ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Facultad de Ingeniería en Electricidad y Computación

Elaboración de artículos divulgativos sobre el estado actual y buenas prácticas de ciberseguridad en Ecuador

PROYECTO INTEGRADOR

Previo la obtención del Título de:

Ingeniero en Telemática

Presentado por:

Bryan Andrés Chunga Mindiola

Christian Andrés Ramos Mesías

GUAYAQUIL - ECUADOR

Año: 2023

DEDICATORIA

Bryan Andrés Chunga Mindiola

El presente proyecto lo dedico a mis padres, por el apoyo brindado a lo largo de toda mi formación académica y a mi familia, por el apoyo y los consejos que me ayudaron a salir adelante.

Christian Andrés Ramos Mesías

El presente proyecto lo dedico a mis padres por el apoyo incondicional brindado durante toda mi etapa universitaria y a mi familia en general también por su apoyo y comprensión.

AGRADECIMIENTOS

Bryan Andrés Chunga Mindiola

Mi más sincero agradecimiento a mi colegio, la Academia Naval Almirante Illingworth, donde nacio mi curiosidad por la informática, al Ing. Ignacio Marin, por su guia y paciencia durante la elaboración de este proyecto, a mis jefes, Jonathan Cagua y Miguel Bailon, por el apoyo y las consideraciones para que pueda terminar mis estudios, a mis amigos cercanos, que desde la escuela estuvimos el uno para el otro motivándonos mutuamente para llegar a este punto, y por ultimo nuevamente a mis padres, por el apoyo brindado.

Christian Andrés Ramos Mesías

Mi más sincero agradecimiento al Ing. Ignacio Marín, por su acompañamiento y siempre predisposición para llevar a cabo este trabajo de grado.

DECLARACIÓN EXPRESA

”Los derechos de titularidad y explotación, me(nos) corresponde conforme al reglamento de propiedad intelectual de la institución; (nombre de los participantes) y doy(damos) mi(nuestro) consentimiento para que la ESPOL realice la comunicación pública de la obra por cualquier medio con el fin de promover la consulta, difusión y uso público de la producción intelectual”

Firmado electrónicamente por:
BRYAN ANDRES CHUNGA MINDIOLA

Bryan Andrés Chunga Mindiola

Christian Andrés Ramos Mesías

EVALUADORES

Ignacio Marín García

PROFESOR DE LA MATERIA

Ignacio Marín García

PROFESOR TUTOR

RESUMEN

La acogida de las nuevas soluciones digitales presentes en el mercado ha expuesto una larga serie de vulnerabilidades, muchas de estas debido a la falta de conocimiento de las personas en cuanto a temas de seguridad digital. Ecuador no es la excepción en los últimos años se han elevado los reportes de ataques informáticos tanto a ciudadanos como a empresas públicas y privadas. El presente trabajo busca fortalecer la seguridad digital de la población ecuatoriana, mediante la presentación de una serie de artículos de carácter divulgativo sobre la ciberseguridad. Para ello se ha diferenciado al público general en tres grupos según su grado de conocimiento en seguridad informática: inicial, intermedio, avanzado. Se llevó a cabo una serie de pasos para la creación de los artículos: Análisis de literatura, conllevó toda la investigación previa para la obtención de información. Clasificación, ordenamiento de la información en función de los grupos previamente diferenciados. Elaboración de artículos. Posteriormente, mediante una encuesta, se presentó los trabajos literarios donde se obtuvo la retroalimentación respectiva. La mayor parte de encuestados estuvo de acuerdo con el contenido mostrado y afirmó haber aprendido algo sobre ciberseguridad luego de leer el artículo, aunque también les parecía extenso y se mostraron indiferentes ante las imágenes mostradas. Los artículos lograron concientizar y dar nociones básicas de ciberseguridad para proteger dispositivos e información, según la retroalimentación de las encuestas realizadas.

Palabras Clave: Ciberataque, Ciberseguridad, Informática, Internet

ABSTRACT

The reception of the new digital solutions present in the market has exposed a long series of vulnerabilities, many of these due to the lack of knowledge of people regarding digital security issues. Ecuador is no exception. In recent years, reports of computer attacks on both citizens and public and private companies have risen. The present work seeks to strengthen the digital security of the Ecuadorian population, through the presentation of a series of informative articles on cybersecurity. For this, the general public has been differentiated into three groups according to their degree of knowledge in computer security: initial, intermediate, advanced. A series of steps were carried out for the creation of the articles: Literature analysis, involved all the previous research to obtain information. Classification, ordering of information based on previously differentiated groups. Preparation of articles. Subsequently, through a survey, the literary works were presented where the respective feedback was obtained. Most of the respondents agreed with the content shown and stated that they had learned something about cybersecurity after reading the article, although they also found it extensive and were indifferent to the images shown. The articles managed to raise awareness and give basic notions of cybersecurity to protect devices and information, according to the feedback from the surveys carried out.

Keywords: Cyberattack, Cybersecurity, Computing, Internet

ÍNDICE GENERAL

ACRONIMOS

ARPA - Agencia de Proyectos de Investigación Avanzados de Defensa (del inglés: Advance Research Projects Agency)

DARPA - Agencia de Proyectos de Investigación Avanzados de Defensa (del inglés: Defense Advanced Research Projects Agency)

ARPAnet - Red de la Agencias de Proyectos de Investigación Avanzada (del inglés: Advance Research Projects Agency network)

IoT - Internet de las Cosas (del inglés: Internet of Things)

UIT - Unión Internacional de Telecomunicaciones

ARCOTEL - Agencia de Regulación y Control de las Telecomunicaciones

SUPERTEL - Superintendencia de Telecomunicaciones

NRI - Índice de Preparación de la Red (del inglés: Networked Readiness Index)

AECI - Asociación Ecuatoriana de Ciberseguridad

EGSI - Esquema Gubernamental de Seguridad de la Información

COIP - Código Orgánico Integral Penal

EcuCERT - Centro de Respuesta a Incidentes Informáticos

URL - Localizador uniforme de recursos (del inglés: Uniform Resource Locator)

ACSC - Centro Australiano de Seguridad Cibernética (del inglés: Australian Cyber Security Centre)

INCIBE - Instituto Nacional de Ciberseguridad

ÍNDICE DE FIGURAS

CAPÍTULO 1

1. INTRODUCCIÓN

El siglo XX fue una época de grandes cambios y acontecimientos para la humanidad, especialmente en el campo tecnológico. Con la aparición de las primeras computadoras, que en esa época eran grandes equipos que ocupaban inmensas habitaciones y que solo estaban disponibles para universidades, empresas y el gobierno, eran capaces de realizar operaciones básicas, aunque a un alto costo de procesamiento y energía [1]. Posteriormente, en Estados Unidos la Agencia de Proyectos para la Investigación Avanzada o ARPA, desarrollaría una red de computadoras capaces de comunicarse entre ellas, denominada ARPANET [2]. Estos dos acontecimientos, ARPAnet junto con las computadoras sentaron las bases de lo que en nuestros días conocemos como Internet, un nuevo mundo, sin fronteras y al que todos podrían acceder.

A fines del siglo XX e inicios del siglo XXI Internet empezó a tener su gran auge, para el año 2001 habían alrededor de 513 millones de usuarios en red y actualmente en 2022 existen más de 5.000 millones en línea[1], gran parte de este considerable incremento se dio principalmente por dos razones: el desarrollo de los dispositivos electrónicos y la aparición de las denominadas redes sociales: YouTube, Facebook, Twitter, y TikTok entre otras.

El desarrollo que tuvieron los dispositivos electrónicos, principalmente las computadoras y con la llegada del Internet de las cosas o IoT, casi todo dispositivo de uso cotidiano puede conectarse a internet [3]. Por otro lado, las redes sociales surgen como sitios que se caracterizan por entablar las relaciones personales y la compartición de información de todo tipo: fotos, videos, música, conocimientos, etc.[4].

[1] Informe 'Digital 2022 April Global Statshot' (https://datareportal.com)

Debido a la extensión de los dispositivos electrónicos y personas conectadas e interactuando, es importante conocer los peligros expuestos al navegar en el denominado ciberespacio.

La seguridad en las redes de datos o ciberseguridad empezó a tener un papel protagónico a medida que las actividades cotidianas se trasladaban al mundo virtual [5]. La ciberseguridad ha sido definida por la Unión Internacional de Telecomunicaciones (UIT) [2], como:

> ”El conjunto de herramientas, políticas, conceptos de seguridad, garantías de seguridad, directrices, enfoques de gestión de riesgos, acciones, capacitación, mejores prácticas, garantías y tecnologías que se pueden utilizar para proteger el entorno cibernético y los activos de la organización y del usuario. Los activos de la organización y del usuario incluyen dispositivos informáticos conectados, personal, infraestructura, aplicaciones, servicios, sistemas de telecomunicaciones y la totalidad de la información transmitida y/o almacenada en el entorno cibernético. La ciberseguridad se esfuerza por garantizar el logro y el mantenimiento de las propiedades de seguridad de la organización y los activos del usuario frente a los riesgos de seguridad relevantes en el entorno cibernético.” [6]

Puesto que el ciberespacio se caracteriza por el manejo de una amplia cantidad de información, sensible en muchos casos, es crucial que todos los usuarios quienes la usan (gubernamentales, empresariales, generales) conozcan, implementen y pongan en práctica métodos, modelos y mecanismos que hagan de Internet un lugar seguro. [7].

En el año 2012, Ecuador paso por un periodo de transformación e implementación digital, donde el uso de las nuevas tecnologías tomaba cada vez mayor acogida en el día a día de las personas. Esto se pudo evidenciar sobretodo dentro del ámbito financiero, ya que muchas instituciones bancarias comenzaron a adaptar y ofrecer servicios que aprovechaban al máximo las tecnologías surgentes de aquella época. Estos avances se pueden atribuir a las propuestas gubernamentales de la época, que fomentaban la expansión y el uso de nuevas tecnologías, así como el establecimiento de normativas para las mismas. Entre los planes lanzados en ese momento se pueden mencionar: mayor rigor en cuanto a los controles de calidad y seguridad por la antigua SUPERTEL (ahora ARCOTEL [3]); la implementación de puntos de acceso gratuitos a internet en áreas

[2] Organismo especializado en telecomunicaciones (https://www.itu.int.es/)

[3] Entidad gubernamental ecuatoriana (https://www.arcotel.gob.ec/)

públicas y la expansión de la conectividad para los sectores rurales, entre otros [8]. Todas estas medidas resultaron a que en el año 2015 Ecuador subiera nueve puestos en el NRI [9]. Sin embargo, el auge, la rápida acogida y la falta de conocimiento de la población sobre las medidas de ciberseguridad han ocasionado que también creciera la cantidad de ciberataques y fraudes. Inclusive, estos ataques no se han limitado únicamente a personas naturales, como se puede evidenciar en los reportes de ciberataques a entidades privadas, entidades financieras e inclusive entidades gubernamentales [10].

Con la llegada del SARS-CoV-2 [11] muchas de las actividades han sido forzadas a implementarse mediante soluciones tecnológicas, con el fin de salvaguardar la salud de la población limitando el contacto físico a través de la interacciones y procesos a través de la web. Si bien con esto se ha logrado una mayor acogida de las soluciones digitales, también a obligado a personas con muy pocos conocimientos en cuando a estos, a enfrentarse a ellos, exponiéndolos a los peligros de un entorno con el que no están familiarizados y dejándolos desprotegidos a la mayoría de las amenazas existentes. Durante este periodo la cantidad de ciberataques reportados a nivel global a crecido un 34%. Adicionalmente, en América Latina los ataques de pishing reportados aumentaron de un promedio de 5.000 ataques semanales a más de 200.000, siendo estos responsables del 90% de las infecciones de malware reportadas y del 72% de las filtraciones y robos de datos e información personal. Este aumento de ataques cibernéticos hizo que el promedio de ataques en América Latina creciera más del 130% durante los cuatro primeros meses de la pandemia [12].

El informe del MIMECAST23 [13] realizado por Mimecast, una empresa que se especializa en la seguridad de correo electrónico basado en nube para los servicios de Microsoft [4], reporta que durante los tres primeros meses de confinamiento la detección de bloqueos de URL peligrosas aproximadamente aumento cerca de un 55%, la detección de malwares subió un un 35%, la detección de casos de suplantación de identidad un cerca de 30% y la detección de spam o correo basura un 26%.

Finalmente, cabe recalcar que en el 2020, la Fiscalía General del Estado del Ecuador informa [12] un total de 5.048 ataques cibernéticos reportados, de los cuales cerca de un 43% corresponden a delitos de suplantación de identidad y robo de información personal. Esto deja en evidencia la poca preparación que tenía la población ecuatoriana en cuenta

[4]Microsoft, emrpesa tecnológica multinacional lider en desarrollo de software (www.microsoft.com)

a nociones de ciberseguridad y protección en el campo digital.

1.1 Objetivos del proyecto

El objetivo de este proyecto integrador es: **Transferir conocimientos en materia de ciberseguridad, mediante la presentación de artículos divulgativos, para mejorar la protección de la información de los usuarios en los sistemas informáticos en el Ecuador**.

Para ello se presentan tres objetivos específicos con los que se espera cumplir con el objetivo principal de este trabajo. :

1. Conocer el estado actual de la ciberseguridad en el Ecuador basándonos en una recopilación de información publica y trabajos científicos realizados en la materia.
2. Determinar las mejores técnicas/mecanismos para evitar los ciberataques tomando como base los conocimientos y habilidades técnicas de la población objetivo.
3. Elaborar diversos artículos divulgativos que fortalezcan la seguridad de los la población objetivo en linea minimizando sus planos de ataques de manera sencilla y acorde a los conocimientos y habilidades técnicas de dichas poblaciones.

1.2 Público Objetivo

Se divide al público general en base al conocimiento técnico de cada uno en cuanto a informática, con la finalidad de que cada grupo tenga acceso a un documento apto para su completo entendimiento. Se definieron tres grupos distintos:

- **Inicial:** En este grupo se considera el mas inexperto en temas de informática y por ende con muy bajos conocimientos en cuanto a ciberseguridad. Se toman en cuenta sobre todo a personas mayores que por lo general cuentan con vagos conocimientos en cuanto a informática y que muchas veces se ven expuestos a métodos fraudulentos o vulneraciones sobre todo al navegar por la web. Se considera también a niños de corta edad que empiezan a hacer uso de equipos informáticos como computadoras, teléfonos inteligentes u otros.
- **Intermedio:** Consiste en usuarios con un uso cotidiano de equipos informáticos, por razones de trabajo como los oficinistas o razones de estudio como un estudiante

universitario. Para este grupo se brindarán las mismas nociones y conceptos básicos del grupo inicial, añadiendo técnicas mas avanzadas que requieren de unos conocimientos técnicos mínimos

- **Avanzado:** El grupo con más conocimiento técnico en informática y temas de seguridad. Para este grupo no se considera la necesidad de informar sobre buenas practicas y nociones de ciberseguridad, pero se considera apropiado el presentar las últimas investigaciones y avances realizados en ciberseguridad, así como presentar diferentes soluciones disponibles que permitan mejorar la seguridad e integridad de la información en equipos informáticos, así como también protección a nivel de red tanto interna como externa.

1.3 Estado del arte

En México, en 2018, la asociación Fundación en Movimiento publicó una guía dirigida a padres y adultos en general para proteger y controlar a niños y adolescentes del mal uso de las tecnologías e Internet. La obra presenta una gran cantidad de información, se muestran los peligros del mundo virtual y como poder identificar, ayudar y prevenir todo tipo de acciones peligrosas o indebidas a las que están sometidos los menores en línea [14].

También, en 2020 y a raíz de la pandemia producida por el SARS-CoV-2, la Secretaría de Comunicaciones y Transporte mexicana, presentó un par de guías para fortalecer la seguridad en línea de sus ciudadanos. El primer documento enfocado en el sector laboral y apoyo al teletrabajo [15], y el segundo dirigido a adolescente en apoyo a la teleeducación [16]. A lo largo de estos documentos se detallan definiciones sobre términos del campo de la ciberseguridad, los peligros que se pueden presentar y recomendaciones para poder evitarlos.

Tanto [14] [15] [16] poseen una corta extensión. [14] con una longitud de 30 páginas y aunque posee pocas imágenes ilustrativas, el lenguaje empleado es sumamente sencillo de entender. [15] [16] cuentan con una extensión menor a 25 páginas, carecen de material visual haciendo su comprensión más difícil para quienes no tienen noción del tema, debido a que se presentan muchas veces términos técnicos del área.

En 2021, el Centro Australiano de Seguridad Cibernética, (ACSC [5])„ presentó una guía

[5]Entidad gubernamental australiana (https://www.cyber.gov.au/)

de 20 páginas orientada a la ciberseguridad para pequeñas empresas. A través del documento se abordan los temas más básicos de la seguridad en línea y acceso a la información de la empresa para los diferentes tipos de usuarios [17]. La información está en proporción con los gráficos presentados a lo largo del trabajo, además el lenguaje empleado es sencillo de comprender.

También encontramos trabajos elaborados por compañías especializadas en ciberseguridad, como elevITy[6] a través de su manual de seguridad cibernética buscan ayudar a mitigar los riesgos presentes en el ciberespacio, a la vez que presentan dos casos de empresas como ejemplo de lo que se debe y no hacer ante un ciberataque [18]. Por otro lado, CyberTalk[7] presentó su guía del comprador digital enfocada en recomendaciones a seguir por parte de las empresas antes de adquirir un servicio o recurso de TI para salvaguardar la integridad de su compañía de las amenazas cibernéticas [19]. Aunque ambos trabajos [18] [19] presentan gran información para el área informática empresarial solo pueden ser encontrados en el idioma inglés, lo que podría significar una barrera para muchos interesados.

En España, el Instituto Nacional de Ciberseguridad, (INCIBE [8]), en conjunto con el Cuerpo Nacional de Policía publicó en 2022 una guía sobre ciberseguridad dirigida principalmente a internautas mayores de 60 años. El documento aborda las nociones más básicas sobre seguridad en dispositivos e Internet y a pesar que la obra posee una amplia extensión, con 71 páginas, dónde se describen cortas definiciones, recomendaciones y procedimientos es muy didáctico su entendimiento, además de poseer una amplia colección de recursos visuales [20].

En Ecuador, las páginas oficiales del gobierno han puesto en publicación una serie de seis guías cortas acerca de ciberseguridad y uso seguro de Internet [21]. Todas las guías tratan de temas diferentes sobre ciberseguridad, no se sigue un orden de relación específico. También el reconocido diario El Universo[9] ha publicado varios artículos sobre el área de ciberseguridad, orientados principalmente en recomendaciones y estrategias que ayuden a los cibernautas a hacer un mejor uso de las herramientas tecnológicas y la información que manejan en internet [22] [23]. Además, de exponer testimonios reales mostrando lo fácil que es caer en estafas o robos por Internet [24].

[6] Proveedor de gestión de tecnología (https://www.gflesch.com/elevity)
[7] Plataforma de liderazgo intelectual a nivel ejecutivo (https://www.cybertalk.org/)
[8] Entidad gubernamental española (https://www.incibe.es/)
[9] El Universo, diario de noticias ecuatoriano (https://www.eluniverso.com/)

En el primer trimestre del 2020, la (AECI [10]) realizó un estudio en donde se determinó que la mayoría de las vulnerabilidades dentro de las diferentes instituciones del país, tanto públicas como privadas, se deben a la falta de gestión e iniciativa por el fortalecimiento en la seguridad informáticas dentro de las mismas. En el mismo año la empresa de consultoria internacional Deloitte[11] presenta los resultados de una encuesta hecha a 100 instituciones, de las cuales solo el 51% cuenta con un encargado para el área de la seguridad digital, y el 13% admite no tener un experto para el campo. [25]

Entre los años 2018 y 2021, en el Ecuador se ejecutó el Plan Nacional de Gobierno Electrónico, gracias al cual se comenzó a generar una mayor conciencia sobre temas de seguridad informática, añadiendo los delitos informáticos dentro del (COIP [12]) y fortaleciendo las sentencias penales para estos, las cuales no habían sido actualizadas desde su implementación en el año 2009. además de aumentar la seguridad informática por parte de los entes del gobierno. Entre las dos principales iniciativas desarrolladas en este periodo de tiempo está el (EGSI [13]), el cual es un marco de seguridad para las instituciones del gobierno, y el (EcuCERT [14]), dirigido por la ARCOTEL, sin embargo, estas medidas parecen no haber sido suficientes. En el año 2021, la figura 1.1, presenta un estudio del estado de la ciberseguridad en el Ecuador por la UIT, concluyendo que el país aún se encuentra en una “etapa inicial”, con campos que denotan cero niveles de desarrollo e inclusive obteniendo una puntuación aún menor al estudio realizado en el 2018 [26].

En el 2022, el gobierno del Ecuador presentó la Estrategia Nacional de Ciberseguridad del Ecuador [27], cuya visión en un lapso de tres años, como se describe en el plan de acción, es hacer del Ecuador un país competitivo dentro del área digital y con la capacidad suficiente para hacer frente a vulnerabilidades y ataques de ciberseguridad.

Ante todo lo expuesto, se evidencia que en la actualidad existe gran cantidad de trabajos sobre el área de la ciberseguridad, estas obras buscan dar a conocer, fortalecer o mejoras los conocimientos que poseen los diferentes usuarios que hacen uso de Internet; por lo que nuestro futuro trabajo estará alineado con la información ya revisada en esta sección.

[10] Organización ecuatoriana (https://aeci.org.ec/)
[11] Deloitte, empresa de consultoria (https://www2.deloitte.com/)
[12] Ley ecuatoriana (https://www.defensa.gob.ec/COIP.pdf)
[13] Norma técnica ecuatoriana (https://www.gobiernoelectronico.gob.ec/EGSI.pdf)
[14] Entidad gubernamental ecuatoriana (https://www.ecucert.gob.ec/)

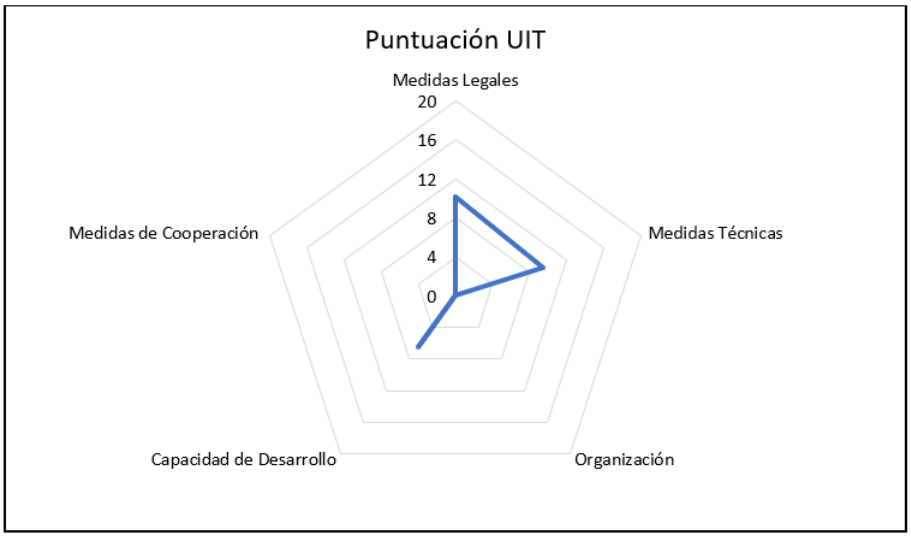


Figura 1.1: Fuente: Reporte del estado del Ecuador en Ciberseguridad, UIT

CAPÍTULO 2

2. METODOLOGÍA

En el presente proyecto se busca la redacción y posterior presentación de artículos científicos de carácter divulgativo, con el objetivo de fomentar una mejor cultura sobre seguridad informática en los lectores. Los pasos por seguir para lograrlo se basan en la recopilación de información sobre el estado actual de la ciberseguridad a nivel mundial, regional y nacional, identificar las vulnerabilidades más frecuentes y brindar soluciones o métodos de prevención prácticas que ayuden a las personas a evitarlos. Para esto, en cada artículo se presentaron temas claves a tomar en cuenta para los diferentes tipos de usuarios que se han planteado en la sección 1.2. Estos se describieron como:

- **Inicial:** Grupo de personas con bajos conocimientos de informática, en el cual nos centraremos en la elaboración de artículos enfocados a las nociones básicas de ciberseguridad, presentando las técnicas más comunes de fraude informático de las que pueden ser víctimas, consejos para salvaguardar información personal y nociones básicas para navegar en la web de manera segura.

- **Intermedio:** Grupo de usuarios con uso cotidiano de equipos informáticos, para el enfoque de los artículos estará en presentar técnicas de protección para datos o información sensible que tengan almacenada en sus equipos, y consejos para la evasión de ataques y vulnerabilidades informáticas como algunos tipos de virus.

- **Avanzado:** Grupo con conocimiento más técnico de sistemas informáticos y nociones de seguridad, para el cual se elaboraron artículos en los que se presenta los últimos avances disponibles en el área de seguridad informática y soluciones actuales para incrementar la información de la seguridad en los equipos informáticos. e

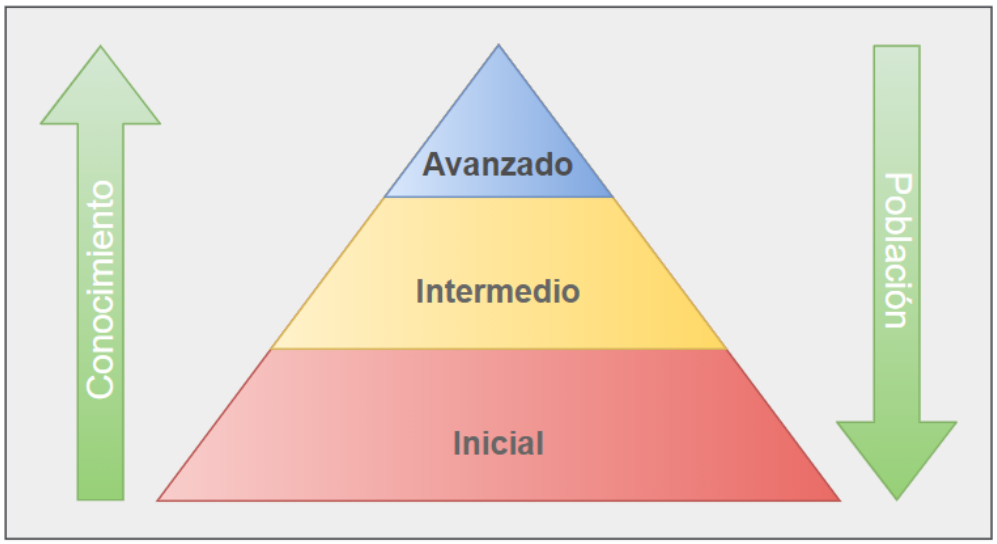


Figura 2.1: Comparación del tamaño de la población en base a su conocimiento sobre ciberseguridad

En la figura 2.1, se puede apreciar como el tamaño de la población objetivo decrece conforme aumenta su nivel de conocimiento sobre informática y ciberseguridad. El grupo con menos conocimiento es el más grande en cuanto a población, y además los mas vulnerables, por lo tanto los artículos que se elaborarán estarán mayormente orientados precisamente a este grupo, con la finalidad de disminuir la probabilidad de que sean vulneradas.

2.1 Métodos

Debido a la naturaleza misma del proyecto integrador, el método que mejor se adaptó para su desarrollado fue el de **investigación - acción**, ya que se fundamenta en el estudio de una problemática social que afecta a un determinado conjunto de personas y posterior toma de acciones respectivas, este tipo de método se caracteriza por generar de manera simultánea conocimientos y cambios sociales [28]. En el caso de este proyecto la problemática es la carencia de conocimientos sobre seguridad digital de las personas en Internet, que afecta a tres grupos de usuarios previamente diferenciados y que a través de una serie de artículos divulgativos queremos ayudar a mejorar o fortalecer los conocimientos en tema de ciberseguridad de la población objetivo.

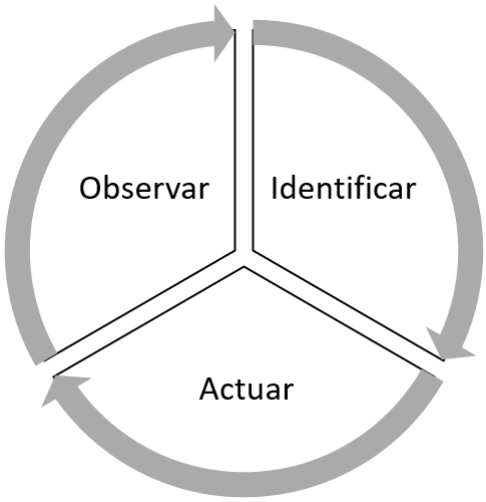


Figura 2.2: etapas del método investigación-acción

En la figura 2.2 se tiene los tres pasos realizados en la elaboración del proyecto: **observar**, esta etapa se recopila la información necesaria, en este caso a través de fuentes de información confiables en Internet, lo que permite pasar a la siguiente etapa, **identificar**, donde se comprende causas, consecuencias y en general como afecta el problema a las sociedades y por último la etapa de **actuar**, donde se proponen soluciones, la elaboración de artículos divulgativos, de manera que se cambie o mejore la situación actual de la población ante la problemática existente.

2.2 Recursos

A continuación presentamos los recursos utilizados durante el desarrollo del proyecto, los mismos han sido organizados en tres categorías según su naturaleza, y son: **recursos de software**. Son todos los programas y aplicaciones utilizadas durante el desarrollo del proyecto, donde tenemos:

- **Bases de datos científica / repositorio de periódicos:** para hallar la información necesaria de fuentes primarias y secundarias pero fiables de conocimiento, como IEEE[1] o Scopus [2] . Nos sirvieron de guía a partir de las que se basaron nuestros artículos.

- **Procesador de texto:** para la creación, redacción y edición (tamaño y tipo de letra,

[1]Base de datos científica (https://ieeexplore.ieee.org/Xplore/home.jsp)
[2]Base de datos científica (https://www.scopus.com/home.uri)

insertar imágenes, etc.) de documentos de texto. Fue nuestra principal herramienta de trabajo utilizada para la escritura de los artículos.

- **Hoja de cálculo:** para trabajar con datos de tipo numérico y realizar cálculos, estadísticas, funciones y gráficas. Toda la matemática necesaria detrás de nuestro proyecto.
- **Buscador de imágenes:** en caso de necesitar material visual que acompañe al texto, como pueden ser: imágenes, viñetas, láminas, logos. Con el fin de mejorar la comprensión del documento.

Otro de los recursos utilizados en este son los **recursos de hardware**. Estos son todos los equipos y dispositivos físicos usados en la elaboración del proyecto. En este se usó una **computadora** que brindó el acceso a Internet asi como los recursos de software descritos anteriormente.

El último tipo de recurso utilizado en este , y quizás más importante fueron los **recursos humanos**. Esos incluían todo el personal humano involucrado en el desarrollo del proyecto, aquí tenemos a los **integrantes del grupo Materia Integradora de Telemática** encargados de recopilación y procesamiento de la información, así como de escribir los artículos divulgativos sobre buenas prácticas de ciberseguridad.

En este capítulo, se abordó la forma en la que se lleva a cabo elaboración de los artículos de carácter divulgativo primero describiendo los grupos objetivos a quienes van dirigidos estos trabajos, y posteriormente el método empleado y recursos utilizados, ahora presentaremos los artículos, como producto final, en el siguiente capítulo.

CAPÍTULO 3

3. PRUEBAS Y RESULTADOS

En esta sección se evalúa el trabajo realizado, los artículos divulgativos sobre ciberseguridad, por lo que se presentan las pruebas realizabas y los resultados obtenidos con su respectivo análisis.

3.1 Pruebas

Para la sección de pruebas se hizo uso del recurso de la encuesta, la misma fue creada en Google Forms (revisar sección de apéndice) y se dividía en tres secciones. La primera parte nos permitiría tener antecedentes o un conocimiento más amplio sobre la perspectiva que se tiene de la ciberseguridad por parte de los ciudadanos ecuatorianos. A continuación, se mostraba una serie de temas relacionados a la seguridad informática y se invitaba al lector a elegir un tema (artículo) según su nivel de conocimiento y preferencia. La última parte de la encuesta, estaba enfocada en una retroalimentación del artículo previamente leído, a modo que se comprendiera cuales eran los puntos positivos y negativos de los artículos elaborados.

Los artículos se encuentran orientados a diferentes grupos de acuerdo a sus nociones previas de ciberseguridad, así tenemos en el primer nivel de conocimiento al **Inicial**, donde los artículos van dirigidos al sector de la población con poco o nulo entendimiento sobre informática y tecnología en general, como pueden ser adultos, adultos mayores y niños. Destacar que la mayor parte de nuestros trabajos escritos están dirigidos a este grupo debido a que es el más numeroso y vulnerable. Para ellos tenemos los siguientes artículos: **Introducción a la Ciberseguridad que es y como puedo proteger mis equipos**, se presentan nociones básicas de ciberseguridad, con lo que se busca introducir al lector a diferentes técnicas y recomendaciones sencillas con las cuales podrá

proteger sus equipos e información contra programas maliciosos que busquen infectar el equipo o del acceso no autorizado. También tenemos, **Navega de forma segura por Internet**, donde se brindan consejos de navegación segura a través de la web, entre los cuales se enseña a los lectores el como identificar páginas web seguras, así como diferentes tipos de páginas y acciones que se deben de evitar mientras se navega por la red. Otro trabajo, denominado **Protección de menores en Internet**, existen diversos tipos de peligros a los que muchas veces los menores se ven expuestos debido al temprano uso de plataformas digitales y dispositivos tecnológicos, por lo que este artículo se brinda consejos y consideraciones a padres y adultos en general para proteger a los niños y adolescentes de estas amenazas. Por último, presentamos **Alerta en las redes sociales**, estas han tomado mucha relevancia en la actualidad y en este artículo se presentas algunas nociones a tener en cuenta como los peligros existentes (información falsa, estafas o robo de información) y consejos básicos para mantener nuestra privacidad en redes sociales.

El siguiente nivel es el **Intermedio**, donde los artículos van dirigidos a un público con uso y conocimiento más habitual de tecnologías, como lo pueden ser estudiantes o profesionales. Para ellos les presentamos los siguientes documentos, **Que es la ciberseguridad: Virus, ataques y métodos de seguridad**, se busca una introducción un poco más profunda al lector y enfocándose concretamente en los softwares maliciosos o virus. Se presentan los tipos de ataques más frecuentes en Internet, como reconocerlos y como evitar ser víctima de uno de estos. El siguiente artículo es **Seguridad informática dentro y fuera de oficina**, se presentan diferentes consejos y técnicas a tener en cuenta para salvaguardar la seguridad de los datos e información que almacenamos en nuestros dispositivos y en la nube. También se brindan consejos sobre el uso de redes publicas y los peligros que puede llevar su uso.

Por último, el nivel **Avanzado**, donde se presenta un artículo orientado al sector empresarial, mostrando las principales consideraciones de ciberseguridad que toda empresa debería conocer y tener.

3.2 Resultados

La figura 3.1, muestra los resultados de la primera pregunta de la encuesta, aquí se conoció que el grupo de personas con mayor uso de dispositivos electrónicos (celular, computadora, tablet, etc.) e Internet en el hogar son los adultos, seguido de los niños/adolescentes y en menor proporción los adultos mayores.

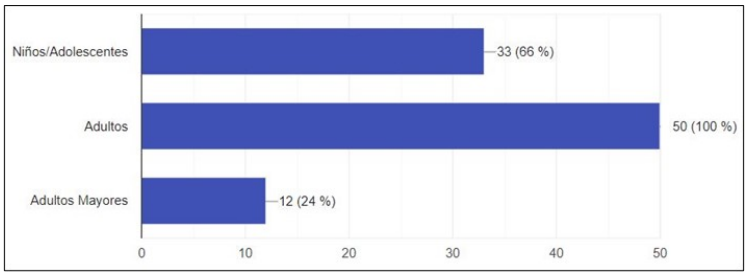


Figura 3.1: grupos de usuarios con uso de tecnologías e Internet

Luego se reveló cual era el nivel de conocimiento de los encuestados, en la figura 3.2. Aquí se tuvo que el grupo más numeroso era quienes tenían **nulo** conocimiento sobre ciberseguridad, seguido de cerca por quienes tienen una percepción más **básica** de seguridad informática y luego aquellos con un nivel **medio**.

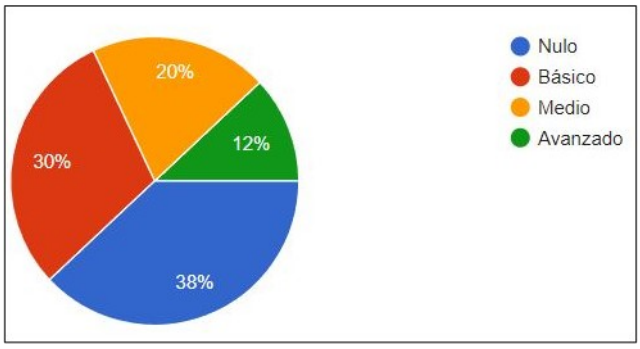


Figura 3.2: Nivel de conocimiento de encuestados sobre ciberseguridad

Posteriormente, en la figura 3.3, se conoció cuales eran los temas que más llamaban la atención de los lectores. Siendo el más popular el artículo : ”Protección de menores de los peligros de Internet”.

De acuerdo a la elección de cada lector, se mostraba el artículo correspondiente y se pasaba a la siguiente sección de la encuesta. En esta parte se mostraban cinco preguntas donde se calificaba y daba la respectiva retroalimentación del artículo leído.

Figura 3.3: Popularidad de artículos entre los encuestados

En la primera pregunta de esta sección, se calificaba la calidad de la información presentada en el artículo que habían leído. La figura 3.4, indica que la mayor parte de los encuestados contesto estar satisfecho con la información adquirida, ningún usuario respondió haber esta totalmente insatisfecho con el artículo.

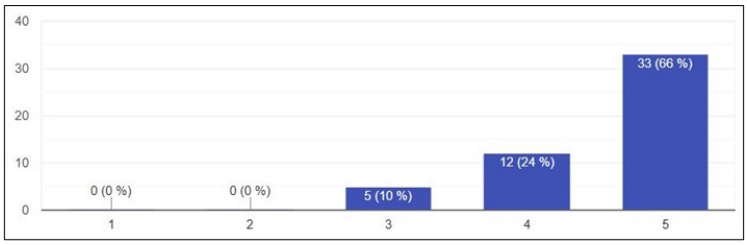


Figura 3.4: Aceptación de la información mostrada desde 1(muy mala) a 5 (muy buena)

Otro punto interesante de conocer acerca de nuestros artículos era la longitud. La figura 3.5, muestra que la mayor parte consideró como muy extenso el documento, otro grupo considerable se mostró neutral y ninguno calificó de muy corto el artículo.

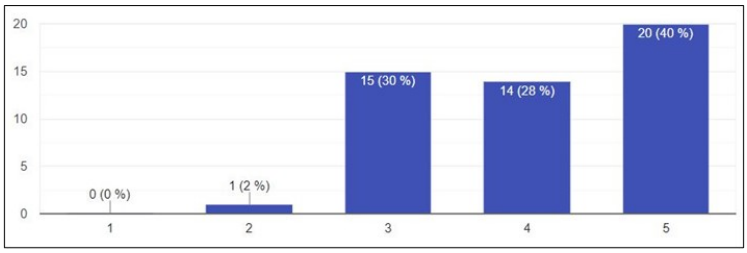


Figura 3.5: Aceptación de la longitud de los artículos mostrados desde 1(muy corto) a 5 (muy extenso)

Luego se preguntó sobre los recursos visuales usados en los artículos. Aquí se obtuvo el rango de respuestas más variado, como se aprecia en la figura 3.6, donde la mayor parte de lectores mantuvo una posición neutral, osea las imágenes no les parecieron ni malas ni buenas. Ningún encuestado dijo que son muy ilustrativas y a un pequeño porcentaje le pareció para nada ilustrativas las imágenes.

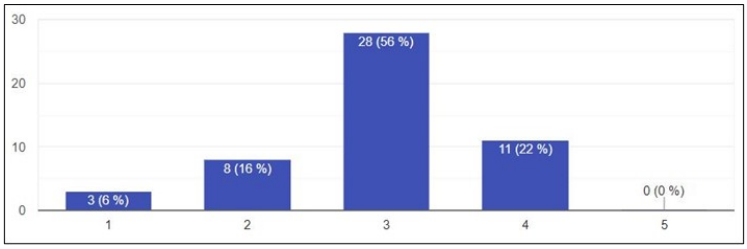


Figura 3.6: Aceptación de las imágenes mostradas desde 1 (poco ilustrativas) a 5 (muy ilustrativas)

En la penúltima pregunta, de manera directa se cuestionaba a los lectores si habían aprendido algo nuevo, luego de haber leido el artículo de su elección. Se conoció que la mayor parte de los lectores aceptaban haber adquirido nuevo conocimiento, mientras un pequeño grupo dijo lo contrario, lo que se muestra en la figura 3.7.

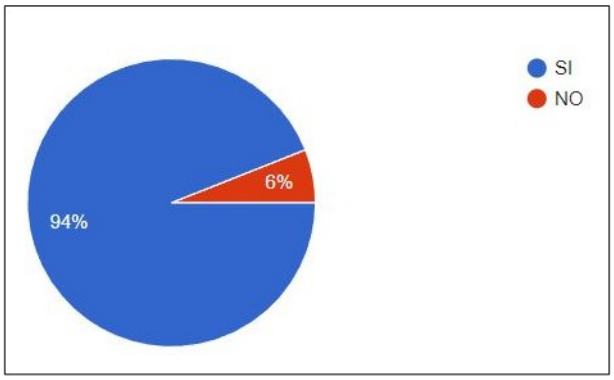


Figura 3.7: Afirmación de conocimientos adquiridos luego de leer los artículos

Finalmente la figura 3.8, muestra la última pregunta, de carácter abierta donde los encuestados podían colocar comentarios extra o recomendaciones para poder mejorar los artículos.

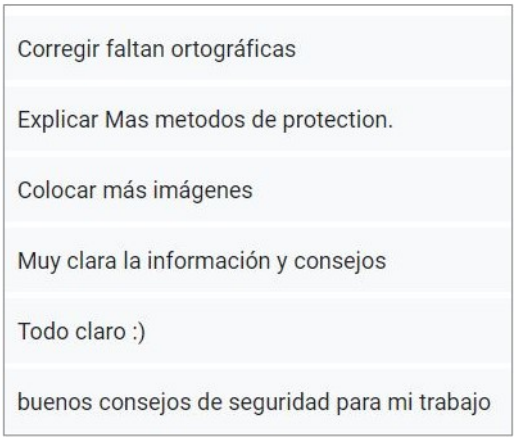


Figura 3.8: Comentarios adicionales de encuestados sobre los artículos leídos

Como se puede evidenciar los artículos han logrado concientizar y dar nociones básicas de ciberseguridad para proteger dispositivos e información, según la retroalimentación de la encuesta realizada.

CAPÍTULO 4

4. CONCLUSIONES, RECOMENDACIONES Y LINEAS FUTURAS

Por último, exponemos las ideas finales acerca de este trabajo de titulación, varias recomendaciones que pueden ayudar a realizar el trabajo de mejor manera y como mejorarlo en un futuro.

4.1 Conclusiones

En base a toda la información recopilada es posible determinar como la desinformación y el desconocimiento, sobre temas y practicas básicas de ciberseguridad, ha conducido a un aumento bastante significativo en la cantidad de personas que son víctimas de algún tipo de estafa o crimen informático a nivel global. Sobre todo en la época actual, donde muchos de los servicios están apostando por las plataformas digitales, hecho que tuvo su mayor crecimiento partir del año 2020 donde la pandemia obligo a muchas personas a usarlas. Ecuador, al igual que el resto del mundo, se vio afectada por este aumento de delitos informáticos, pero debido a la baja preparación en ciberseguridad de la población e incluso las bajas medidas de protección de algunas instituciones publicas y privadas provocado que el teme de seguridad informática sea unas de las prioridades de todas las instituciones en estos últimos dos años.

El tipo de amenaza mas frecuente al que las personas se ven expuestas según los reportes de ciberataques a nivel global, regional y nacional corresponden a delitos de robo de información personal, suplantación de identidad y estafas. Muchos de estos ataques se dan mediante métodos muy básicos como el spam vía e-mail o llamadas telefónicas falsas, que pudieron ser evitadas fácilmente si las personas hubieran tenido un conocimiento muy básico sobre ciberseguridad. Se identificó que este es un punto

urgente a tratar, por lo que se enfoca los temas a tratar en los artículos en como reconocer los tipos de delitos cibernéticos mas frecuentes, así como en mencionar técnicas de seguridad básicas para evitar caer en ellos. Algunos de los temas tratados son el evitar compartir información personal en los diferentes medios de internet o evitar abrir o responder correos de dudosa procedencia o veracidad.

Para ampliar mas el campo que abarcan los temas tratados en los artículos se realizó una síntesis de los tipos de virus mas frecuentes detectados a nivel mundial. Con esto el objetivo es concientizar a las personas sobre los peligros existentes a los que pueden estar expuestos en internet si no se toman las medidas de precaución adecuadas. Entre los virus mas frecuentes que se explican están los Adware, Spyware y los Ransomware, los cuales son los principales tipos de amenazas detectadas por los sistemas de antivirus a nivel global.

Se identificó que muchos usuarios de dispositivos electrónicos han tenido sus dudas con respecto a las plataformas de nube, sobre todo en cuanto al funcionamiento de la seguridad de lo datos que suben en los servicios de almacenamiento. Por lo tanto, se consideró oportuno el explicar el funcionamiento de credenciales y la forma correcta de compartir archivos alojados en la nube. De la misma forma se considero oportuno explicar este mismo campo orientándolo a una solución para las empresas, donde en ocasiones empresas medianas o pequeñas no tienen del claro las responsabilidades en cuanto a la gestión de seguridad de los servicios y datos que alojan en nube y en muchos casos se llega a pensar que la seguridad corresponde únicamente al proveedor del servicio de nube.

Para finalizar, basados de en la retroalimentación recibida por las encuestas realizadas podemos concluir que los artículos elaborados han cumplido con la finalidad: concienciar a las personas sobre los peligros existentes en internet, y brindarles medios y mecanismos básicos de ciberseguridad. Con esto ahora muchos de los lectores tienen una mayor noción sobre formas de aumentar la seguridad de sus dispositivos e información digital.

4.2 Recomendaciones

Se debería conocer con antelación el medio encargado de publicar los artículos, de esta manera los escritores conocerán todas las pautas y restricción impuestas antes

de empezar a escribir. Así se podrían evitar inconvenientes posteriores y continuas revisiones hasta que sean aprobados y publicados.

La inclusión de recursos visuales es importante, principalmente en textos extensos. Las imágenes pueden ayudar a esclarecer las dudas que los lectores podrían tener, por lo que es importante saber como y donde usarlas.

Realizar un pequeño test a los lectores, luego de haber leído los artículos sobre ciberseguridad, permitiría conocer si en verdad hubo un entendimiento sobre el tema. De esta manera se tendría un mejor panorama de los documentos elaborados, hacer las respectivas correcciones y llegar a mejores conclusiones.

4.3 Líneas Futuras

Debido a los bajos hábitos de lectura de los ecuatorianos, sería bueno transmitir la información de los artículos mediante recursos visuales. Esto se podría hacer mediante historietas, cortas animaciones, dramatizaciones; en las que se eduque sobre temas de ciberseguridad. Se podría tratar de un proyecto multidisciplinario entre gente de FIEC encargada del área investigativa y FADCOM encargados de las producciones audiovisuales.

Se podría crear una página web o aplicación móvil, en la que se eduque sobre seguridad informática. Esta podría estar organizada por módulos, en donde se agrupen varios temas y al final de cada capítulo un pequeño test que verifique el nivel de entendimiento. Para hacerlo más interesante se podría entregar un certificado de aprobación de curso avalado por la universidad y motivar así a la gente a la vez que aprende.

Realizar charlas sobre ciberseguridad sería otra alternativa para transmitir conocimientos. Visitar escuelas o centros comunitarios donde se presente la información, lo que permitiría tener un mayor control sobre el público.

BIBLIOGRAFÍA

[1] S. D. Crocker, “Arpanet and its evolution—a report card,” *IEEE Communications Magazine*, vol. 59, no. 12, pp. 118–124, 2021.

[2] S. Lukasik, “Why the arpanet was built,” *IEEE Annals of the History of Computing*, vol. 33, no. 3, pp. 4–21, 2010.

[3] I. Saleh, *Internet of Things (IoT): Concepts, Issues, Challenges and Perspectives*, pp. 1–26. 2018.

[4] M. Ros-Martín, “Evolución de los servicios de redes sociales en internet,” *Profesional de la información*, vol. 18, no. 5, pp. 552–558, 2009.

[5] M. Veale and I. Brown, “Cybersecurity,” *Internet Policy Review*, vol. 9, no. 4, pp. 1–22, 2020.

[6] UIT, *SERIE X: REDES DE DATOS, COMUNICACIONES DE SISTEMAS ABIERTOS Y SEGURIDAD Seguridad en el ciberespacio – Ciberseguridad Aspectos generales de la ciberseguridad*. Ginebra: Union Internacional de Telecomunicaciones, 2008.

[7] M. Machín, Nieva Gazapo, “La ciberseguridad como factor crÍtico en la seguridad de la uniÓn europea,” *Revista UNISCI*, 2016.

[8] L. R. H. . R. P. R. C. Robert Vargas Borbúa, “Cyber-defense and cybersecurity, beyond the virtual world: Ecuadorian model of cyber-defense governance,” *URVIO - Revista Latinoamericana de Estudios de Seguridad*, no. 20, pp. 31–45, 2017.

[9] Telegrafo, “Ecuador escala 9 puestos en ranking de aplicación de las tic,” 2014.

[10] L. Institute, “Avances de la ciberseguridad y el cibercrimen desde la realidad de ecuador,” 2021.

[11] S. Zelada, “Covid-19, un acelerador de la transformación digital,” *Deloitte*, 2021.

[12] W. Z. . R. P. Aura Zambrano, Fausto Loor, “Delitos informaticos en tiempos de covid: Revision literaria ecuador,” 2021.

[13] M. B. . A. Monteiro, “El ciberespacio, durante y después de la pandemia covid-19,” *Revista de la Academia de Guerra del Ejército Ecuatoriano*, vol. 14, no. 1, 2021.

[14] F. en Movimiento, *Guía completa para padres - protege a tus hijos en internet*. Ciudad de México: Fundación en Movimiento, 2018.

[15] SCT, *Guía de ciberseguridad para el uso seguro de redes y dispositivos de telecomunicaciones en apoyo al teletrabajo*. Ciudad de México: Secretaría de Comunicaciones y Transporte, 2020.

[16] SCT, *Guía de ciberseguridad para el uso de redes y dispositivos de telecomunicaciones en apoyo a la educación*. Ciudad de México: Secretaría de Comunicaciones y Transporte, 2020.

[17] ACSC, *GUÍA DE CIBERSEGURIDAD PARA LA PEQUEÑA EMPRESA*. Canberra: Australian Cyber Security Centre, 2021.

[18] ElevITy, *The Cybersecurity Handbook*. Wisconsin: ElevITy, 2020.

[19] CyberTalk, *BUYER’S GUIDE TO CYBER SECURITY*. CyberTalk, 2021.

[20] INCIBE, *Guía de ciberseguridad - La ciberseguridad al alcance de todos*. Madrid: Instituto Nacional de Ciberseguridad, 2022.

[21] EcuCERT, “Guías y consejos.” Available at https://www.ecucert.gob.ec/guias-y-consejos/ (2022/10/24).

[22] ElUniverso, “15 tips de ciberseguridad para pequeños negocios.” Available at https://www.eluniverso.com/larevista/tecnologia/15-tips-de-ciberseguridad-para-pequenos-negocios-nota/, 2022.

[23] ElUniverso, “7 cosas que no se deben compartir en internet bajo ningún motivo.” Available at https://www.eluniverso.com/larevista/tecnologia/7-cosas-que-no-se-deben-compartir-en-internet-bajo-ningun-motivo-nota/, 2022.

[24] ElUniverso, “Los seis datos para identificar posibles estafas en compra y venta de artículos en internet.” Available at https://www.eluniverso.com/noticias/seguridad/los-seis-datos-para-identificar-posibles-estafas-en-compra-y-venta-de-articulos- 2021.

[25] J. Sayago-Heredia, “Ciberseguridad en ecuador y latinoamérica,” *Killkana: Entre Modoelos, Simulaciones y Comportamientos*, vol. 5, no. 1, 2022.

[26] F. G. del Estado, “Ciberdelitos: Perfil criminológico,” *Revista Científica de Ciencias Jurídicas, Criminología y Seguridad*, vol. 30, no. 1, 2021.

[27] M. de Telecomunicaciones y de la Sociedad de la Información, “Estrategia nacional de ciberseguridad del ecuador,” 2022.

[28] M. Vidal Ledo and N. Rivera Michelena, “Investigación-acción,” *Educación Médica Superior*, vol. 21, no. 4, pp. 0–0, 2007.

APÉNDICES

Apéndice A: Encuesta sobre artículos dirigidos a la ciberseguridad

En esta sección se presentan las preguntas que se emplearon para obtener retroalimentación de los trabajos escritos

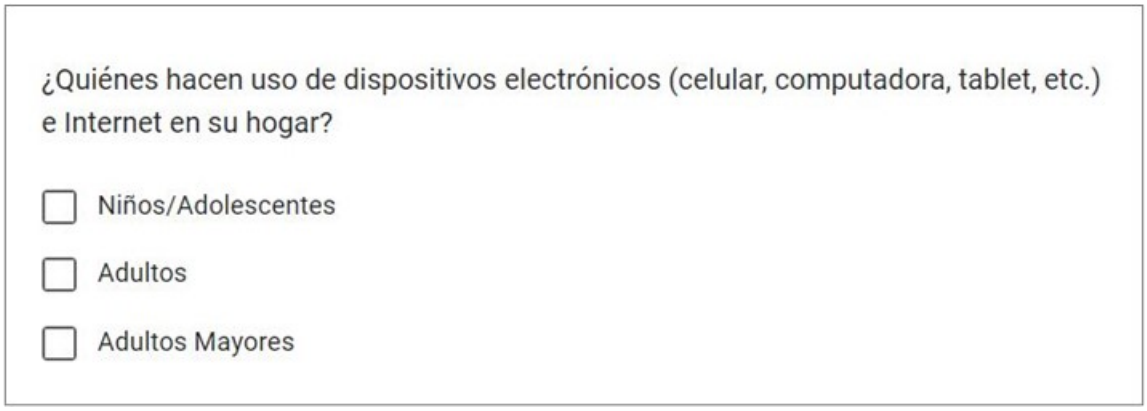


Figura 1: pregunta 1 de la encuesta

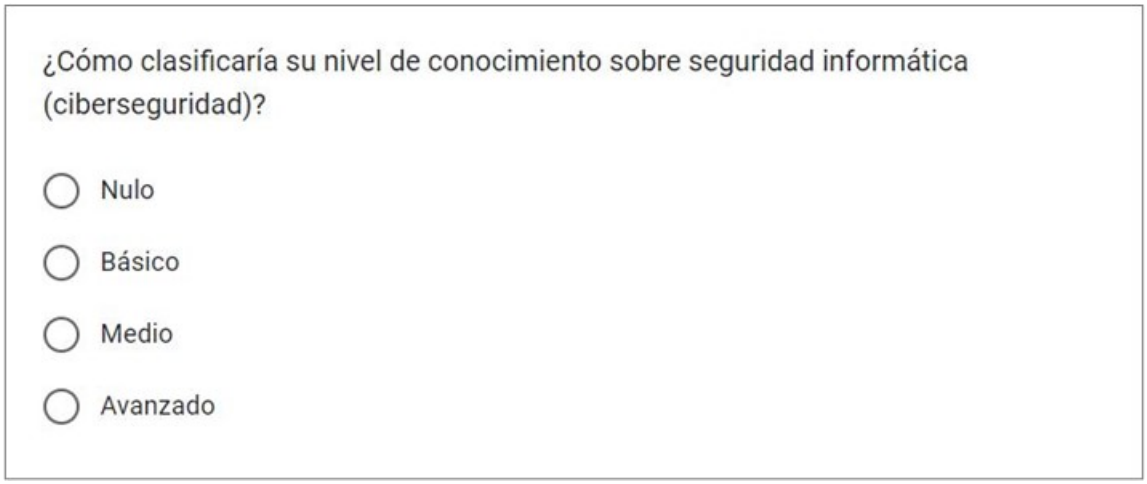


Figura 2: pregunta 2 de la encuesta

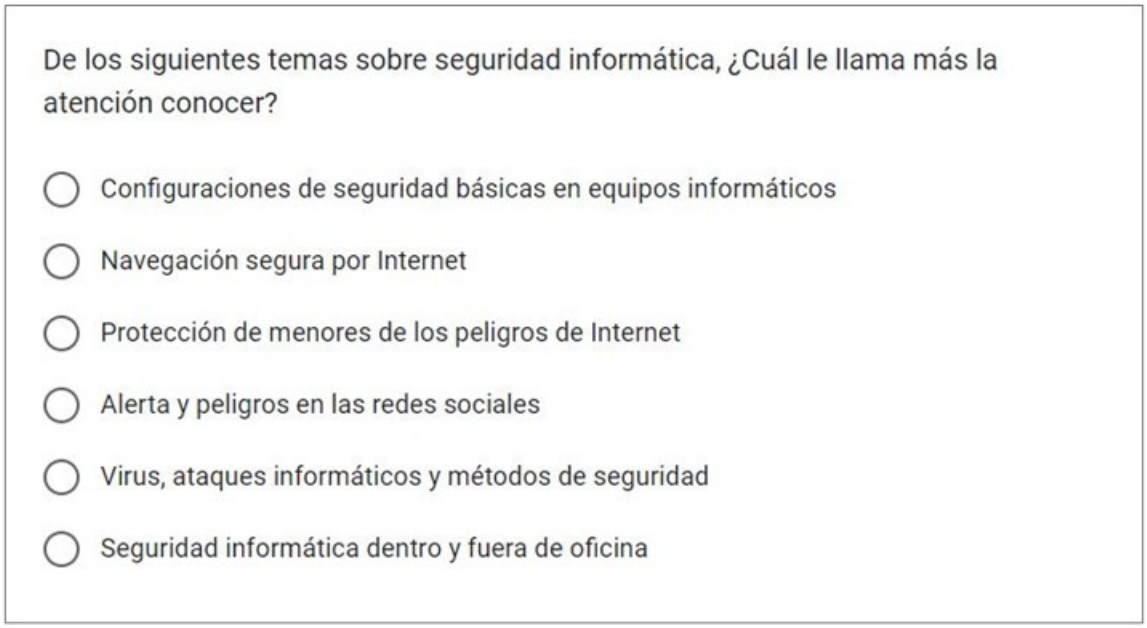


Figura 3: pregunta 3 de la encuesta

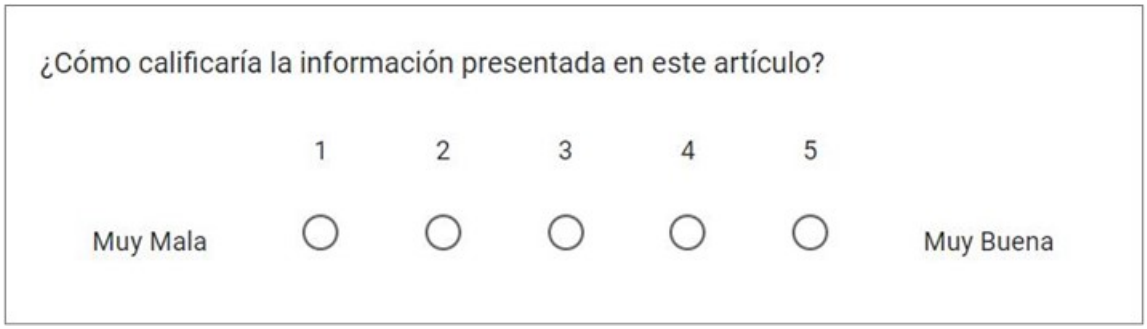


Figura 4: pregunta 4 de la encuesta

Figura 5: pregunta 5 de la encuesta

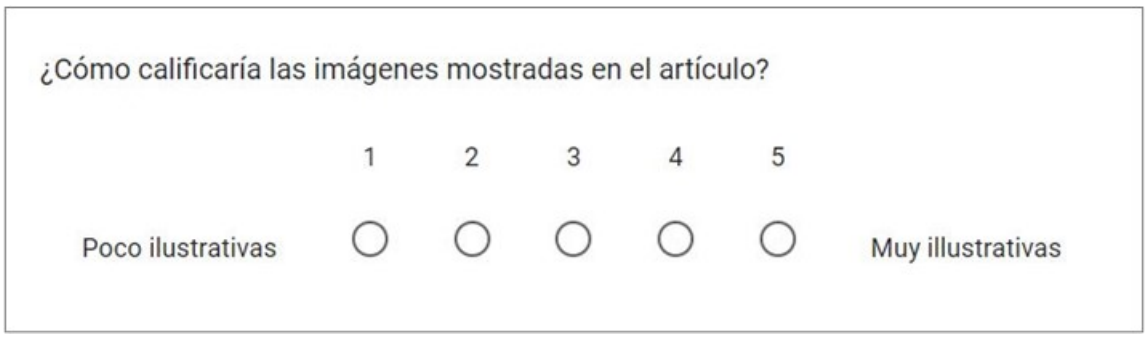


Figura 6: pregunta 6 de la encuesta

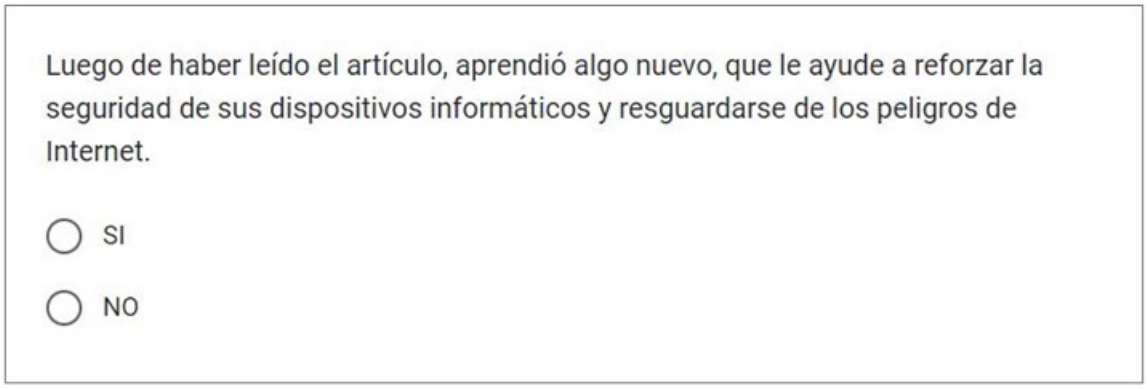


Figura 7: pregunta 7 de la encuesta

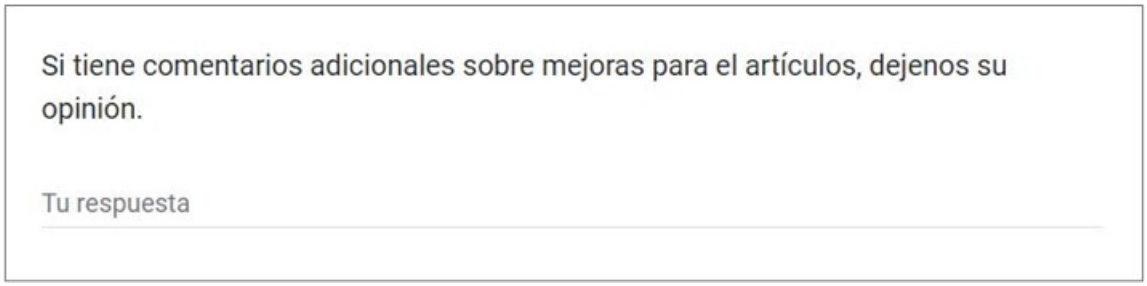


Figura 8: pregunta 8 de la encuesta

Apéndice B: Artículo divulgativo elaborado n°1

El periódico

Año 2023 Febrero Ciudad, Guayaquil

Introducción a la Ciberseguridad: que es y como puedo proteger mis equipos

por Bryan Chunga

Desde el uso de un teléfono inteligente o usa computadora a equipos más especializados, la tecnología ya forma parte del día a día de las personas. Todos los días vemos avances y nuevas tecnologías disponibles, sin embargo, también es necesario tener en cuenta algunas nociones básicas para proteger nuestros dispositivos y la información que almacenamos en ellos. Es por esto por lo que a continuación presentamos algunas nociones básicos sobre ciberseguridad que deberías tener en cuenta.

Mantén actualizado tus dispositivos.

Los fabricantes de dispositivo, ya sea un teléfono, computador u otro equipo informático, lanzan de forma constante actualizaciones de software. En estas actualizaciones se incluyen mejoras de rendimiento o funcionalidades nuevas, pero también se incluyes parches de seguridad para el equipo. Estos parches de seguridad están enfocados a corregir errores que afectan a la vulnerabilidad del dispositivo por lo cual es necesario instalar estas actualizaciones para asegurarse que el equipo tenga los parches de seguridad mas recientes. Recuerda siempre descargar estas actualizaciones desde el sitio oficial del fabricante o proveedor, el cual muchas veces está disponible a través del menú de configuración de dispositivo. Evita en cualquier circunstancia descargar una actualización desde un sitio no oficial.

Establece contraseñas seguras

Bloquear tu dispositivo con una contraseña es la forma más básica de prevenir un acceso o uso no autorizado de tus equipos, cualquiera sea el método, PIN, contraseña alfanumérica o patrón, la función es la misma. Algunos consejos para establecer tu contraseña son:

- Pon una contraseña fácil de recordar.
- Evitar poner como contraseña datos como tu nombre o tu fecha de nacimiento.
- Evita contraseñas sencillas como “12345” o “abcde”.
- Usa combinaciones de letras, números y símbolos para la contraseña. Ej: C0ntr4s3ñ4!
- Si decides usar un patrón, evita usar formas sencillas como “Z” o “L”.

Otra opción mas segura es usar el sistema de bloqueo con **autentificación biométrica**, el hace validaciones con las huellas dactilares o reconocimiento facial, de forma que únicamente el usuario podrá desbloquear el dispositivo. Esta función esta presente en la mayoría de los teléfonos modernos.

Siempre usa un antivirus

Los antivirus son programas que puedes y **deberías instalar** en tus dispositivos. La función de estos es detectar diversos tipos de virus o programas maliciosos que pudieran entrar en tu dispositivo. Al detectar un virus en el equipo, el antivirus te podrá ofrecer diferentes posibles acciones como tratar de recuperar el archivo infectado o eliminarlo. Muchos antivirus incluyen un método de prevención donde son capaces de bloquear el virus antes de que este ingrese en el dispositivo, por lo que es importante siempre tenerlo activado. Algunos sistemas operativos traen un sistema de antivirus integrados, por ejemplo *Windows* trae consigo **Windows Defender**, pero tambien tienes la opciones de usar antivirus de terceros como *AVAST*, *AVG* o *Norton*.

Al igual que con las actualizaciones del equipo, también **es necesario mantener actualizado el antivirus**, ya que en las actualizaciones se incluyen mejores técnicas de prevención y recuperación, además de incluir en la base de datos registros de nuevos tipos de virus de forma que el antivirus sea capaz de identificarlos.

El Firewall

El firewall es un **conjunto de reglas** que tienen muchos equipos informáticos. Estas reglas son las que rigen la comunicación del equipo a través de la red. Por defecto el equipo viene configurado con todas las reglas necesarias para permitir únicamente el tráfico de comunicaciones autorizadas, por lo que no es necesario realizar mayores cambios a este. Sin embargo, ahora sabiendo la importancia del firewall para la seguridad del dispositivo, es de vital importancia que **evites a toda costa desactivarlo**.

Siguiendo todos estos simples consejos ahora seras capaz de aumentar la seguridad de tus equipos informaticos y tu informació frente a programas malisiosos o el acceso de personas no autorizadas. No olvides que **tus contraseñas son exclusivamente para tu uso personal, por lo tanto no las compartas con nadie**.

Apéndice C: Artículo divulgativo elaborado n°2

El periódico

Año 2023 Febrero Ciudad, Guayaquil

Navega de forma segura por Internet

por Bryan Chunga

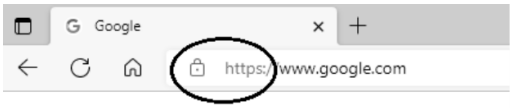
Internet nos brinda acceso a una gran cantidad de información de todo tipo, y a la vez es una de las vías más usadas por los piratas informáticos que buscan infectar los dispositivos de las personas para robar información personas, documentos, cometer fraudes, etc. Existen métodos que permiten tomar acción para protegerse de estas vulnerabilidades por lo que en este articulo presentaremos algunas pautas básicas a seguir para proteger tus dispositivos cuando navegues por internet.

Los navegadores

Los navegadores son programas a través de los cuales podemos acceder a los distintos sitios web disponibles. Estos de encargan de interpretar la información y presentar a los usuarios el contenido de los sitios web, así como permite la interacción del usuario con el sitio que visita, además incluyen configuraciones de seguridad para la protección en la web. Existe gran variedad de navegadores disponibles, sin embargo, algunos de más seguros en cuanto a gestión de seguridad al navegar entre dientes sitios pueden ser: *Mozilla Firefox*, *Microsoft Edge* u *Opera*, los cuales son los navegadores más populares actualmente. Otra opción de navegador que esta tomando relevancia es Brave, el integra por defecto un bloqueador de anuncios el cual nos evita la publicidad invasiva de algunos sitios. Por otro lado, si queremos una opción mas segura, los desarrolladores de antivirus como *AVG* o *AVAST* han lanzado opciones de navegadores totalmente orientados a la seguridad y privacidad del usuario durante la navegación, sin embargo, estos pueden ser algo mas lentos que los demás debido a todas las validaciones se seguridad que ejecutan en cada sitio web que se visita.

Paginas Web Seguras

Existen páginas web que tienen **certificados de seguridad**, los cuales son verificados por tu navegador al momento que accedes a cada uno de los sitios. Estos certificados de seguridad permiten hacer una validación de los datos del propietario del sitio web, verificando la autenticidad del sitio al que accedes, con el objetivo de evitar caer en un sitio web falsificado. Podemos reconocer que en sitio web posee certificados de seguridad viendo el enlace de la pagina en la que estamos, esta debe empezar con "**https:**" donde la 's' denota que la pagina posee certificados de seguridad, además en muchos navegadores podemos ver una imagen de un **candado cerrado** junto a la barra de direcciones cuando estemos dentro de un sitio web con certificados de seguridad.



La mayoría de los sitios web oficiales poseen estos certificados por lo que es una forma fácil de reconocerlos y de saber que no estas en un sitio web falsificado donde tu infomración tu informacion puede correr peligro.

Navega de forma segura

Al navegar en internet existen ciertas pautas sencillas que nos ayudan a navegar de forma segura a través de diferentes sitios web, a continuación te presentaremos algunas de ellas.

Algunos sitios presentaran **publicidad invasiva** en su interfaz, pero muchas veces la publicidad que se encuentra puede tener fines maliciosos. Por lo general presentan un anuncio llamativo para que ingreses y después tratar de vulnerar tu dispositivo. Por lo tanto, evita dar click en estos anuncios y muchos menos aceptar permisos a sitios sospechosos. Puedes usar un **bloqueador de anuncios**, como *AdBlock* o *AdGuard* para evitar estas publicidades o un navegador como *Brave* que incluye bloqueador de anuncion por defecto. Algunos sitios van aún mas allá, con publicidad invasiva y pop ups que iniciarán abrirán nuevas ventanas de tu navegador únicamente con publicidad. En caso de reconocer un sitio de este estilo evita visitarlo nuevamente.

No compartas ningún tipo de información personal o contraseñas a traves de foros, redes sociales, blogs, etc. Estos datos podrian ser vistos por atacantes informaticos que los aprovevharian para tratar de vulnerar tu seguridad. Si buscas asistencia o asesoramiento para algun tramite acude siempre a los sitios oficiales para informate.

Evita cualquier tipo de descargas de sitios no oficiales, y si de pronto se genera una descarga al entrar en algún sitio web, evita a toda costa abrir el archivo descargado y ejecuta de manera inmediata el antivirus de tu equipo para detectar cualquier problema, finalmente procura eliminar el archivo.

Apéndice D: Artículo divulgativo elaborado n°3

El periódico

Año 2023 Febrero Ciudad, Guayaquil

Protección de menores en Internet

por Christian Ramos

"La irrupción de las nuevas tecnologías nos obliga a educar a los niños de distinta forma"
(Howard Gardner)

Es cierto que cada vez es más temprana la edad a la que los menores entran en contacto con las nuevas tecnologías e Internet. Seguramente ha notado como niños y adolescentes manejan con mucha destreza todo tipo de dispositivos electrónicos y posiblemente acuda a ellos si tiene problemas con su teléfono celular o requiere ayuda con Internet, y aunque parezcan unos expertos en el tema, no están exentos de las amenazas existentes en la web.

Principalmente, Internet se ha convertido en una fuente de descubrimiento sobre muchos temas para los menores, ¿Se ha puesto a pensar en todo el material sensible e inapropiado al que se puede acceder con unos cuantos clicks?. Por ejemplo, el contenido visual al que se tiene acceso en *Youtube*, *Netflix* u otras plataformas de entretenimiento no siempre es apto para ciertas edades. **Muchas veces los niños imitan lo que ven**. Al igual que los videojuegos, muchos de ellos pueden llegar a ser muy violentos, adictivos o irritantes y podrían acarrear problemas de conducta en los más pequeños principalmente. Otro peligro de los videojuegos, en especial los juegos en linea, es que varios permiten interactuar con otros usuarios por chat de texto o de voz, por lo que los chicos podrían estar hablando a menudo con desconocidos.

Por otro lado, entre los adolescentes, las redes sociales son muy famosas. Varios especialistas señalan que la edad idónea para iniciar en estos sitios es a partir de los 14 años. Aunque muchos manejan más de una red social, como: *Facebook*, *Instagram*, *TikTok*, etc. Pocos conocen los peligros a los que se pueden enfrentar. Por ejemplo, la información que mostramos o publicamos puede ser usado por otros usuarios con muchos fines como suplantar identidades, conocer datos personales o ubicaciones en tiempo real. Otro peligro que debería conocer es el *grooming*, consiste en una persona mayor haciendoce pasar por un menor mediante un perfil falso, posteriormente ganarse la confianza de otros menores para luego pedir cosas indebidas. En muchos casos puede terminar en encuentros reales, lo que supone ya un serio peligro. También tenemos el acoso virtual o *ciberbullying*, donde un usuario puede molestar, chantajear o amenazar a otro y debido a la presión u hostigamiento que siente el afectado puede llevar a problemas psicológicos y en casos más extremos a cometer suicidio.

. *¿Qué puede hacer usted como padre o adulto en general para proteger a los menores en la red?*

Para mantenerlos a salvo en el hogar, procure siempre **supervisar** la actividad de los menores, no los deje mucho tiempo solos. Si tiene equipos con conexión a Internet compartidos como una computadora de escritorio, una *Smart* TV o una consola de videojuegos es mejor ubicarlas en espacios públicos del hogar como la sala. La comunicación también es importante. Pregunte frecuentemente lo que hacen o ven cuando navegan por la red, ya que podrían toparse con alguna situación inusual a la que debería prestarle más atención. También imponga reglas, **limite el tiempo** de uso de dispositivos, establezca horarios, especialmente durante la noche donde es más probable que se desvelen y no duerman el tiempo necesario para su edad.

Además, al igual que les prohibe hablar con desconocidos en la calle, prohibales **hablar con extraños** por la web, especialmente en redes sociales, **no compartir información** de ningún tipo, ni acceder a peticiones que les hagan. Adicionalmente, es importante que evite hacer mal uso de las tecnologías frente a sus hijos, **ponga el ejemplo**. Procure no usar dispositivos electrónicos durante la hora de la comida o cuando conduce, ya que esto es muy peligroso y es una práctica común en adolescentes que inician a conducir, ellos pueden asimilar estos hábitos como normales y replicarlos.

Por último, si desea tener un control más amplio sobre los menores, cuando no está a su alcanze la supervisión continua, le interesaría conocer sobre el **control parental**. Es una aplicación que le permite configurar los dispositivos de los menores para que solo puedan acceder a contenido indicado para su edad en Internet. Actualmente existen controles parentales más invasivos, con configuraciones más avanzadas como notificaciones de texto, ubicación en tiempo real, filtros y reportes de búsqueda en Internet, entre otras.

¡Recuerde!, el mundo virtual es igual de peligroso que el mundo real, y los menores de edad el grupo humano más fácil de persuadir y al que debemos de prestarle más atención.

Apéndice E: Artículo divulgativo elaborado n°4

El periódico

Año 2023 Febrero Ciudad, Guayaquil

Alerta en las redes sociales

por Christian Ramos

Las redes sociales son los sitios más visitados de Internet y seguramente usted usa los servicios de mensajería instantánea y videollamada, como: *Messenger*, *WhatsApp* o *Telegram* para poder comunicarse con sus familiares y conocidos. Todos los días se comparten millones de publicaciones que incluyen información personal y laboral, que en muchos casos puede ser vista por cualquier persona. Esto supone un terrible peligro para nosotros como usuarios ya que da aceso a nuestras vidas. Por eso le presentamos algunas recomendaciones que una vez aplicadas le ayudarán a estar protegido y alerta en estos sitios.

La primero que hace para ingresar a su red social preferida es iniciar sesión, pues la consideración inicial y más importante es tener una **clave** segura. Dependiendo del sitio, la **contraseña** debe incluir letras mayúsculas y minúsculas, números así como símbolos especiales. Otra de las exigencias es que deben de tener una longitud mínima (usualmente mayor a 8 caracteres). Por ello es importante seleccionar una **contraseña** compleja y a la vez fácil de recordar como por ejemplo: S3gur!d4D. Adicionalmente no se debe de usar la misma **contraseña** en diferentes sitios web. Generar y recordar tantas contraseñas puede resultarle difícil por lo que si usted es de las personas que siempre las olvida, puede usar una aplicacion de **gestión de claves**. Estas existen de paga como *1Password* y *Daslane* o gratuitas como *LastPass* y *KeePass*. Estas aplicaciones le ayudarán a crear, mantener y gestionar todas sus contraseñas de manersa segura.

Una vez dentro de la red social, recuerde que por defecto todo perfil de usuario es público, es decir que cualquier persona podrá ver nuestra información. Muchas de las redes sociales ofrecen varios niveles de seguridad que usted puede configurar según sus necesidades. Limite quienes pueden enviarle solicitudes de amistad, ver sus pubicaciones o lista de amigos, es preferible poner su **perfil en privado**, de esta manera estamos limitando el acceso a nuestra información solo a quienes conocemos. **¡Recuerde lo fácil que es crear una cuenta de usuario en redes sociales!** Evite a los extraños, sino conoce a alguien evite entablar comunicación con ellos o aceptar solicitudes de amistad. Por otro lado, si nota un comportamiento inusual o indebido de un usuario hacia usted, bloqueelo directamente o reportelo a la página para que pueda proceder con la eliminación del usuario peligroso. Por último, **limite lo que publica**. A mucha gente le gusta publicar lo que hace en su día a día. Si usted es una de estas personas, debería ser más precavido en lo que deja ver. Siempre evite compartir datos personales, laborales, financieros. Tampoco muestre su ubicación y mucho menos publique los planes que tiene o hará. Ladrones, secuestradores y otros delincuentes podrían aprovecharse de esta información.

"Ën el pasado, eras lo que tenías ahora eres lo que compartes"
(Godfried Bogaard)

Otros tipos de peligros a los que se exponen los usuarios en redes sociales e Internet en general, son las **estafas**. Ciertamente la primera opción para compras online son las tiendas oficiales, sin embargo, muchas de ellas no tienen cobertura en nuestro país. Por esto acudimos a páginas de terceros para adquirir los productos que deseamos. Lo primero que debe tener en cuenta es si el sitio web es confiable, la forma más sencilla de saberlo es buscar en la barra de direcciones la figura de un **candado** esto asegura que la página web que visita es confiable (como se muestra en la figura).

También debe comprobar si el vendedor posee un perfil verificado, esto es que lo acredite como vendedor en la página, además de que las opiniones acerca de sus ventas sean mayoritariamente positivas. Observe que las imágenes que se muestran del producto sean creíbles, ya que pueden ser sacadas de otros sitios de Internet. Fíjese en el precio del producto y compare con el precio de tiendas oficiales. Si tiene un precio muy inferior al comercial, posiblemente sea una estafa o peor aún de origen ilícito. Por último, y más importante, revise las formas de pago oficiales y si están protegidos sus derechos de consumidor por la página web en caso de inconvenientes. Nunca realice pagos por adelantado, ni de información sobre sus tarjetas de crédito/débido. Tampoco es buena idea quedar con el vendedor en un punto de encuentro físico para la entrega del producto y si lo hace procure ir acompañado y en un lugar público como un centro comercial o un parque.

Algo más que debe tener en mente, no todo lo que vemos en Internet es cierto, lo fácil con lo que se puede hacer viral una publicación con ayuda de las redes sociales es sorprendente, en pocos minutos puede recorrer el planeta y llegar a nuestros ojos, las **noticias falsas (Fake news)** solo buscan desinformar y causar caos en la población, por eso siempre verifique que la información que lee sea de fuentes oficiales o páginas verificadas como sitios de prensa o de gobierno, observe que el formato de la noticia sea el adecuado, cuide la estética, use buena ortografía e imágenes de calidad y si aún sigue teniendo dudas busque la información en diversas fuentes para corroborar que la noticia sea verídica.

Por último, está la **ingeniería social**. Se refiere a técnicas para sacar provecho del comportamiento humano, por lo general un usuario (victimario) presenta una situación aparentemente real a otro usuario (víctima), con el fin de obtener algún tipo de beneficioso de este último. Seguramente usted

ha recibido mensajes o llamadas en las que le ofrecen participar en concursos o que talvez se ha ganado un premio, también sobre alguna oferta de trabajo ofreciendo excelentes sueldos, o incluso alguien haciéndose pasar por un familiar o conocido pidiéndole dinero o sus datos personales. Todos estos escenarios son usados para engañar a la gente y sacar provecho, así que debe estar alerta. No establezca comunicación de ningún tipo con estos usuarios mal intencionados, bloquéelos directamente, evite dar cualquier tipo de información, comuníquese directamente con sus familiares o amigos si sospecha que se están haciendo pasar por ellos. Si recibe mensajes de desconocidos con enlaces a otros sitios de internet o archivos adjuntos, es preferible no abrirlos ya que no son confiables.

¡Recuerde!, lo mucho que se puede hacer detrás de una pantalla. Las redes sociales nos han permitido estar cada vez más conectados, pero también han traido los peligros del mundo real a estos sitios, los mismos que debemos conocer y estar preparados para enfrentarlos.

Apéndice F: Artículo divulgativo elaborado n°5

El periódico

Año 2023 Febrero Ciudad, Guayaquil

Que es la ciberseguridad: Virus, ataques y métodos de seguridad

Cybersecurity and Ciberresilience Group (CCG) Bryan Chunga, Christian Ramos, Ignacio Marin-Garcia

La seguridad informática, o ciberseguridad, es un área que en muchas ocasiones ignoramos, ya sea por falta de conocimiento sobre cómo proteger nuestros equipos e información, o el desconocimiento sobre los posibles riegos a los que estamos expuestos. Existen muchos métodos mediante los cuales un ciberdelincuente puede atacar a tu equipo, incluso los atacantes pueden buscar formas de infectar tu equipo sin siquiera tu ser el objetivo final del ataque.

En esta guía se presentaremos algunos conceptos claves de seguridad informática y técnicas para que puedas proteger tus equipos e información.

Los software maliciosos: que son y como protegerse de ellos.

Un software malicioso es in programa que se infiltra a tu equipo y ejecuta diferentes acciones en el, dependiendo del objetivo para el que se haya desarrollado. La aparición de estos programas es un mal que va en aumento debido a las ganancias que generan al crimen informático organizado. Acontinuación te presentaemos los algunos de los ataques informaticos mas frecuentes y te explicaremos como funcionan.

Los **adware** son unos de los tipos de ataques más populares hoy en día tanto en computadores como teléfonos inteligentes debido a su simpleza y la forma rápida de generar ingresos para los cibercriminales. Estos virus son aparentemente "inofensivos" ya que no buscan robar directamente a sus víctimas, no dañan directamente al equipo infectado ni la información que contenga, su objetivo es llenar el dispositivo con publicidad invasiva a forma de ventanas emergentes en los computadores, o de notificaciones en los teléfonos. Aunque estos virus no son perjudiciales como tal, los anuncios que nos muestra pueden tener otras intenciones, como hacer a los usuarios caer en una estafa o robar su información. Es frecuente que en estos tipos de virus se muestren anuncios de grandes ofertas en productos con la intención de robar datos bancarios o de actualizaciones disponibles del equipo para que el usuario descargue algún otro programa malicioso.

Los **botnet** o **equipos 'zombie'** son otro método bastante popular y que aparentan ser inofensivo. Este virus tampoco busca hacer daños al equipo infectado, si no, "tomarlo prestado". Los ataques DoS es algo a lo que muchas empresas se ven expuestas, en estos los atacantes buscan "detener" el servidor de la empresa por medio de una sobrecarga de peticiones web, para lograr esto es necesario que el atacante disponga de una gran cantidad de dispositivos que se conecten simultaneamente al servidor y una forma de hacerlo es mediante las botnets o redes de equipos "zombi". Estas redes zombis son dispositivos infectados que están a la espera de una orden, que por lo general únicamente consiste en un comando para conectarse consecutivamente a una dirección web concreta. Las botnets grandes consiguen miles y miles de equipos infectados, con los cuales son capaces de generar grandes cargas, suficientes para hacer colapsar servidores si estos no cuentan con una medida de protección adecuada. Los dispositivos que confirman la red zombi por lo general son equipos personales como computadoras o celulares, e incluso dispositivos IoT. El virus en estos equipos es imperceptible ya que pasa "dormido" hasta el momento donde llega la orden del atacante, una vez terminado el trabajo vuelve a ponerse en modo espera hasta la siguiente orden.

Los ataques con **spyware** son un método comúnmente usado contra empresas o entidades públicas. Estos programas tienen como objetivo el robo de información confidencial o sensible que este almacenada en el dispositivo, incluso algunos pueden llegar a tomar control de la cámara web o micrófono del dispositivo con fines de espionaje. Estos virus por lo general buscan ser imperceptibles ante los usuarios, por lo que no realizan cambios evidentes en el sistema.

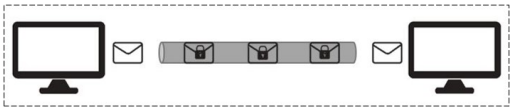
Otro tipo de ataque en general orientado generalmente a empresas son los **ransomware**. Estos virus "secuestran" los archivos del computador, generalmente estableciendo una contraseña para poder acceder a ellos, y luego dejan una nota donde se exige un pago monetario para recuperarlos. Usuarios comunes también son víctimas de este tipo de ataque, sin embargo, si no se tiene documentos tan importantes basta con formatear el equipo para no dejar rastro del virus, por otro lado, en empresas muchas veces estos documentos son de vital importancia y es necesario recuperarlos por lo que terminan realizado el pago requerido por los cibercriminales.

En general, una forma sencilla de protegerte de los virus es instalando un **antivirus** en tus equipos, algunas opciones pueden ser AVAST, AVG o Norton. Otro consejo para evitar que tu computador se infecte con estos virus es evitar descargas de sitios no oficiales. Por último, en el peor de los casos donde tu equipo se llegase a infectar y tengas que formatearlo, es aconsejable llevar un respaldo de la información de forma periódica para minimizar los datos que puedas llegar a perder en caso de ser vulnerado.

El phishing: de qué se trata y como evitar caer en este tipo de estafas

En este tipo de ataques una persona adquiere una identidad falsa, como un representante de un empresa o entidad, que se contacta con el objetivo de reportarte algún inconveniente y que te ayudará a resolverlo, pero su único objetivo será robarte tu información. Muchas veces podrás encontrar en tu correo electrónico mensaje con títulos como "has sido acreedor", "has sido seleccionado", "tu encarga a sido retenido" o "tu cuenta ha sido vulnerada", incluso podrás recibir mensajes de texto, llamadas telefónicas o contacto a través de redes sociales con estos mismos patrones, donde te piden que para poder continuar con el proceso respondas con información personal, contraseñas o incluso datos bancarios. En caso de que detectes uno de estos casos y tengas dudas lo mejor será contactarte directamente con la organización a través de sus medios oficiales. Nunca abras los archivos ni enlaces que te puedan enviar ya podrían contener algún malware o llevar a una página falsa.

Las VPN: como estas ayudan a la seguridad de mi información



Una VPN es una red privada virtual, la cual se usa para ocultar nuestra identidad en el internet creando un canal entre nosotros y el servidor a donde deseamos acceder donde el proveedor de la VPN hará de intermediario estableciendo un canal de comunicación seguro. Cuando nos conectamos a través de una VPN esta se encarga de la cifrar toda la información entrante y saliente de nuestra red, incluso nuestra dirección será escondida y saldremos a internet a través de una dirección propia de nuestro servidor de VPN. Cabe tener en cuenta que el proveedor de VPN será el que administre toda la seguridad de la comunicación, lo que incluye la encriptación de nuestros datos, por lo que es recomendable que al contratar un servicio de VPN este incluya un contrato o certificado donde se asegure la confidencialidad de la información.

Apéndice G: Artículo divulgativo elaborado n°6

El periódico

Año 2023 Febrero Ciudad, Guayaquil

Seguridad informática dentro y fuera de oficina

por Christian Ramos

Debido a las exigencias de su trabajo, es probable que este familiarizado con términos informáticos como WiFi. Maneje habitualmente la computadora, el teléfono celular y tenga estos dispositivos configurados con una contraseña. Tal vez, le interese conocer un poco más sobre conceptos y técnicas de seguridad informática, ya que usa Internet a diario para sus actividades laborales principalmente.

¿Si se encuentra en su trabajo, qué puede hacer?

Es muy importante que sepa usar las tecnologías y herramientas que tiene a su disposición. Pero antes de eso, lo primero que debe hacer es **separar su información**. Evite mezclar sus datos personales y laborales. Compartir informacion en ambos ambientes hace más probable que sean robados. Si tiene la posibilidad, es sumamente recomendable tener un dispositivo para uso personal y otro exclusivo para su trabajo. Otra opción que ofrecen ciertas empresas para dividir su información, es la configuración de un portal empresarial. Un portal empresarial es una aplicación que le permite configurar perfiles en sus dispositivos. Además, le permitirle el acceso seguro a los recursos y servicios privados de la compañía. Adicionalmente, si se le asigna un correo institucional, uselo unicamente para temas laborales. Cuanto **¡menos comparta mejor!**

Si hace uso constante del correo, la amenaza más frecuente es el **phishing**. Esto consiste en el engaño donde el cibercriminal se hacen pasar por otra persona, entidad o servicio legítimo para solicitarle que realice acciones que terminan en el robo de información personal, laboral o bancaria. Por eso, usted debe siempre verificar la dirección de correo del emisor tal. Otra recomendación es revisar la gramática y redacción del mensaje. Si observa agresividad o urgencia, como: «Si no ingresa a ... »,«Responda ahora mismo este correo para ... »; empiece a sospechar. Generalmente, estos correos falsos traen adjuntos links o archivos, así que **nunca** los abra. Al final del día el sentido común es su mejor arma: Si algo parece raro es probable que lo sea. El personal técnico de la empresa esta ahí para ayudarlo. **¡No dude en consultarles!**

Otra herramienta que probablemente use a diaro en el trabajo, es "la nube"... Pero, ¿Qué es "la nube" ? Pues lo principal que debe saber es que esta le permite acceder a sus archivos y aplicaciones en cualquier momento y desde cualquier dispositivo electrónico con conexión a Internet. ¿Cuándo hacemos eso? Cada vez que guardamos o compartimos un archivo en *OneDrive*, *Google Drive*, *DropBox* o *incluso WhatsApp*. También cuando trabaja en un archivo de texto o una hoja de cálculo con un compañero. "La nube" es buena porque es confiable ya que es practicamente imposible que su información se pierda. Sin embargo "la nube" esta en Internet y debemos tener unas consideraciones al usarla. La más imporante es la configuración de permisos. Al estar su información en Internet debe limitar quienes pueden ver y editar sus archivos. Si comparte información laboral limite el acceso solo para mienbros de su organización. Si la informacion es familiar unicamente a los miembros de la familia. Finalmente otra técnica de seguridad que puede implementar es asegurar sus archivos con contraseña o establecer un límite de tiempo para que el archivo sea visible.

Por otro lado, si usted es de los que lleva el trabajo a todos lados, también debe estar alerta donde se encuentre.

¿Sabe qué hacer para estar protegido fuera de oficina?

Lo primero que debería saber es que no todas las redes que permiten acceder a la web son seguras, en especial las públicas como las que puede encontrar en parques, centros comerciales o aeropuertos; si se encuentra en un establecimiento como un restaurante pregunte por la red oficial del lugar. Una buena costumbre es **siempre priorizar el uso sus datos móviles**. Usted controla esta conexión y por lo tanto tiene más seguridad. En caso de no contar con este servicio, procure acceder a las redes abiertas para realizar actividades de poca relevancia como leer un mensaje, buscar algo en *Google* o tal vez acceder a *YouTube*. **Nunca** intente iniciar sesión en alguna página o revisar su información bancaria. Tenga en cuenta que todo mundo tiene acceso a las redes libres, por lo que es probable que alguien pueda estar monitoreando su comunicación. Además, recuerde que los lugares públicos se caracterizan por estar llenos de personas, así que no deje ver lo que hace en sus dispositivos y peor aún los deje descuidados, esta es una forma sencilla pero efectiva de robar información.

El en peor de los casos, si su dispositivo llegase a perderse o sustraerse, otra configuración de seguridad importante es el cifrado (disponible como: Bitlocker en Windows o FileVault en MacOS). Lo que logra con ello es bloquear el acceso no autorizado a su disco local mediante una contraseña. De esta manera, quien quiera que busque acceder a la información de su disco local deberá ingresar ese contraseña que usted mismo configuró. Tenga en cuenta que esta configuracion de seguridad también es posible realizar en teléfonos celulares o unidades de almacenamiento externas como un Pendrive.

Usted es el responsable del manejo y cuidado de su información. Los peligros de Internet se encuentran dentro y fuera de su lugar de trabajo, por lo que es importante que los conozca para poder enfrentarlos. Si requiere más información sobre seguridad informática, le invitamos a leer otros artículos de esta serie sobre ciberseguridad.

¡Recuerde! cuanto más sepamos los usuarios, más seguro estarán nuestros sistemas.

Apéndice H: Artículo divulgativo elaborado n°7

El periódico

Año 2023 Febrero Ciudad, Guayaquil

Ciberseguridad empresarial

por Bryan Chunga y Christian Ramos

Como empresa debe tener un control total y manejo responsable del área tecnológica existente en su compañía. Debido a la gran extensión de la organización y numerosos usuarios, es mejor que cuente con su propio departamento de sistemas, personal profesional encargado del área informática. Esta y otras recomendaciones son a continuación mostradas como una guía de ciberseguridad empresarial que debería conocer y aplicar para mantener a salvo su infraestructura tecnológica de las amenazas existentes.

La **infraestructura tecnológica**, es un punto crucial para el buen funcionamiento de su compañía. Antes de adquirir un nuevo equipo de comunicación o final, primero realice un análisis previo, donde pueda conocer puntos relevantes, así podrá hacer una elección más acertada de equipos. Evite adquirir equipos que no cumplan con sus exigencias por ahorrar costos, mejor véalo como una inversión para su empresa.

Las **aplicaciones de Machine Learning**; son otra solución viable para mejorar la seguridad de redes y equipos informáticos, sobre todo para implementar métodos de prevención contra formas de ataque frecuente. Algunas de las aplicaciones más usadas para este caso son sistemas de detección de intrusos, anomalías y soluciones para servicios de mensajería que ayudan a prevenir phishing o spam. Las aplicaciones de machine learning para los sistemas IDS generar una alerta a los encargados de seguridad sobre la detección de una conexión no autorizada en el sistema de forma temprana, de esta forma estos podrán tomar las medidas pertinentes para evitar que el atacante lleve a cabo su cometido. Por otro lado, los sistemas para detección de anomalías se centran en el análisis del comportamiento de la red, los que permite alertar sobre intentos de ataques de tipo DOS, este tipo de soluciones son muy usados por los proveedores de internet y de servicios en nube. Otras aplicaciones son los sistemas de detección de pishing o spam, los cuales son comúnmente implementados dentro del servicio de correo electrónico institucional de muchas empresas. Muchos proveedores de servicios de correo como G Suite (Google) o Office 365 (Microsoft) ofrecen estas soluciones en su servicio, y algunos como ProtonMail van más allá aumentando medidas de cifrado extremo a extremo que aumentan la seguridad.

"Construyendo confianza en un cielo nublado", McAfee. Muchas **soluciones en nube** han tenido acogida gracias a las ofertas de disponibilidad e infraestructura a todo tipo de escalas, por lo que muchas empresas han tomado la decisión de llevar sus plataformas a este tipo de servicios como el Amazon Web Services (AWS) o Google Cloud Platform (GCP). La seguridad de la información es uno de los puntos en contra que tuvieron durante sus inicios, y es que muchas personas no depositaban toda su confianza en poner información crítica en la nube. Debido a esto las plataformas proveedoras de servicios en nube han regido sus métodos de seguridad en diferentes campos, enfocándose sobre todo en la protección contra fugas de los datos de sus clientes, implementación de sistemas de gestión y acceso seguros, y gestión de planes de contingencia en cuanto a conectividad y respaldo de información, todo esto siguiendo diferentes marcos de gobernanza de tecnologías de información. Entre los sistemas de prevención con los que cuentan los proveedores de nube también se encuentran sistemas de detección de anomalías en red, por lo que también es capaz de detectar posibles ataques o intrusiones, lo cual permite la generación de una alerta para una rápida toma de acción o incluso la ejecución de una contramedida de seguridad de forma automática. Sin embargo, se debe tener en cuenta que la responsabilidad de la seguridad de una plataforma en nube es compartida entre el proveedor y los clientes que alojar sus servicios en él. El proveedor se encarga sobre todo de la integridad física de la información alojada y la gestión de seguridad de la red. La empresa que usa el servicio en la nube será totalmente responsable de como esta gestiona los permisos de acceso de los usuarios a dicha plataforma y de toda la configuración de esta. En otras palabras, el proveedor es responsable de garantizar la seguridad de la infraestructura, mientras que el cliente deberá ser responsable de la seguridad del servicio que ofrece dentro de dicha infraestructura.

Por último los **pentest** son pruebas que se llevan a cabo para encontrar posibles fallos o brechas de seguridad dentro de una red o un sistema informático. Estas pruebas son llevadas a cabo por un auditor en ciberseguridad y a través de ellas una empresa puede identificar vulnerabilidades y corregirlas de manera efectiva con el fin de salvaguardar la integridad de la información de sus equipos. Existen tres métodos para realizar las pruebas de penetración y se denominan test de caja blanca, gris y negra. Los test de caja blanca son realizados generalmente por un miembro interno del equipo de sistemas informáticos con el conocimiento completo de la infraestructura a evaluar. Este tipo de prueba es más analítica y consiste en un análisis integral del sistema auditado, donde gracias al conocimiento que tiene el auditor es posible evaluar posibles mejoras o integraciones a implementar. El test de caja negra son un escenario mas real de la prueba de penetración. Son realizados por un auditor externo, totalmente ajeno a la empresa y sin ningún conocimiento previo del sis-

tema a auditar. Es un trabajo más técnico ya que tendrá que analizar todas las áreas y posibles vulnerabilidades existentes desde cero, lo que permite recrear las posibles acciones que cualquier ciberdelincuente podría efectuar. Hacer un pentest desde cero es un proceso que lleva mucho tiempo, sobre todo en las fases iniciales donde el tester se dedica a recabar toda la información posible, la cual muchas veces es muy básica y sirve únicamente para determinar una estrategia de ataque. Es por esto que existen los test de caja gris, donde se le brinda al auditor información básica limita con el fin de que este no pierda tanto tiempo en la fase de obtener información sobre la infraestructura a auditar y pueda entrar directamente en la fase de planeación y estrategias para el ataque. Para poder hacer un correcto análisis es recomendable realizar un test de caja blanca en conjunto con un test de caja gris o negra. Realizar un test de tipo caja blanca permite a los miembros internos responsables del sistema o la red evaluar todo tipo de posibles soluciones y tener un panorama completo sobre la estructura lo que facilita la toma de decisiones sobre las medidas a tomar frente a los resultados de las pruebas de tipo caja negra o gris.

La **información** que maneja la empresa debe recibir un tratamiento especial. Muchas veces, debido a la confidencialidad o sensibilidad debe manejar varios filtros de seguridad, limitando el acceso solo al personal calificado para conocer del tema. Imagine lo que puede ocurrir si llega a caer en manos equivocadas, exponer al público información que perjudicaría la imagen de su empresa, o talvez beneficiar a sus competidores. También haga respaldos, realizar copias periódicas de sus datos le ayudará a recuperar su información en caso de daño o perdidas.

Por último, **¡recuerde!** que el eslabón más débil de la ciberseguridad es el humano. De nada sirve que cuente con lo último en tecnología y seguridad informática sino se sabe usar, por lo que todo el personal laboral debe ser capacitado en el uso de tecnologías e Internet. Algunas consideraciones esenciales que debería tener con sus empleados: Mantengan bajo contraseña todos los equipos provistos por la empresa, límite el rango de sitios web que puedan visitar. El desconocimiento del personal sobre ciberseguridad puede hacer que entren en sitios webs no seguros, descarguen un archivo con un algún tipo de virus o abran un correo malicioso. Siempre que desvincule un empleado de su empresa realice una copia de la información más relevante que posea y posteriormente de su baja de usuario, correo y demás. Si desea tener más información sobre ciberseguridad básica para su personal le podría interesar nuestra serie de artículos sobre ciberseguridad.