recuperado de: http://www.academia.edu/download/40280261/Monografia_virus_informaticos.docx
29. González, J. A., Meana, H. P., & López, P. G. Gusanos informáticos. recuperado de: https://www.amc.edu.mx/revistaciencia/images/revista/66_3/PDF/Gusanos.pdf
30. Guadalupe, G. A. (07 de 10 de 2011). Impacto de las tecnologías de información en las organizaciones. Obtenido de https://www.gestiopolis.com/impacto-tecnologias-informacion-organizaciones/
31. Guadalupe, G. A. (07 de 10 de 2011). Impacto de las tecnologías de información en las organizaciones. Obtenido de https://www.gestiopolis.com/impacto-tecnologias-informacion-organizaciones/
32. Guindel, S. E. (23 de 11 de 2009). *CALIDAD Y SEGURIDAD DE LA INFORMACIÓN Y AUDITORÍA INFORMÁTICA*. Obtenido de h: ttps://e-archivo.uc3m.es/bitstream/handle/10016/8510/proyectoEsmeralda.pdf

33. GUTIÉRREZ, J. M. (02 de 2016). Ingeniera Social, elemento Humano de la seguridad, contra medias y planes de acción para fortalecer la seguridad. Obtenido de http://rd.udb.edu.sv:8080/jspui/bitstream/11715/1182/1/60909%20_tesis.pdf
34. GUTIÉRREZ, J. M. (02 de 2016). Ingeniería Social, El elemento Humano de la seguridad; contramedida y planes de la acción para y planes de Acción para fortalecer la seguridad. Obtenido de http://rd.udb.edu.sv:8080/jspui/bitstream/11715/1182/1/60909%20_tesis.pdf
35. Hernández, Pérez, Flor Ángel, and Zaldívar, Pedro M Ricardo. Glosario de Términos Informáticos, edited by Flores, Miguel (ed.) Sosa, El Cid Editor, 2006. Disponible en, http://ebookcentral.proquest.com/lib/unadsp/detail.action?docID=3167493.
36. HUERTA, D. (2010). Ingeniería Social. *Revista de Derecho Informático*, 43.
37. INCIBE. (12 de 05 de 2014). La ingeniería social en la empresa: aprovechando la naturaleza humana. Obtenido de https://www.incibe.es/protege-tu-empresa/blog/ingenieria-social-en-empresas
38. INCIBE. (12 de 05 de 2014). La ingeniería social en la empresa: aprovechando la naturaleza humana. Obtenido de https://www.incibe.es/protege-tu-empresa/blog/ingenieria-social-en-empresas
39. INCIBE. (12 de 05 de 2014). *La ingeniería Social en una empresa: aprovechando la naturaleza humana*. Obtenido de https://www.incibe.es/protege-tu-empresa/blog/ingenieria-social-en-empresas
40. *Ingeniería social: los 8 métodos más comunes*. Obtenido de https://www.taringa.net/+ebooks_tutoriales/ingenieria-social-los-8-metodos-mas-comunes_16hh9w

41. JARAMILLO, L. C. (s.f.). La Ingeniería Social: Un desafío Investigativo. *Universidad eafiat N 104*, 94.
42. JIMÉNEZ, R. M. (04 de 06 de 2019). Estudio de metodologías de Ingeniería Social. Obtenido de http://openaccess.uoc.edu/webapps/o2/bitstream/10609/81271/6/rmarinjTFM0618memoria.pdf
43. JIMÉNEZ, R. M. (04 de 06 de 2019). Estudio de metodologías de Ingeniería Social. Obtenido de http://openaccess.uoc.edu/webapps/o2/bitstream/10609/81271/6/rmarinjTFM0618memoria.pdf
44. Lic., B. C. (2006). Capacitación y Concientización de Seguridad en Organizaciones. Segun.Info.
45. Línea, G. e. (s.f.). CENTRO DE INFORMACIÓN Y RESPUESTA TÉCNICA A INCIDENTES DE SEGURIDAD INFORMÁTICA DE COLOMBIA. Obtenido de http://programa.gobiernoenlinea.gov.co/apc-aa-files/5854534aee4eee4102f0bd5ca294791f/CIRTISI_COLOMBIA_aprobado_24_de_mayo_de_2007_2.pdf
46. MALDONADO, G. F. (s.f.). La pedagogía como ingeniería social, Revista Educación y pedagogía 14y 15. 335. Obtenido de http://aprendeenlinea.udea.edu.co/revistas/index.php/revistaeyp/article/viewFile/5594/5016
47. MALDONADO, G. F. (s.f.). La pedagogía como ingeniería social, Revista Educación y pedagogía 14y 15. 335. Obtenido de http://aprendeenlinea.udea.edu.co/revistas/index.php/revistaeyp/article/viewFile/5594/5016
48. MEJÍA, A. (2016). Buenas prácticas de seguridad informática en microempresas colombianas. CÍES-ISSN 22116-0167Volumen 7 Numero 1.
49. Mieres, J. (2009). Ataques informáticos. Debilidades de seguridad comúnmente explotadas). Recuperado http://proton. ucting. udg. mx/tutorial/hackers/hacking. pdf.

50. Ministerio de Tecnologías de la Información y las Comunicaciones. SEGURIDAD Y PRIVACIDAD DE LA COMUNICACIÓN [en línea], 29 de julio de 2016 [revisado 15 de mayo de 2019]. Disponible en internet: https://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf
51. NIC, b. (2016). INTERNET SEGURO. Centro de Estudios, Resposta e Tratamiento de Incidentes de Segurança no Brasil.
52. NIÑO, F. (21 de febrero de 2019). Fraude a través de la ingeniería social: el desafío es la prevención. Obtenido de https://www.ambitojuridico.com/noticias/analisis/financiero-cambiario-y-seguros/fraude-traves-de-la-ingenieria-social-el-desafio
53. ORELLA Pazmiño, J. b. (2012). "Propuesta de Best Práctica para el análisis de vulnerabilidades, métodos de protección aplicados a la infraestructura de red del laboratorio de Sistemas". Obtenido de Previa a la obtención de título de Ingenieros en electrónica, telecomunicaciones y Redes: http://dspace.espoch.edu.ec/bitstream/123456789/1943/1/98T00013.pdf
54. orres Diaz, O. A. (2017). *DISEÑO E IMPLEMENTACIÓN DE UN PLAN DE CONCIENTIZACIÓN FRENTE A LA INGENIERÍA SOCIAL PARA LA EMPRESA PROMOCIONES Y COBRANZAS BETA S.A.* Obtenido de Trabajo de Grado de la Universidad Piloto de Colombia.
55. PabloYglesias. (s.f.). *#Mundo Hacker: Los 6 principios básicos de la ingeniería social*. Obtenido de https://www.pabloyglesias.com/mundohacker-ingenieria-social/
56. Pandasecurity.com. (15 de 09 de 2015). Técnicas de ingeniería social: ¿cuáles son y cómo evitarlas en las empresas? Obtenido de https://www.pandasecurity.com/spain/mediacenter/seguridad/ingenieria-social-empresas/
57. Pandasecurity.com. (15 de 09 de 2015). Técnicas de ingeniería social: ¿cuáles son y cómo evitarlas en las empresas? Obtenido de

https://www.pandasecurity.com/spain/mediacenter/seguridad/ingenieria-social-empresas/

58. PATIÑO D, L. E. (2013). INGENIERÍA SOCIAL: Un ataque a la confianza y al servicio en el sector financiero. *Revista Digital Apuntes de Investigación Vol. 7*, 31.
59. Presidencia, M. d. (2017). Guía de Seguridad de las TIC CCN-STIC 804. *Centro Criptológico Nacional,* 100.
60. publicas, M. d. (2012). 126GUÍA/NORMA DE SEGURIDAD DE LAS TIC (CCN-STIC-807). *CRIPTOLOGÍA DE EMPLEO EN EL ESQUEMA NACIONAL DE SEGURIDAD*, 119.
61. PURBA, N. (5 de octubre de 2016). Las organizaciones deben capacitar sobre Ingeniería Social, según una especialista. Obtenido de https://www.welivesecurity.com/la-es/2016/10/05/capacitar-sobre-ingenieria-social/
62. R., A. J. (2011). Seguridad Informática en Colombia Tendencias. Obtenido de http://52.0.140.184/typo43/fileadmin/Revista_119/Investigacion.pdf
63. RAMOS, D. (18 de 07 de 2017). *Fraude al CEO: ingeniería social al servicio del cibercrimen*. Obtenido de https://www.silicon.es/a-fondo-fraude-ceo-ingenieria-social-cibercrimen-2346572
64. Rascagneres, P. (2016). Seguridad informática y Malwares. Recuperado de: https://www.ediciones-eni.com/libros/webs-referenciadas/.8014f35ecd618ffce2bb7c79f7bfe1d5.PDF
65. RedUSERS. (04 de diciembre de 2015). Ingeniería Social y cuáles son sus tipos de ataque. Obtenido de http://www.redusers.com/noticias/ingenieria-social-cuales-son-los-tipos-de-ataque/
66. Revisión de las políticas de seguridad informática de la Facultad de Ingeniería. (2017). 16. Obtenido de

http://www.ptolomeo.unam.mx:8080/xmlui/bitstream/handle/132.248.52.100/177/A8.pdf?sequence=8

67. Roa, Buendía, José Fabián. Seguridad informática, McGraw-Hill España, 2013. disponible en, http://ebookcentral.proquest.com/lib/unadsp/detail.action?docID=3211239.
68. RURAL, M. D. (21 de marzo de 2017). Plan de Sensibilización de seguridad de la Información Obtenido de https://www.minagricultura.gov.co/Furag2017/Evidencias/Pregunta%20144/I/PLAN%20DE%20SENSIBILIZACI%C3%93N_2017.pdf
69. SALAZAR, C. (11 de marzo de 2015). Lecciones de Ingeniería Social en una escuela par Hackers, periódico La Nación.
70. SANDOVAL, C. E. (2002). Ingeniera Social corrompiendo a la mente Humana. Revista Seguridad 1251478,1251477, Revista Bimestral.
71. SANDOVAL, C. E. (2002). Ingeniería Social: corrompiendo mente Humana. Revista Seguridad 1251478,1251477, Revista Bimestral.
72. Security, C. (2 de 08 de 2016). *DIVERSAS METODOLOGÍAS Y TIPOS DE ATAQUES DE INGENIERÍA SOCIAL*. Obtenido de https://iicybersecurity.wordpress.com/2016/09/02/diversas-metodologias-y-tipos-de-ataques-de-ingenieria-social/
73. SEGURIDAD. Gómez, Vieites, Álvaro. Auditoría de seguridad informática, RA-MA Editorial, 2014. Disponible en , http://ebookcentral.proquest.com/lib/unadsp/detail.action?docID=3229127.
74. Sena, L., & Tenzer, S. M. (2004). Introducción al riesgo Informático. Facultad de Ciencias Económicas y de Administración. Universidad de la República de Montevideo, Uruguay, 16-17.
75. SIETE24seguridad y tecnología. SEGURIDAD EN INGENIERÍA SOCIAL [en línea], 25 de abril 2003 [revisado 15 de mayo de 2019]. Disponible en

internet: https://blog.siete24.com/ingenieria-social-importancia-contar-personal-seguridad-capacitado

76. SOCIAL, C. N. (22 de 01 de 2016). POLÍTICA NACIONAL DE SEGURIDAD DIGITAL. Obtenido de https://www.mintic.gov.co/portal/604/articles-14481_recurso_1.pdf
77. SOUZA, A. (s.f.). May Ingeniería social y los impactos en el medio corporativo. Obtenido de https://ostec.blog/es/generico/ingenieria-social-impactos
78. SOUZA, A. (s.f.). May Ingeniería social y los impactos en el medio corporativo. Obtenido de https://ostec.blog/es/generico/ingenieria-social-impactos
79. Tecno XXI, T., (08 de 05 de 2017). *Capacitación en Seguridad de la Información*. Obtenido de https://www.tecnoxxi.com/blog/negocios/capacitacion-en-seguridad-de-la-informacion/
80. TIC, M. (s.f.). *En TIC Confio*. Obtenido de https://www.enticconfio.gov.co/ tutoriales, E. (06 de 06 de 2018).
81. tutoriales, E. (06 de 06 de 2018). *Ingeniería social: los 8 métodos más comunes*. Obtenido de https://www.taringa.net/+ebooks_tutoriales/ingenieria-social-los-8-metodos-mas-comunes_16hh9w
82. Universidad Tecnológica de Pereira. (2011). Quinto Angelica, Restrepo Arley. Los antivirus y sus tendencias futuras, RECUPERADO DE. http://repositorio.utp.edu.co/dspace/bitstream/11059/2513/1/0058M
83. VELÁZQUEZ, K. (1 de febrero de 2018). Por qué la ingeniería social podría afectar tu esquema de seguridad cibernética. Obtenido de https://marketing4ecommerce.mx/por-que-la-ingenieria-social-podria-afectar-tu-esquema-de-seguridad-cibernetica/

84. VIZCAINO, R. J. (2014). Ingeniería Social. La práctica de obtener información confidencial. *Revista Síntesis Semilleros de Investigación*, 54-57

Contenido del documento:

El trabajo se encuentra documentado de la siguiente manera:

- ✓ Introducción.
- ✓ Titulo
- ✓ Definición del problema
- ✓ Planteamiento del Problema
- ✓ Justificación
- ✓ Objetivo general y especifico
- ✓ Delimitaciones
- ✓ Marco Referencial
- ✓ Marco teórico
- ✓ Marco conceptual
- ✓ Marco legal
- ✓ Estudio sobre la Ingeniería social y su desarrollo en la actualidad.
- ✓ Metodología y tipos de ataque de la Ingeniería Social
- ✓ Estrategias de estudio desarrolladas en las Instituciones relacionadas con capacitación en seguridad e Ingeniería Social
- ✓ Análisis de la situación actual de la secretaria de educación departamental de Nariño con relación a su conocimiento de seguridad informática.
- ✓ Análisis de la encuesta
- ✓ Estructura plan de trabajo de capacitación y sensibilización
- ✓ Conclusiones
- ✓ Recomendaciones

Conceptos nuevos: Gracias a la investigación realizada se logró adquirir conocimiento en temas importantes como de Metodologías, técnicas, tácticas de

la ingeniería social, las estrategias de estudio en Seguridad Informática, los cuales manejan conceptos nuevos y es de vital importancia que nos familiaricemos con ellos ya que nos ayudar a tomar decisiones importantes y evitar ser víctima de esta práctica de manipulación que a todo momento estamos expuestos.

Conclusiones:

Con el desarrollo de la presente monografía se logro:

Se realizo un estudio sobre la Ingeniería Social y su desarrollo en la actualidad donde se logró identificar las metodologías y tipos de ataques con el fin de dar a conocer al personal la forma o temas de presentación el fin de tener información confidencial accesos o privilegios en los sistemas de información perjudicando y exponiendo a un organismo u entidad en este caso como es la secretaria de Educación departamental de Nariño.

Con los los datos recolectados de encueta realizada se obtuvo información clave para lograr identificar que esta entidad los funcionarios no tienen pleno conocimiento Seguridad Informática Seguridad de la Información e ingeniera social; según el análisis de las gráficas reflejan altos índices de riesgo por falta de manejo o conocimiento en estos temas en relación donde requieren gran importancia por ser una de las medidas que ayuden para garantizar menos riesgos en perdida o manipulación de la información preservando siempre la privacidad y minimizar la vulnerabilidad de los sistemas, redes o proceso que se maneja en esta entidad.

Al Implementar el análisis de brecha sobre el conocimiento de seguridad de la información a los funcionarios de la Secretaria de Educación del Departamento Nariño se logró identificar la situación actual y puntos críticos de gran relevancia correspondientes al desconocimiento en seguridad Informática e ingeniería social colocando en riesgo los activos información más importantes de esta Entidad.

Acorde a los resultados del análisis de brecha se propone un plan de capacitación y sensibilización dirigido a los funcionarios de esta Entidad teniendo en cuenta que no existen planes ni programas de capacitación que acrediten el uso y buen manejo de la información física y digital que esta maneja por lo tanto es de vital importancia estructurar estos planes acordes a cada necesidad que quedó reflejada en el análisis de la anterior encuesta y de acuerdo a los hallazgos encontrados y tratar de mitigar de una u otra manera esta y salvaguardar la información requerida.

AUTOR: MARLODY REGINA GÓMEZ URBANO