Estrategias para la concienciación en seguridad de la Información en la Familia

Strategies for awareness of Information Security in the Family

Jonathan Fabian Mendoza Moreno

Luis Orlando Valbuena Carvajal

Oscar Javier Morales Varón

Yenny Isabel Serrato Rodríguez

RESUMEN

La evolución de la tecnología y la dependencia directa o indirecta nos ubica hoy en día, en una conectividad constante, las noticias reportadas por entidades de gobierno o privadas, encargadas del monitoreo de la seguridad de la información y ciberseguridad, evidencian un flujo cada vez mayor de ataques o intentos de ataques orientados a comprometer Confidencialidad Integridad y/o Disponibilidad – CID, estos tres conceptos son conocidos como: la triada de la seguridad de la información, esto, genera una alerta para los usuarios de la tecnología, pues estos eventos, tienen como objetivo principal acceder de forma ilícita a dispositivos, aplicaciones y en general, a los sistemas de información para obtener los datos personales de las víctimas, para hacer uso de ellos en escenarios de chantaje por secuestro de datos, divulgación de información sensible, suplantación de identidad durante el acceso a cuentas bancarias o billeteras virtuales para sustraer fondos entre otros, generando un impacto a nivel económico, social y reputacional.

Usualmente las personas desconocen los riesgos a los que se exponen con el uso diario de las tecnologías y la evolución constante de los métodos con los cuales se ejecutan los ataques, lo anterior, acompañado de un desconocimiento generalizado en cuanto a la importancia de la seguridad de la información personal o familiar y las medidas de control que pueden implementar para garantizar en cierta medida la seguridad de la información

Los métodos de seguridad como los que implementan los proveedores tecnológicos de internet, que normalmente son básicas y estándar a la hora de configurar los servicios en cada hogar, lo cual es desconocido por el usuario final y facilita el trabajo al ciberdelincuente pues este conoce las vulnerabilidades de estos servicios.

En este artículo, se pretende identificar el nivel de conciencia de los riesgos asociados al uso de las tecnologías, también generar materiales como:

documentos, boletines, videos, entre otros, para incentivar el pensamiento preventivo para minimizar la probabilidad y el impacto ante la materialización de un evento que pueda llegar a comprometer la CID de los sistemas y/o información.

Palabras clave: Estrategias, ciberseguridad, defensivo, ciberdelincuente, conciencia.

ABSTRACT

The evolution of technology and direct or indirect dependence on it, brings us today, in a constant connectivity, the news reported by government or private entities, responsible for monitoring the security of information and cybersecurity, show an increasing flow of attacks or attempted attacks directed to compromising confidentiality Integrity and / or Availability - CID, these three concepts are known as: the triad of information security, generating an alert for technology users, these events, have as main objective to illicitly access devices, applications and in general, information systems to obtain the personal data of the victims, to make use of them in scenarios of blackmail by data kidnapping, disclosure of sensitive information, supplanting identity, during access to bank accounts or virtual wallets to subtract funds and others, generating an economic, social and reputational impact.

Usually people are unaware of the risks to which they are exposed with the daily use of technologies and the constant evolution of the methods with which attacks are executed, the above, accompanied by a generalized lack of knowledge regarding the importance of the security of personal or family information and the control measures that can be implemented to ensure information security methods.

Security methods such as those implemented by Internet technology providers, which are normally basic and standard when setting up services in homes, are unknown to the end user and this makes the cybercriminal's job easier because they know the vulnerabilities.

In this article, we pretend to identify the level of awareness of the risks associated with the use of technologies, also to generate resources such as: documents, bulletins, videos, and others, to encourage preventive thinking to minimize the probability and impact before the occurrence of an event that may compromise the CID of the systems and/or information.

Keywords: Strategies, cybersecurity, defensive, cybercriminal, awareness.

1. INTRODUCCIÓN

En la actualidad en familias colombianas sin importar la edad de quienes la conforman, se desconocen los riesgos que pueden comprometer o exponer la confidencialidad, integridad, disponibilidad de la información cuando se procesa o almacena en dispositivos como celulares, Tablet, Equipos de Escritorio, Portátil o Smart TV, en el país, hoy en día un alto porcentaje de hogares cuentan con internet (70% según el DANE). Estar conectados se vuelve una necesidad cada vez mayor (clases virtuales, uso de redes sociales, visita a páginas de interés, transacciones bancarias, compras en línea, etc.), los ciberdelincuentes buscan explotar las debilidades de los sistemas de información, con el objetivo de acceder de forma ilegal a los sistemas de información y/o dispositivos, este escenario genera la necesidad de crear estrategias para fortalecer el nivel de conciencia en seguridad de la información y ciberseguridad.

En respuesta a este escenario se investigara para documentar en el desarrollo de este artículo, estrategias para la concienciación en seguridad de la información, representadas en contenidos dirigidos a las familias colombianas, como: documentación de noticias, documentos de interés generados por actores relevantes en el medio de seguridad de la información y ciberseguridad, como el ministerio de las Tecnologías de la Información, La Cámara Colombia de Informática y Telecomunicaciones, el COLCERT, INCIBE entre otras , videos, charlas y ejercicios de capacitación, con el fin de crear conciencia en la prevención de los riesgos antes mencionados.

Para obtener un diagnóstico que permita identificar el nivel de concienciación en seguridad de la información y ciberseguridad, la interacción con internet, redes sociales y algunos conocimientos básicos sobre la legislación asociada a datos personales en Colombia, se

aplicará una encuesta dirigida a las familias de los integrantes del grupo de trabajo y a los estudiantes compañeros del grupo de la especialización en seguridad de la información, para llevar a cabo la recolección de datos inicialmente se determina una política de protección de datos alineada a los requerimientos de la ley 1581 y decretos reglamentarios.

Hoy, es común ver noticias relacionadas con ataques informáticos que generan impacto a los colombianos, lo anterior, sumado a la nueva realidad de los hogares consecuencia de la virtualidad y el desarrollo de las actividades comunes del día a día.

como parte de su día pues no están exentos de sufrir un ataque que afecte la seguridad de la información, esto basados en los cambios introducidos por la pandemia, pues muchas de nuestras actividades pasaron a la virtualidad, realizando actividades como uso de las redes sociales, videollamadas, reuniones laborales o familiares por medios virtuales, transacciones no presenciales (bancarias-compras) entre muchas más, lo anterior nos vuelve un blanco para los ciberdelincuentes debido al poco o nulo conocimiento en lo relacionado con seguridad de la información y ciberseguridad.

Las familias están compuestas personas de diferentes edades, quienes a su vez interactúan con la tecnología sin un conocimiento previo o con un mínimo, el cual puede ser básico o limitado al momento de analizar y tomar decisiones frente a los eventos que se puedan presentar en la interacción con la web y las redes sociales, esto, puede comprometer al dispositivo, la información y hasta la integridad de los usuarios.

También se realiza un análisis previo dentro de los grupos interesados con el propósito de evidenciar el nivel de conocimiento e interacción con internet y redes sociales, para luego simular herramienta con la finalidad de almacenar el contenido generado.

2. REFERENTES TEÓRICOS

Para el desarrollo del proyecto, se toman como referentes las normas relacionadas con seguridad de la información como ISO 27001:2013, gestión de riesgos como la ISO 31000:2018, también se tuvo en cuenta la normatividad legal vigente en Colombia como: Articulo 15 de la Constitución Política de Colombia, Ley 1581 de 2012, decretos reglamentarios 1377 de 2013, 886 de 2014 y 1081 de 2015.

En desarrollo de la investigación soportado en conocimientos previos adquiridos durante el ejercicio laboral podemos encontrar el programa " En Tic Confío + (MinTic, 2022)" https://www.enticconfio.gov.co/ este portal web expone contenido relacionado con seguridad de la información y ciberseguridad a través de videos con tips, academias, con un contenido general, el cual puede llegar a no ser fácil de entender para los colombianos y también lucha con el desconocimiento general de su existencia por tener un enfoque global en cuanto al público objetivo.

También se tiene como referente el juicio experto en seguridad de la información y ciberseguridad, generado por la experiencia profesional, pues este contexto ha permitido gestionar escenarios desfavorables en el proceso de cultura y conciencia por parte de los involucrados en un SGSI.

3. METODOLOGÍA

Es importante que las familias conozcan y entiendan la criticidad que tiene la información y cómo posiblemente influye en la vulneración de su privacidad. para ello es necesario conocer la Ley 1581 de 2012.

En cuanto esta Ley y sus decretos reglamentarios antes mencionados se realizará un análisis para determinar los conceptos mínimos que deben abordar los contenidos a desarrollar. (Pública, 2012)

Respecto a la ISO 31000:2018 el análisis determinará conceptos mínimos de gestión de riesgos para aportar herramientas orientadas a facilitar la ejecución de análisis de riesgos en la toma de decisiones. (ISO, 2018)

Inicialmente, se plantea determinar la necesidad de generar estrategias para la concienciación en seguridad de la información en las familias, identificando si el contenido se enfoca en sensibilización, capacitación o concienciación en seguridad de la información, lo anterior, a partir del entendimiento de las diferencias entre estos tres conceptos.

Una vez identificado el enfoque se desarrollará una encuesta inicial en la cual se busca en general, establecer el nivel de concienciación en seguridad de la información y ciberseguridad, estará dirigida a las familias para identificar el interés en temas relacionados a la seguridad de la información, evaluar conocimientos previos, se plantearán preguntas con relación al uso de la información en redes sociales, páginas de interés, uso de navegadores, uso de redes sociales por parte de menores de edad entre otras, lo anterior permitirá medir el nivel de conciencia, pensamiento y actuación segura frente a posibles eventos.

En paralelo, se realizará el análisis de la cláusula 7.3 Toma de Conciencia y el Dominio A7 de la ISO 27001:2013, para determinar su aplicabilidad y aporte al logro de los objetivos propuestos en el proyecto. (ICONTEC, 2013)

Una vez determinados los contenidos a publicar, se analizará la información recopilada para identificar las limitaciones como restricciones, derechos de autor y supuestos, lo anterior respecto a los documentos de interés, también la forma de abordar los contenidos propios para clasificar cuales se tratarán como noticias, infografías y videos.

4. RESULTADOS y DISCUSIÓN

4.1. Análisis

El análisis del numeral 7.3 TOMA DE CONCIENCIA de las cláusulas de la norma NTC-ISO/IEC 27001:2013, (ICONTEC, 2013) permite determinar la orientación del requisito hacia la generación de acciones para la toma de conciencia, cuando una organización implementa o mantiene un Sistema de Gestión de Seguridad de la Información – SGSI. Se hace evidente el enfoque empresarial, sin embargo, puede generar aportes para salvaguardar la información de las familias, recordando que el numeral 5.2 indica la necesidad de crear una política para la seguridad de la información; la definición de una política familiar puede generar una directriz de conciencia frente a la necesidad de pensar en dónde, quién, cómo y cuándo, se almacena y trata la información de cada integrante.

Con respecto al análisis y relación que tiene la ley 1581 con la estrategia planteada durante la realización de este proyecto, se determinan los puntos relevantes a tratar en los contenidos, en primera instancia se puede abordar el concepto de la autorización por parte del titular de los datos, se efectúa a través de una autorización para el tratamiento de datos personales, la cual puede o no ser aceptada y se concibe para contar con una evidencia para el tratamiento de los datos.

Otro concepto es base de datos, hace referencia a todo dato organizado objeto de tratamiento; el termino dato personal, hace referencia a la información vinculada directamente a una persona. Con el análisis surge otro concepto, encargado del tratamiento, es la persona de naturaleza privada quien por cuenta propia o encargo del responsable lleva a cabo el tratamiento de la información o datos suministrados por el titular, este se refiere a toda persona natural cuyos datos sean objeto de tratamiento, otro actor es el responsable del tratamiento, se determina como la persona de naturaleza privada que decide sobre la base de datos y el tratamiento de los mismos.

Con lo anterior, se genera conciencia para que las personas de a pie, requieran a las organizaciones que almacenan, procesan o transforman su información, el mantenimiento de controles de seguridad durante el desarrollo de su actividad de tratamiento de datos personales, como por ejemplo el manejo de la información médica por parte de las entidades prestadoras de servicios de salud. Otro actor, pueden ser las instituciones de educación en general, pues estos obtienen acceso a datos semiprivados, privados o sensibles, por lo cual tienen el deber legal de proteger en todo momento y por tiempos determinados en la ley, hasta realizar una disposición final segura de la información.

Para el planteamiento de las preguntas se referenciaron temas generales en seguridad de la información y que hacen parte de la interacción que tienen las personas con el uso de la tecnología, redes sociales, navegadores, páginas web, contraseñas, configuraciones de seguridad y uso adecuado de los dispositivos, protección de datos personales, antimalware y el control sobre el uso de la tecnología por parte de menores de edad.

4.2. Discusión

Para dar continuidad al ejercicio, se hace necesario crear la estrategia de cambio de mentalidad soportado en la generación de contenidos, creados en respuesta a las necesidades identificadas en la encuesta, con el fin de facilitar la adopción de las buenas prácticas en seguridad de la información y conocimiento sobre los derechos otorgados por la legislación sobre protección de datos para las familias colombianas, en un lenguaje más cercano a la cotidianidad.

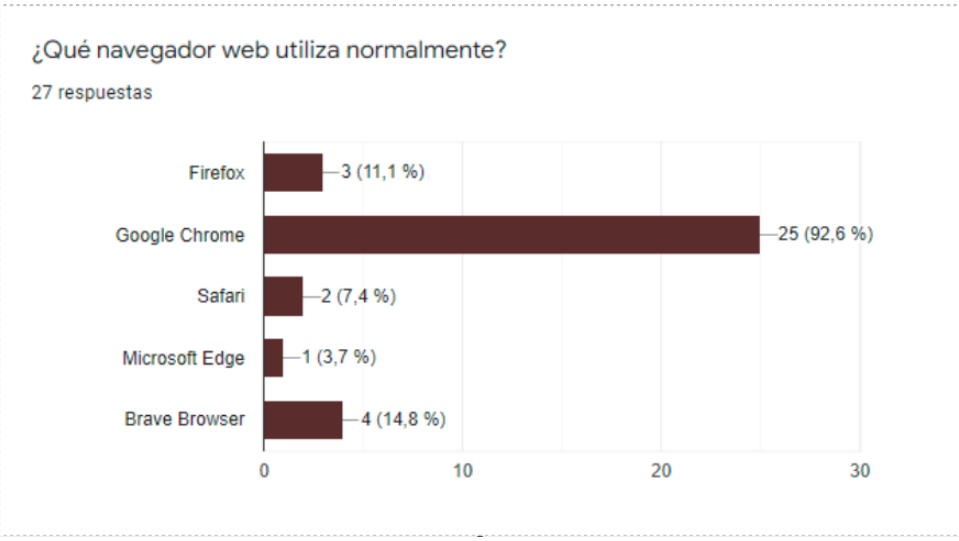
Ilustración 1
Identificación de páginas web seguras.

Nota: Resultado a la pregunta ¿Sabes cómo identificar si una página web es segura? realizada en la encuesta.

Al consultar a los encuestados, respecto a si tienen conocimiento de cómo identificar un sitio web seguro, se evidencia que un gran porcentaje de los encuestados no tienen conocimiento

referente a la identificación de una página web segura, resultado que permite trabajar en la creación de contenidos relacionados con tips para identificar si un sitio web es seguro, como: video sobre las características de seguridad en sitios web, infografía de técnicas para identificar escenarios de suplantación de sitios web.

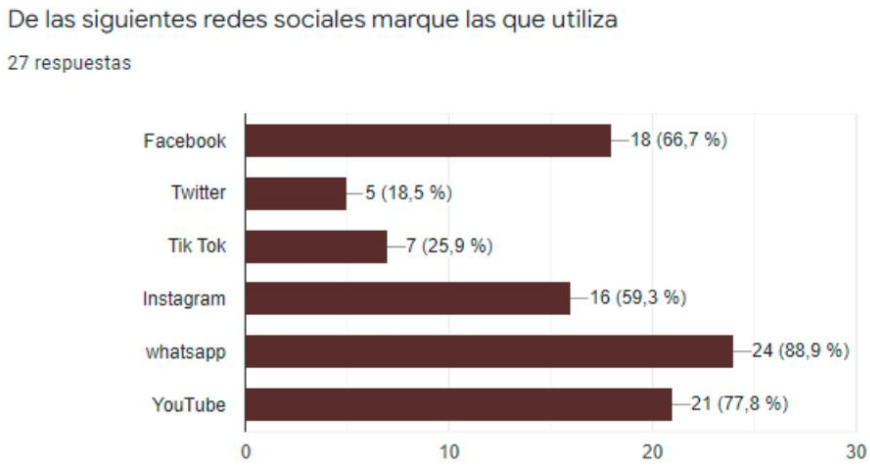
Ilustración 2
Navegador web utilizado normalmente.



Nota: Resultado a la pregunta, ¿Qué navegador web utilizas normalmente? realizada en la encuesta.

Esta pregunta permite reconocer las preferencias con relación al uso de navegador web al momento de acceder a internet, con base en estas respuestas se pueden generar contenidos con ejemplos y ejercicios del paso a paso para configurar la seguridad del navegador, validación de versión y actualización y manejo de extensiones.

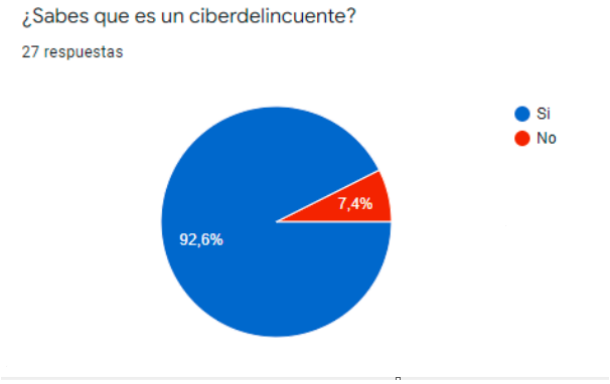
Ilustración 3
Uso de redes sociales..



Nota: Resultado de las respuestas referente a las redes sociales que utilizan.

La grafica anterior permite conocer las redes sociales que normalmente utiliza el público encuestado, para idear contenidos encaminados a fortalecer el conocimiento con relación al uso responsable y el aseguramiento de las redes sociales, como: Conceptos de seguridad a través de gamificación cómo sopa de letras, ordenar por grupo, crucigrama, configuración de segundo factor y/o bloqueo de ubicación automático.

Ilustración 4
Ciberdelincuente



Nota: Resultado a la pregunta ¿Sabes que es un Ciberdelincuente? realizada en la encuesta.

Aunque el 92% de los encuestado afirma saber que es un Ciberdelincuente, es importante abordar contenidos para generar conciencia sobre el modo de actuar, tipos de ataque y escenarios que pueden favorecer al ciberdelincuente, para fortalecer los conceptos relacionados con seguridad de la información y ciberseguridad en las familias.

Ilustración 5
Nivel de seguridad en contraseñas de acceso.

Nota: Resultado a la preguntas relacionadas con el nivel de seguridad de las contraseñas usadas para acceder las redes sociales.

Es vital hacer énfasis en la importancia de tener contraseñas robustas en las cuentas utilizadas en internet y/o aplicaciones, a partir del resultado de la encuesta, en donde se evidencia que un 33% de los encuestados considera que la contraseña no es segura y el 29.6% desconoce cómo definir una contraseña segura, se pueden generar contenidos para guiar al usuario en la definición y administración segura de contraseñas, a través de infografías que incluyan características como: Cantidad mínima de caracteres, Periodicidad de Cambio, Herramientas para gestión centralizada de contraseñas, sugerencias para evitar almacenar contraseñas en los navegadores web.

Ilustración 6

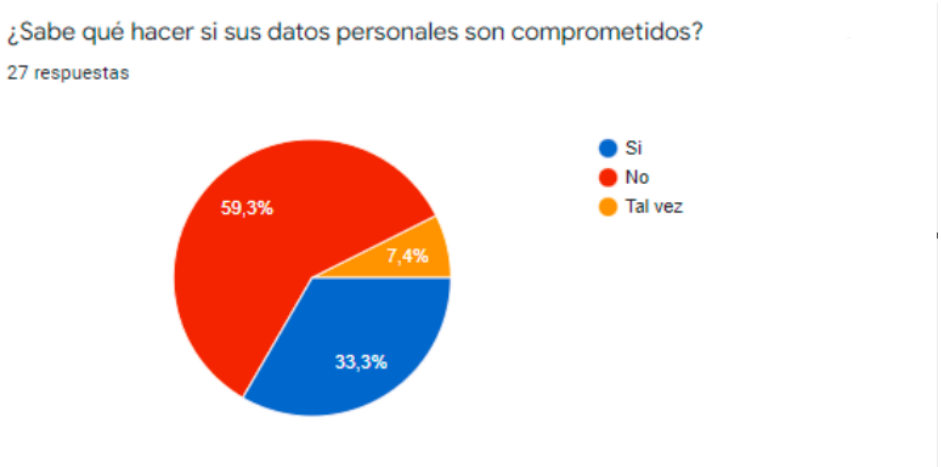
Configuración de seguridad en las redes sociales

NOTA: Resultado a la preguntas de configuración de seguridad en las redes sociales.

En las preguntas relacionadas con la configuración y uso de seguridad en las redes sociales, se evidencia que la mayoría de los participantes, indican no conocer como configurar o aumentar la seguridad en el control de acceso a las redes sociales, este escenario es favorable para la generación de videos que oriente al usuario en el fortalecimiento de la seguridad del acceso y privacidad en redes sociales.

Ilustración 7

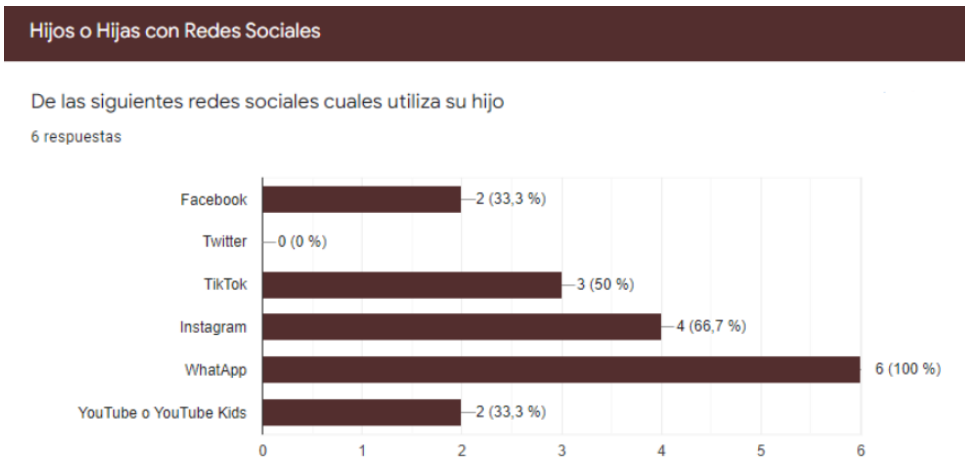
Compromiso de los datos personales.



NOTA: Resultado a la pregunta ¿Qué hacer si sus datos personales son comprometidos? realizada en la encuesta.

Esta pregunta permite identificar un 59.3% de desconocimiento en temas asociados a protección de datos personales y las condiciones que favorecen a dueño de la información ante escenarios de vulneración o incumplimiento de la ley, se pueden fortalecer estos vacíos con artículos y ejemplos que faciliten la comprensión y aprendizaje de los derechos de los titulares y las obligaciones de los responsables o encargados del tratamiento de datos, para generar conciencia en las personas que integran las familias.

Ilustración 8
Hijos y el uso de redes sociales.



NOTA: Resultado a la pregunta relacionada con el control de uso de redes sociales por parte de los hijos.

La seguridad de la información de los más pequeños en casa debería ser lo primordial, sin embargo, en la actualidad, el comportamiento de los padres es el de facilitar el acceso de los menores a redes sociales a muy temprana edad, esto acompañado de un bajo nivel de control y supervisión de las actividades en la interacción de los menores con la tecnología.

Este comportamiento facilita el actuar malicioso en las redes sociales e internet, para cerrar esta brecha se generan tips sobre aplicaciones para el monitoreo desde el rol de padres y/o administrador del uso de la tecnología en casa.

Este ejercicio de investigación y recolección de datos muestra la interacción casi rutinaria con la tecnología, en un contexto de parcial desconocimiento de los riesgos a los que se está expuesto, facilitando el trabajo a los ciberdelincuentes quienes tienes como objetivo explotar las vulnerabilidades a nivel técnico (hardware y software) o a nivel de conciencia con ejercicios de ingeniería social.

El análisis de los resultados de la encuesta, evidencia el nivel de conciencia de las familias, para determinar los contenidos que se plasmaran en Infografías, boletines de noticias o artículos y videos, abordando temas como:

Artículos o Noticias

La importancia de la seguridad informática en casa; backups y su importancia; cinco tips en la seguridad de la información; cinco principales ataques en el 2022; cómo analizar tu red; diferencias entre Ciberseguridad y Seguridad de la información; ¿Sabes realmente qué pasa con tu información en la red?

Infografías

Sugerencias de seguridad para redes sociales; tips sobre transacciones seguras; Resumen de una noticia o eventos sobre seguridad; píldoras informativas.

Videos

Contenido didáctico que genere interés y permita el fácil entendimiento de temas como:

Higiene digital; como actúa un Malware; uso de doble factor de autenticación; como habilitar el doble factor en Redes Sociales; Sugerencias para la configuración de notificaciones en banca virtual personal.

En general es destacable la ausencia de cibercultura, pues en la interacción con la tecnología, no se muestra interés por investigar y adquirir conocimientos sobre el uso y derechos del titular de la información personal o familiar y canales de ayuda en caso de sufrir un ciberataque.

Esto coincide con las investigaciones realizadas por (Kemp, 2022) en la cual se evidencia que el factor predominante en la cibercultura en colombiana es el consumo de contenido de entretenimiento.

Ilustración 9
Sitios Web más Visitados en Febrero 2022.

Nota: Sitios web más visitados en el mes de febrero de 2022. Tomada de (Kemp, 2022). Diapositiva 34. https://bit.ly/3mfgGEr

Donde se evidencia, el flujo de consultas y visitas a internet, destacando, el contenido multimedia, redes sociales, sitios de apuestas y contenido para adultos. Estos factores intervienen directamente en la percepción de las familias sobre seguridad de la información, por lo anterior con el desarrollo de los contenidos propuestos se puede reducir la brecha de desinformación he impulsar la concienciación en seguridad de la información y protección de datos.

5. CONCLUSIONES

Es importante dar continuidad a este tipo de investigaciones con la ampliación la muestra poblacional, para identificar un mayor porcentaje de (des)conocimiento en seguridad de la información y protección de datos personales de cada uno de los miembros de la familia Colombia.

Los programas de Gobierno Nacional, Departamental y/o Distrital deben fortalecer las estrategias para el desarrollo de programas transversales que aborden contenidos sobre temas asociados a Seguridad de la información, Ciberseguridad, además de privacidad y protección de datos personales en busca de generar e impulsar en la adopción en Colombia de una cultura de pensamiento basado en el riesgo y el impacto del mismo en su día a día.

Las instituciones de educación superior deben fortalecer la estrategia de responsabilidad social, generando aportes de mayor relevancia, con el desarrollo de proyectos a cargo de los estudiantes de pregrado o posgrado, con el fin de generar un impacto social, que vaya más allá del objetivo de cumplir un requisito para culminar una formación profesional.

Se puede abordar el cambio de cultura personal en seguridad de información, clara muestra, es la estrategia aquí plasmada, que surge en respuesta a los resultados obtenidos por los análisis realizados, así las cosas, es posible crear diversos mecanismos de concienciación, capacitación y sensibilización al público en general, haciendo uso de diversos mecanismos de comunicación.

Mencionar que esto No es un trabajo individual y es un trabajo a largo plazo para llevar a Colombia a un estado básico de responsabilidad en el uso de los medios digitales. (identidad digital)

6. AGRADECIMIENTOS

El acompañamiento de la experiencia es relevante para el desarrollo de cualquier proyecto sin importar el ámbito de aplicación, por lo anterior agradecemos el apoyo brindado por los docentes de la especialización, en lo particular la guía de la Ingeniera Yenny Isabel Serrato Rodríguez.

También agradecemos a las familias por la motivación y apoyo constantes durante el desarrollo de la especialización y la compresión ante las limitantes de tiempo para las actividades en los espacios libres o de ocio generadas por la dedicación al proyecto.

7. GLOSARIO

Para poner en contexto al lector a continuación se detallan términos usados en el artículo

AUTORIZACIÓN
Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales 8

CIBERDELINCUENTES
Es una persona cuyo conocimiento informático le permite realizar acciones delictivas en Internet .. 3

CIBERSEGURIDAD
Conjunto de elementos, medidas y equipos destinados a controlar la seguridad informática de una entidad o espacio virtual. 1

COLCERT
El Grupo Interno de Trabajo de Respuesta a Emergencias Cibernéticas de Colombia 3

CONCIENCIACIÓN
Acción y efecto de crear conciencia entre la gente acerca de un problema o fenómeno que se juzga importante.....3, 6

CONFIDENCIALIDAD
Es el principio que garantiza que la información solo puede ser accedida por las personas que tienen autorización 1

DATO PERSONAL
Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables..... 8

DATOS SEMIPRIVADA
Dato que no tiene naturaleza íntima, reservada, ni pública y cuyo conocimiento o divulgación puede interesar no solo a su titular sino a cierto sector o grupo de personas o a la sociedad en general, como el dato financiero y crediticio de actividad comercial o de servicios..... 9

DISPONIBILIDAD
Asegura la fiabilidad y el acceso oportuno a los datos y recursos por parte de los individuos o personas autorizadas..... 1

DIVULGACIÓN
el acto de hacer pública una información que esté al alcance de todas las personas..... 1

ENCARGADO DEL TRATAMIENTO
Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del Responsable del Tratamiento..... 8

EVENTO
Indica que el sistema, la seguridad o los servicios de red y de infraestructura han sido comprometidos o vulnerados. Esto indica que los controles implementados han fallado y/o que no se ha seguido la política de seguridad de la información de la organización. 2

IEC
Esta norma se compone de documentos técnicos que ayudan a diseñadores y fabricantes, a garantizar la seguridad (de funcionamiento, EMC), fiabilidad y la eficiencia de los dispositivos 8

INTEGRIDAD
Garantiza la exactitud de los datos transportados o almacenados, asegurando que no se ha producido su alteración, pérdida o destrucción, ya sea de forma accidental o intencionada 1

ISO 27001:2013
Es la norma internacional que proporciona un marco de trabajo para los sistemas de gestión de seguridad de la información (SGSI) con el fin de proporcionar confidencialidad, integridad y disponibilidad continuada de la información, así como cumplimiento legal. 5

ISO 31000:2018
Está destinada a personas que crean y protegen el valor en las organizaciones mediante la gestión de riesgos, la toma de decisiones, el logro de objetivos y la mejora del desempeño. 5

LEY 1581
Tiene por objeto desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas. 5

PRIVADA
Dato que por su naturaleza íntima o reservada solo es relevante para su titular[1]. Únicamente puede accederse a ellos por orden de autoridad judicial competente y en ejercicio de sus funciones 9

RESPONSABLE DEL TRATAMIENTO
Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el Tratamiento de los datos 9

SEGURIDAD DE LA INFORMACIÓN
Se entiende el conjunto de medidas preventivas y reactivas que permiten resguardar y proteger la información. Dicho de otro modo, son todas aquellas políticas de uso y medidas que afectan al

8. COAUTORES

A continuación, se realiza una breve descripción biográfica de los autores del presente artículo:

J.F. Mendoza Moreno. Nació en Fortul-Arauca, Colombia. Candidato a especialista en Seguridad de la Información de la Universidad los libertadores e Ingeniero en sistemas de la Universidad Remington. Email jfmendozam@libertadores.edu.co , Es certificado como: ITIL Fundamentals, Scrum Master. Se ha desempeñado como, Líder de infraestructura de redes para empresas privadas.

O.J. Morales Varón, Nació en Bogotá, Colombia. Candidato a especialista en seguridad de la información de la universidad los libertadores e Ingeniero de Sistemas de la Corporación Tecnológica Industrial Colombiana - TEINCO, Email: ojmoralesv@libertadores.edu.co , con formación y experiencia en Seguridad de la Información, Gestión de Riesgos, Continuidad de Negocio con una trayectoria profesional de más de 8 años, formación complementaria como Auditor interno en ISO 27001:2013, ISO27032:2012, ISO22301:2019 e ISO 20000-1:2018, se ha desempeñado como Analista en el soporte de servicios tecnológicos, también como Profesional en Seguridad y Riesgos, auditor interno de procesos para el mantenimiento de Sistemas de Gestión de Seguridad de la Información y Calidad en compañías como Comware S.A. y Olimpia IT S.A.S.

L.O. Valbuena Carvajal. Nació en Albania Caquetá, Colombia. Candidato a especialista en seguridad de la información de la universidad los libertadores e Ingeniero de sistemas de la Corporación Tecnológica industrial colombiana TEINCO. Email: lovalbuenac@libertadores.edu.co , certificado como: Auditor interno ISO 27001:2013 e ITIL, con conocimientos en análisis y desarrollo de sistemas, ciberseguridad y auditoría interna. Se ha desempeñado como técnico en sistemas, técnico Nivel II en sistemas de información para TEINCO, analista en soporte corporativo, Ingeniero II en soporte corporativo, profesional en

Y.I. Serrato Rodríguez. Nació en Bogotá, Colombia. Especialista en Seguridad de la Información de la Universidad Sergio Arboleda e Ingeniero en Telemática de la Universidad Distrital Francisco José de Caldas. Email: yiserrator@libertadores.edu.co , Es certificada como: CEH, Auditor Líder e interno ISO 27001:2013, Auditor interno ISO 22301:2019, ITIL, Cobit, Scrum Foundations, entre otros. Adicional, posee conocimientos en informática forense, ciberseguridad, auditoría interna y manejo de proyectos. Se ha desempeñado como Oficial de seguridad de la información para empresas multinacionales, consultor para empresas públicas y privadas liderando equipos de trabajo multidisciplinarios además docente universitario en varias universidades.

9. REFERENCIAS BIBLIOGRÁFICAS

Briceño, I. (05 de 05 de 2022). Niños y ciberseguridad en Colombia: ¿cómo protegerlos? *Radio Santa Fe 1070 a.m. Bogota*, pág. 1.

ICONTEC. (20 de 12 de 2013). *NORMA TÉCNICA NTC-ISO-IEC* . Obtenido de ISO/IEC 27001: 2013.: https://www.icontec.org/eval_conformidad/certificacion-iso-27001-sistemas-de-gestion-de-seguridad-de-la-informacion-2/

ISO. (2018). *ISO 31000:2018(es).* Obtenido de Online Browsing Platform (OBP): https://www.iso.org/obp/ui#iso:std:iso:31000:ed-2:v1:es

Kemp, S. (15 de Febrero de 2022). *DIGITAL 2022: COLOMBIA*. Obtenido de DATAREPORTAL: https://datareportal.com/reports/digital-2022-colombia?rq=colombia

Lemos, M. (2021). Colombia tiene el segundo nivel más alto de preocupaciones de seguridad en un nuevo estudio global; Sin embargo, la falta de conciencia sobre las amenazas pone en riesgo a los empleadores. *Unisys*, 1.

MinTic. (15 de Febrero de 2022). *En Tic Confio +*. Obtenido de enticconfio: https://www.enticconfio.gov.co/

Pública, F. (18 de Octubre de 2012). *Ley 1581 de 2012*. Obtenido de funcionpublica.gov.co: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981

Reset. (2021). Ciberseguridad en Colombia y el mundo: 10 cifras para tener en el radar. *resetmarketingdigital*, 1.