GUIA DE BUENAS PRÁCTICAS DE SEGURIDAD PARA DISPOSITIVOS MOVILES CON SISTEMA ANDROID

GUIDE TO GOOD SECURITY PRACTICES FOR MOBILE DEVICES WITH ANDROID SYSTEM

Nelson Yecid Pérez Morales.

Joan Nicolas Sánchez Rubiano

Javier Vargas Prieto.

Héctor Manuel Herrera.

RESUMEN

Este artículo pretende dar a conocer la importancia de la seguridad en los dispositivos móviles con sistema operativo Android, Iniciamos realizando una contextualización al lector de la importancia de aplicar buenas prácticas de seguridad en dispositivos móviles especialmente a la población adolescente.

En los últimos años y debido a los tiempos de pandemia a causa del COVID 19, la consolidación del sistema Android, como el sistema operativo más utilizado en Smartphone según el comunicado de prensa de Gartner (Gartner, 2022) lo convierte en blanco del mayor número amenazas, que ponen en riesgo la privacidad de la información (Mejía, 2019).

Finalmente se propuso una guía para de mitigar los riesgos encontrados y brindar sugerencias para la protección de la información.

Palabras Clave: *Android, Sistema Operativo, Amenazas, Riesgos,* Smartphone

ABSTRACT

This article tries to make known the importance of security in mobile devices with Android operating system. We begin by contextualizing the reader of the importance of applying good security practices in mobile devices, especially to the adolescent population.

In recent years and due to the pandemic times due to COVID 19, the consolidation of the Android system, as the most used operating system on Smartphones according to the Gartner press release (Gartner, 2022), makes it the target of the largest number threats, which put the privacy of information at risk (Mejía, 2019)

Finally, a guide was proposed to try to mitigate the risks found and provide suggestions for the protection of information.

Keywords: *Android, Operating System, Threats, Risks, Smartphone.*

1. INTRODUCCIÓN

El inmenso abanico de posibilidades que ofrecen los smartphones hace que cada vez estén más extendidos estos dispositivos entre los adolescentes, de modo que gran parte de sus actividades cotidianas se canalizan a través del móvil. Sin embargo, no están exentos de riesgos, ya que, por ejemplo, se pueden dañar, ser robados o incluso perderse, derivando en la pérdida y falta de control de la información que se tiene almacenada en ellos. Además, si se detienen unos segundos a pensar, podrán darse cuenta de todo lo que los dispositivos conocen sobre sus usuarios: quiénes son los contactos, aplicaciones que utilizan, lugares favoritos que frecuentan, páginas web que visitan, credenciales que utilizan para acceder a sus cuentas, fotografías y vídeos que graban (Internauta, 2020).

Pregunta de investigación

¿Cómo generar hábitos de buenas prácticas en seguridad de Información en dispositivos móviles con sistema operativo Android?

Objetivo General

Proponer una guía de buenas prácticas dirigida a la disminución de posibles riesgos de seguridad en dispositivos móviles con sistema operativo Android.

Objetivos Específicos

- Identificar los riesgos de seguridad enfocados en la tecnología, las aplicaciones y el factor humano para dispositivos móviles con sistema operativo Android por medio de encuestas aplicadas a estudiantes de secundaria.
- Analizar y valorar las encuestas realizadas reuniendo los principales riesgos que requieren mejoras en seguridad, acordando las medidas que se deben tener en cuenta para mitigar los riesgos encontrados.
- Diseñar una guía con las estrategias y controles de seguridad para disminuir la mitigación de los riesgos encontrados.

Alcance

La población objeto de esta investigación son estudiantes ubicados en Bogotá (Cundinamarca) Colombia de los grados 9°, 10° y 11° de Bachillerato del Liceo Avenida las Américas, Se propone el desarrollo de una guía para mejorar los hábitos de los adolescentes en la protección de la información en sus dispositivos móviles.

2. MARCO TEÓRICO

Gracias a esta guía aprenderán a usar y configurar los dispositivos de forma segura, teniendo en cuenta una serie de consideraciones básicas y protegiendo siempre la información para que, pase lo que pase, no la pierdan ni esté disponible para terceros que intenten consultarla (Internauta, 2020).

Las distintas configuraciones que encontraran en esta guía están basadas en la versión Android 10. Además, tener en cuenta que, dependiendo del fabricante del dispositivo, los literales o ubicaciones de las distintas opciones que se mostraran pueden ser ligeramente diferentes (Internauta, 2020).

Antecedentes

El propósito principal de esta publicación es establecer una guía de gestión uniforme y dar orientación sobre la planificación, ejecución y el mantenimiento integral de seguridad para dispositivos móviles con sistema operativo Android.

En cuanto a la norma ISO/IEC 27001:2013 Anexo : A.6.2 Dispositivos móviles y teletrabajo incluye en el dominio de organización de la seguridad de la información, un control enfocado a la creación de políticas de seguridad que permitan la gestión de los riesgos asociados a la introducción de dispositivos móviles en las compañías. (2700, s.f.)

Luego de mencionar el marco de referencia ISO/IEC 27001:2013 vemos que las personas cuentan con los instrumentos necesarios para modificar sus políticas actuales y estas se encuentren alineadas de acuerdo con las necesidades cambiantes del mundo y la tecnología, recalcando la necesidad que en la administración del riesgo sean incluidos los dispositivos móviles de los usuarios como parte de los activos de la organización y del tratamiento de riesgo según los resultados de la valoración obtenidos. (2700, s.f.)

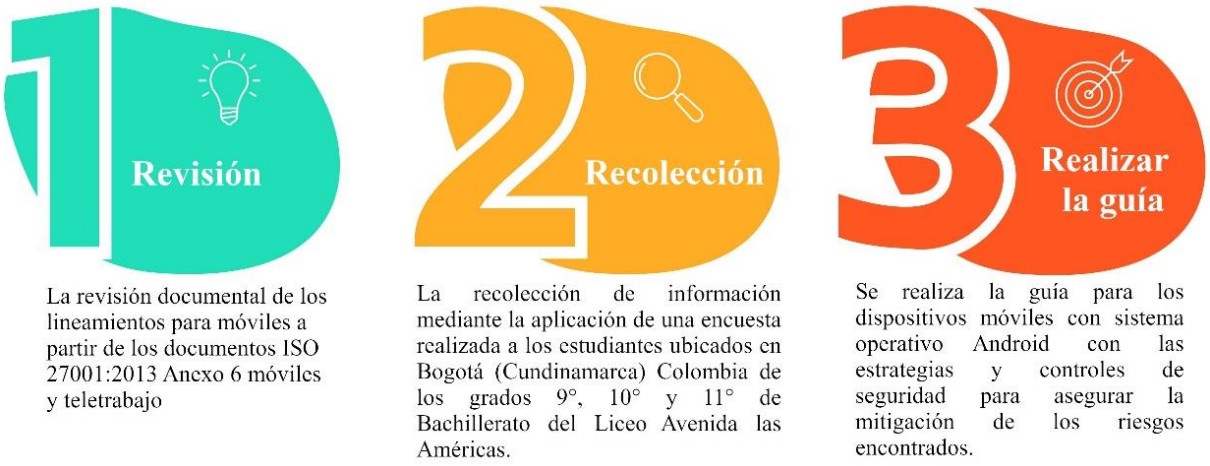
"*Tanto los padres como sus hijos dicen que su teléfono móvil o smartphone es el dispositivo más influyente de su vida. Los padres colocan el móvil entre los dos primeros puestos de la lista, con su teléfono móvil en un 59 %, seguido del ordenador o portátil en un 42 %. Los estudiantes de secundaria también ponen su dispositivo móvil o smartphone en el primer puesto de la lista, aunque con un concluyente 74 % a escala mundial, seguido de su consola de juegos".* (Mcafee, 2022)

Nota: Se aclara que para la investigación realizada se toma como base la norma ISO/IEC 27001:2013 Anexo: A.6.2 Dispositivos móviles y teletrabajo y no la recién emitida ISO/IEC 27001:2022 ya que la investigación se inició a elaborar antes de que se oficializara la nueva versión.

3. METODOLOGÍA.

Esta investigación, se basará en un enfoque cualitativo y descriptivo en tres fases:

Ilustración 1 Etapas de la metodología



Fuente: Autor

1. La revisión documental de los lineamientos para móviles a partir de los documentos ISO 27001:2013 Anexo 6 móviles y teletrabajo.

2. La recolección de información mediante la aplicación de una encuesta realizada a los estudiantes ubicados en Bogotá (Cundinamarca) Colombia de los grados 9°, 10° y 11° de Bachillerato del Liceo Avenida las Américas.

   Se informó debidamente a los participantes de la institución educativa, no involucró el uso de información sensible de acuerdo con lo establecido en la Ley1581 de 2012, que hace referencia al tratamiento de datos personales efectuado en Colombia. (mintic, 2020)

3. Se realiza la guía para los dispositivos móviles con sistema operativo Android con las estrategias y controles de seguridad para asegurar la mitigación de los riesgos encontrados.

4. RESULTADOS

En esta investigación participaron 155 estudiantes de los grados 9°, 10° y 11° de Bachillerato del Liceo Avenida las Américas. ubicado en Bogotá (Cundinamarca) en Colombia.

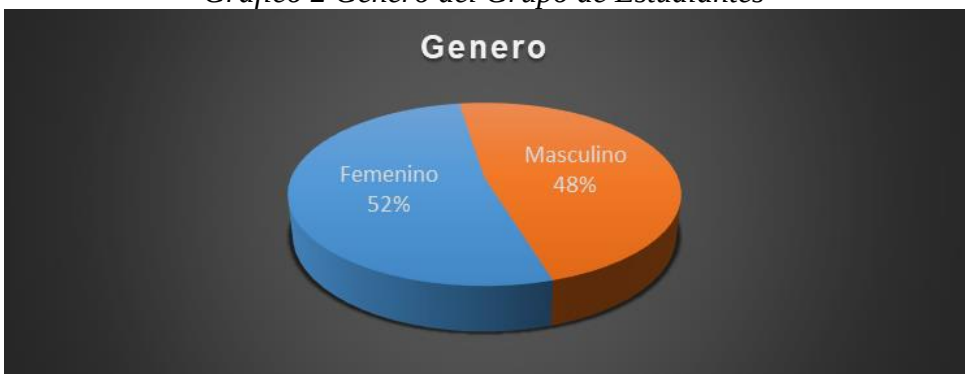
En el grupo, el 7,10% fueron estudiantes de 14 años, 21,29% estudiantes de 15 años, 42,58% de 16 años, 25,16% de 17 años y 3.87% de 18 años, (Ver Gráfico 1).

Gráfico 1 Edades del Grupo de Estudiantes

Fuente: Autor

En el grupo indagado, el 52% fueron estudiantes de sexo femenino y 48% de sexo Masculino, (Ver Gráfico 2).

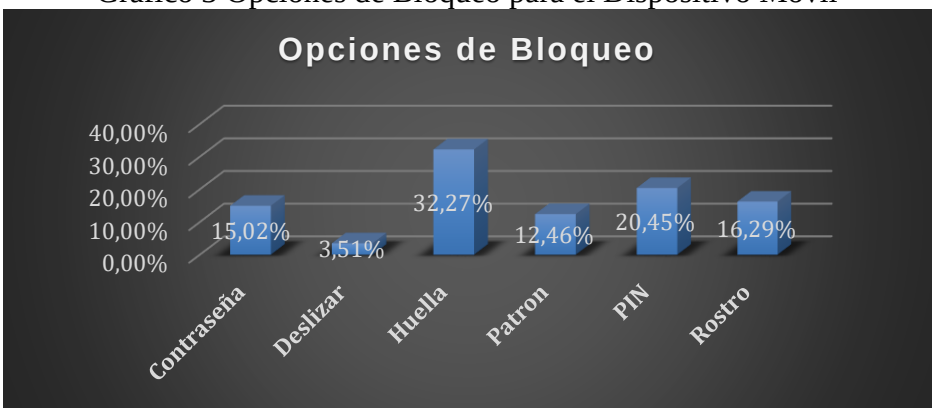
Gráfico 2 Genero del Grupo de Estudiantes



Fuente: Autor

Ahora bien, en relación con el tipo de seguridad que los estudiantes utilizan para bloquear su dispositivo se pudo determinar que el 32,27% de los indagados utilizan el método de huella, el 20,45% utilizan el método de PIN, el 16,29% utilizan el método de Rostro, el 15,02% utilizan el método de contraseña, el 12,46% utilizan el método de Patrón y solo un 3.51% utilizan el método de Deslizar. (Ver Gráfico 3).

Gráfico 3 Opciones de Bloqueo para el Dispositivo Móvil



Fuente: Autor

Establece contraseñas seguras:

Disponen de varias medidas de seguridad para bloquear su dispositivo e impedir que terceras personas puedan hacer uso de él. ¡Gestiona sus contraseñas de manera segura!

Doble factor de autenticación:

Además del uso de una contraseña, añade una capa adicional de seguridad a su cuenta de Google para que, si alguien captura o adivina su clave de acceso, no pueda acceder a ella.

El grupo de encuestados manifiesta que un alto porcentaje tiene configurado su dispositivo para realizar las actualizaciones del sistema, (Ver Gráfico 3).

Gráfico 4 Realiza Actualizaciones del Sistema Operativo

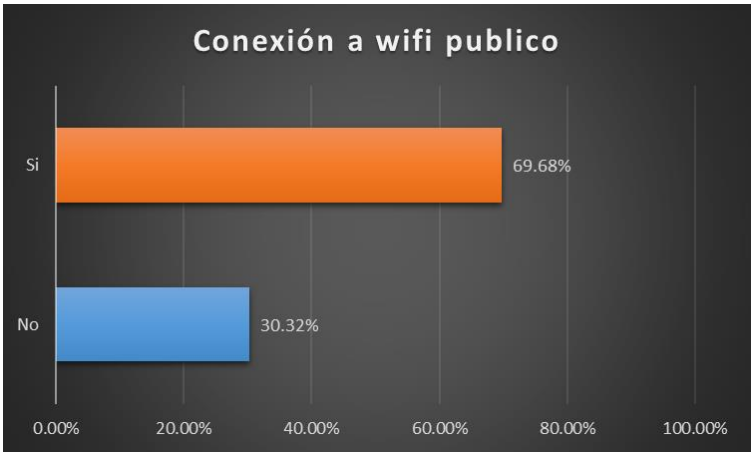
Fuente: Autor

Actualización de software:

Durante la existencia útil del sistema operativo, los desarrolladores van manifestando errores y defectos de seguridad que necesitan ser resueltos. Sin actualizaciones, su dispositivo estaría más expuesto y vulnerable frente a los ataques de los ciberdelincuentes.

El grupo de encuestados manifiesta que un 69.68% de los encuestados acceden al wifi publico solo un 30.32% no lo realiza, (Ver Gráfico 5).

Gráfico 5 Se conectan a Wifi Públicos

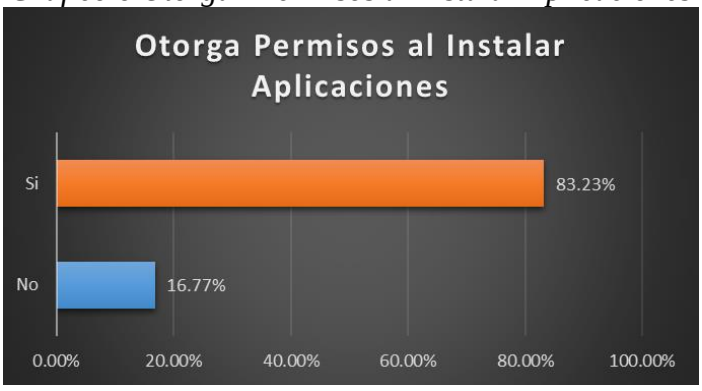


Fuente: Autor

Recuerden: evitar el uso de redes wifi públicas y, si por alguna razón tiene que hacerlo, no accedas a sus cuentas o servicios para que no se hagan con sus credenciales de acceso.

Es importante aclarar que, en el grupo de encuestados, el 83.23% otorga permisos sobre el dispositivo al momento de instalar aplicaciones y solo un 16.77% no los concede, (Ver Gráfico 6).

Gráfico 6 Otorgan Permisos al Instalar Aplicaciones



Fuente: Autor

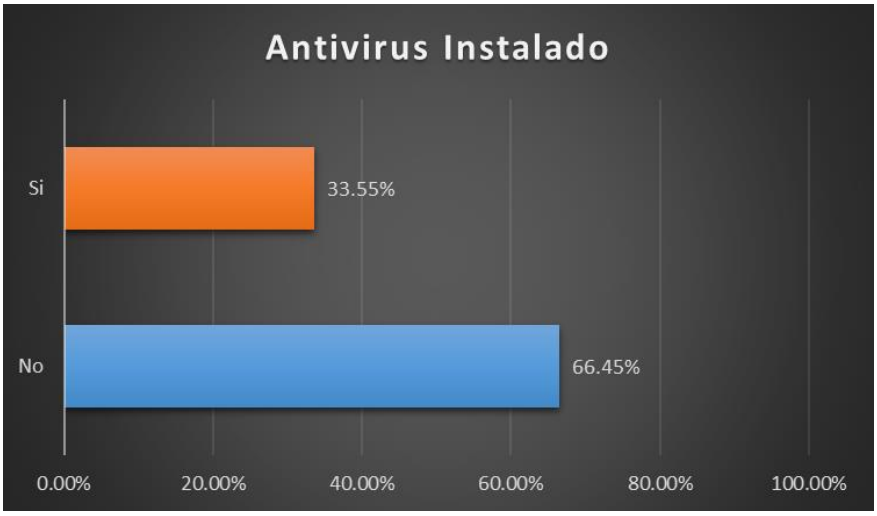
Permisos de apps:

Cuando una app pide permisos, está solicitando acceso a alguna funcionalidad de su dispositivo.

Revisar con mucha atención si tiene sentido que pida un permiso determinado si la app no tiene nada que ver con ese permiso.

Se identificó que el porcentaje de estudiantes que no tienen un antivirus instalado está en un 66,45% frente a 33.55% que, si lo tienen instalado, *(Ver Gráfico 7).*

Gráfico 7 Tiene Instalado un antivirus en el móvil



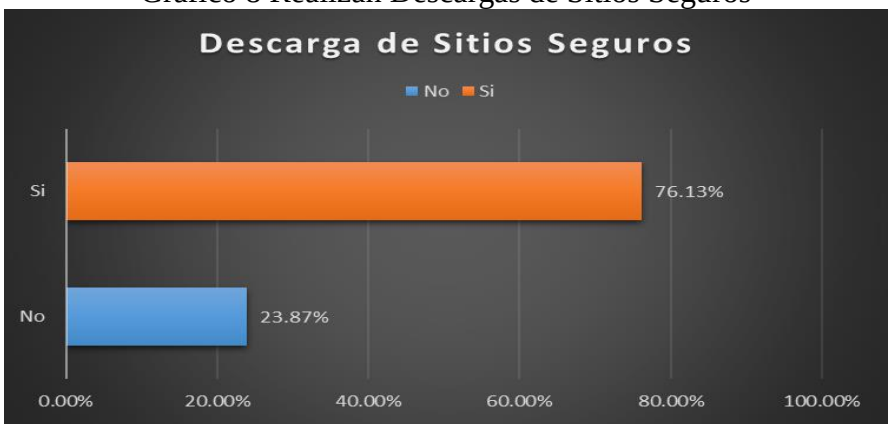
Fuente: Autor

Los dispositivos no están exentos de riesgos de infectarse por algún virus a través de una app o al descargar un archivo infectado.

Para protegerlo: Selecciona un antivirus directamente desde la tienda oficial Play Store, asegurándose de que previamente leen las reseñas de este y valoraciones del mismo.

Así mismo , el 76,13% de los estudiantes manifestó que realizan las descargas de aplicaciones desde sitios seguros y solo el 23,87% no lo realiza *(Ver Gráfico 8).*

Gráfico 8 Realizan Descargas de Sitios Seguros



Fuente: Autor

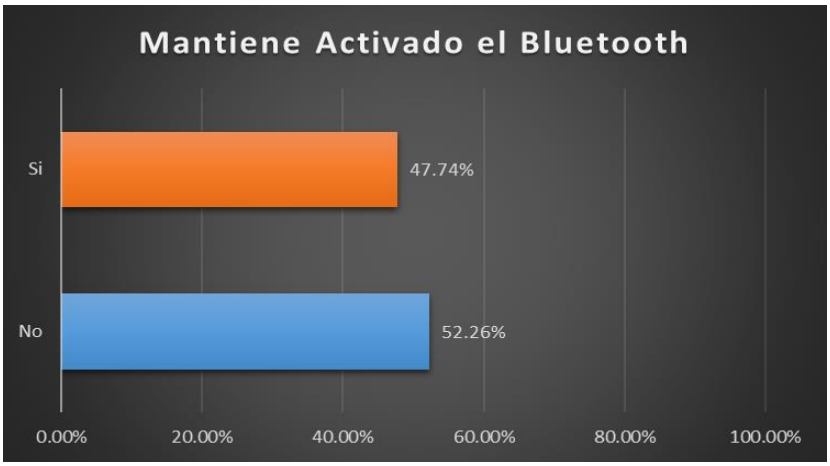
Los Juegos, música, vídeos y muchísimos más tipos de apps están a su disposición para instalar en su dispositivo móvil. En cuestión de segundos tendrán instaladas todas las apps que quieran, pero ¡Cuidado!, las apps se instalan en su dispositivo y acceden a determinadas funcionalidades a través de permisos. Si la app no es del todo fiable, puede hacer un mal uso de estos permisos y poner en riesgo su seguridad y privacidad.

Instalación de apps desde Play Store:

Para instalar apps en su dispositivo Android, deben ir a la tienda oficial de Google Play Store que ya viene instalada por defecto.

Se identificó que el porcentaje de estudiantes que mantienen inactivo el Bluetooth son el 52,26% frente a 47.74% que si lo tienen activo *(Ver Gráfico 9).*

Gráfico 9 Mantiene Activado el Bluetooth del Móvil

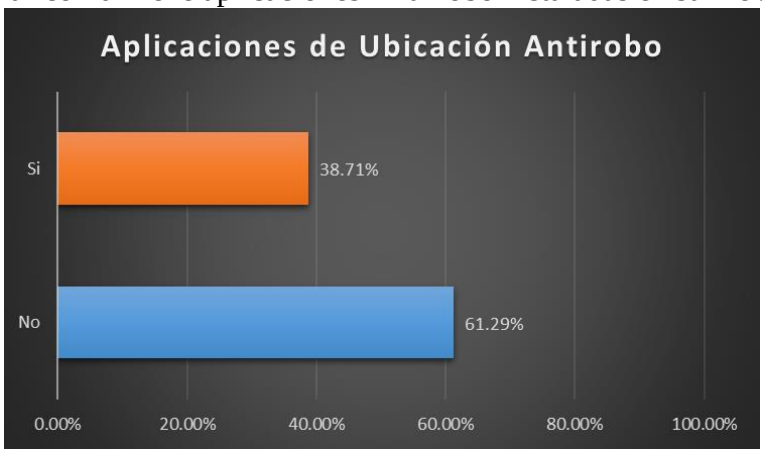


Fuente: Autor

Se recomienda que una vez haya terminado de utilizar el Bluetooth, desactivarlo. Así evitaran que terceros puedan llegar a conectarse y robar información personal como fotos o vídeos o transferirnos algún archivo malicioso a nuestro dispositivo.

Con respecto a la pregunta si tienen aplicaciones antirrobo en sus celulares el 61,29% manifiesta que no tienen instalado ninguna app (Ver Gráfico 10), este factor, pese a su importancia en materia de inmediatez, se convierte en preocupación cuando el dispositivo móvil se extravía o es robado, pues los datos incluidos en él corren el riesgo de ser vulnerados o infectados con algún virus informático.

Gráfico 10 Tiene aplicaciones Antirrobo instaladas en su movil

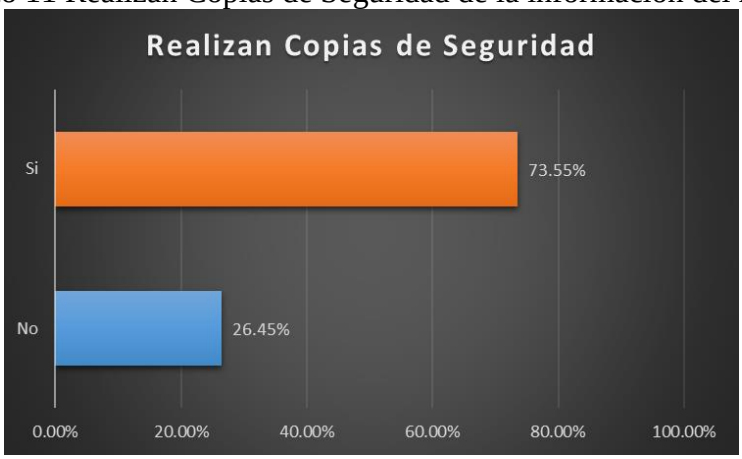


Fuente: Autor

El problema de los robos de celulares se vive con intensidad en Colombia, dicho escenario hace evidente la necesidad no solo de proteger los teléfonos celulares, sino también de encontrar maneras de localizarlos desde ubicaciones remotas. Es ahí donde aplicaciones ayudaran a mitigar estos riesgos.

Los dispositivos móviles se han convertido en una pieza de uso indispensable en la vida diaria de los adolescentes, almacenan contactos, correos, documentos y una infinidad de información personal que utilizan de forma habitual y que no queremos perder de ningún modo, según nuestra encuesta el 73,55% de los estudiantes están realizando copias de seguridad y solo un 26,45% no lo está realizando, (Ver Gráfico 11).

Gráfico 11 Realizan Copias de Seguridad de la información del móvil.

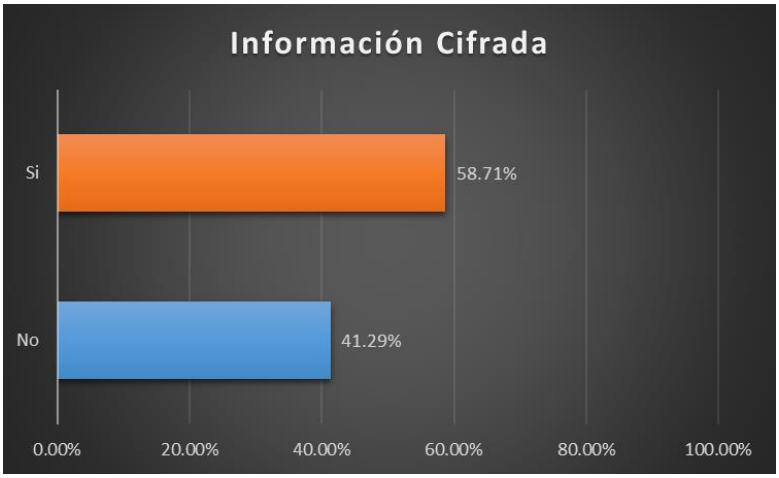


Fuente: Autor

Realizar copias de seguridad de la información que almacenamos en nuestros dispositivos móviles regularmente nos garantizara recuperar toda esta información y, de este modo, evitar la pérdida definitiva de la información

Cifrar el contenido de un teléfono móvil es una medida extra de seguridad que podemos acoger para que su información sea inaccesible por otras personas. Las apps, documentos, Imágenes, etc. quedan indescifrables, aunque se logre acceder a la memoria por cualquier medio, aunque el 58,71% de los estudiantes están realizando esta práctica nos queda un porcentaje del 41,29% que no lo está realizando, (Ver Gráfico 12).

Gráfico 12 Tienen cifrada la información en el movil



Fuente: Autor

Como parte del análisis y los resultados obtenidos se realizó una Guía web donde se planteó consideraciones para proteger la información de los dispositivos móviles (ver Ilustración 2, Ilustración 3).

Ilustración 2 Pagina web – Guía de buenas prácticas

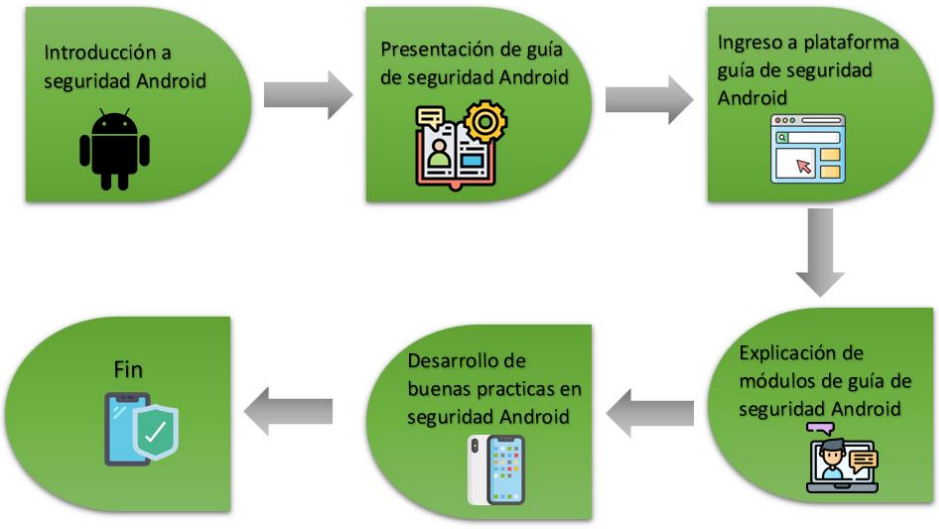
Fuente: Autor

Ilustración 3 Pagina web – Guía de buenas prácticas

Fuente: Autor

En esta Guía los estudiantes de los grados 9°, 10° y 11° encontrarán una ayuda para formarse y comprender temas de seguridad de la información en los dispositivos móviles Android, incluye una explicación de cómo evitar los peligros y ataques que ponen en riesgo nuestra información personal, con recomendaciones para evitarlos, se propone a docentes y estudiantes la siguiente forma de aplicar la guía (ver Ilustración 4).

Ilustración 4 Como aplicar la Guía de Buenas Prácticas



Fuente: Autor

5. CONCLUSIONES

En virtud de lo argumentado, podemos concluir que los móviles de los adolescentes pueden contener información personal muy valiosa, por esta razón es muy importante tener algunas precauciones y buenos hábitos a la hora de trabajar con ellos.

A partir de la evidencia recolectada y analizada en las encuestas podemos concluir:

1. Las contraseñas que son las llaves de acceso a nuestro móvil y a toda la información contenida en el dispositivo es la primera barrera de seguridad, por lo que si alguien no autorizado hiciera

uso de las mismas estaría comprometiendo la privacidad de la información y datos a los que pudiera acceder, de esta manera, la administración de las contraseñas se convierte en uno de los aspectos más importantes a la hora de proteger nuestra información, para disminuir los riesgos observados se recomienda poner en práctica la sección ***implementa una contraseña*** de la guía de buenas prácticas publicada como resultado de nuestro proyecto.

2. Con respecto a las apps, no se trata de que no puedan instalar juegos o aplicaciones en el móvil, el problema es que, en las tiendas de apps móviles tanto oficiales como no oficiales hay millones de aplicaciones que aparentando ser inofensivas, esconden un comportamiento malicioso que podría ocasionar que información confidencial nuestra o de la empresa acabe en manos incorrectas, tener en cuenta algunas medidas preventivas pueden evitar que el adolescente descargue alguna aplicación insegura a su teléfono móvil, verificar que la apps sea de un desarrollador oficial, que estén mejor evaluadas y bien valoradas, con comentarios positivos.

3. Por otra parte, los móviles deben disponer de herramientas especiales que aumenten la seguridad del dispositivo y de nuestras comunicaciones (Antivirus, herramientas de cifrado, apps antirrobo, etc.), se recomienda poner en práctica las secciones ***hay que estar totalmente seguro y prepararte en caso de perder tu móvil*** de la guía de buenas prácticas publicada como resultado de nuestro proyecto.

4. Con respecto al uso de redes públicas es un punto de conexión WiFi abierto al público. Muchos estudiantes lo utilizan para sus conexiones por la ciudad, hay que hacerles saber que estas redes hay que usarlas con precaución, **no son seguras,** sugerimos a los estudiantes no usar estas redes para acceder a páginas que puedan contener material privado, se recomienda poner en práctica la sección ***conexiones seguras*** de la guía de buenas prácticas publicada como resultado de nuestro proyecto.

Debido a la necesidad del buen uso de la seguridad de la información en un dispositivo móvil es clave una buena comunicación con la población adolescente exponiendo pautas claras y concisas, de carácter eminentemente práctico, presentamos la guía de buenas prácticas para dispositivos móviles con sistema operativo Android en la página web http://13.82.150.96/GUIA/index.html.

Si los adolescentes ponen en práctica las recomendaciones de la guía, su información de todo tipo:

contactos de familiares y amigos, fotos personales, documentos confidenciales, ubicaciones geográficas, mensajes, etc. Estarán protegidos frente a las amenazas como un robo o pérdida del móvil o de intrusión de algún tipo de virus en su dispositivo, la protección de nuestros datos debe ser una acción constante, que con el tiempo se vuelve algo natural y cotidiano.

6. AGRADECIMIENTOS

Agradecimientos a la institución Liceo Avenida las Américas y los estudiantes de los grados 9°, 10° y 11° que participaron activamente en el aporte de los datos de esta investigación.

REFERENCIAS

2700, I. (s.f.). *https://normaiso27001.es/*. Obtenido de https://normaiso27001.es: https://normaiso27001.es/a6-organizacion-de-la-seguridad-de-la-informacion/

Gartner. (02 de 03 de 2022). *https://www.gartner.com/en/newsroom/press-releases/2022-03-01-4q21-smartphone-market-share*. Obtenido de https://www.gartner.com/en/newsroom/press-releases/2022-03-01-4q21-smartphone-market-share: https://www.gartner.com/en/newsroom/press-releases/2022-03-01-4q21-smartphone-market-share

Internauta, O. d. (01 de 01 de 2020). *https://www.osi.es.* Obtenido de https://www.osi.es: https://www.osi.es/es/guia-para-configurar-dispositivos-moviles

Mcafee. (24 de 02 de 2022). *https://www.mcafee.com*. Obtenido de https://www.mcafee.com/: https://www.mcafee.com/blogs/es-es/family-safety/moviles-y-adolescencia-que-esconde-la-pantalla-de-bloqueo/

Mejía, J. (18 de 12 de 2019). Detectando aplicaciones maliciosas en Smartphone con sistema Android a través del uso de una aplicacion. *Revista Ibérica de Sistemas y Tecnologías de Información*, pág. 82.

mintic. (01 de 03 de 2020). *https://www.mintic.gov.co*. Obtenido de https://www.mintic.gov.co: https://www.mintic.gov.co/portal/inicio/Atencion-y-Servicio-a-la-Ciudadania/Transparencia/135881:Ley-1581-de-2012-Proteccion-de-Datos-Personales