Actividad 2 – Prevención de Fuentes de Ataques e Intrusión

Seguridad Informática I

Ingeniería en Desarrollo de Software

Tutor: Jessica Hernández Romero

Alumno: Kathya Viridiana Chávez Domínguez

Fecha: 11/05/2024

Índice

Introducción

La detección y prevención de amenazas se han vuelto aspectos críticos para proteger a las organizaciones de posibles ciberataques. Este proceso implica analizar detenidamente la información y los datos de la empresa con la finalidad de identificar irregularidades que podrían ocasionar un ataque. Una vez encontradas, estas irregularidades, se analizan exhaustivamente para determinar su potencial como amenazas. Posteriormente, la organización puede actuar y desarrollar soluciones efectivas para eliminar cualquier riesgo. Esta medida se vuelve esencial, ya que permite minimizar los daños y las pérdidas financieras que se puedan provocar tanto para la empresa como para sus clientes.

A través de esta actividad, analizaremos las amenazas que se encontraron en la práctica anterior para proponer al menos una recomendación que nos permita proteger, mejorar o monitorearlas y con ello prevenir futuros ataques e intrusiones. Al finalizar, seremos capaces de entender la importancia que tiene realizar este análisis y la necesidad de trabajar en las posibles amenazas para garantizar la seguridad de las organizaciones.

.

Descripción

En la primera actividad identificamos las diversas amenazas y vulnerabilidades del colegio tomando en cuenta el escenario planteado. En esta ocasión como analista de seguridad, se nos solicita proponer recomendaciones que ofrezcan soluciones a estos eventos. Por lo tanto es necesario planificar, mejorar e implementar las medidas necesarias que permitan proteger tanto los aspectos físicos como los relacionados con la información, teniendo presente que la información que no esta segura puede ser un factor de riesgo critico para cualquier institución.

Para lograrlo, es fundamental aplicar herramientas que posean las funcionalidades requeridas para cumplir con el objetivo de esta actividad. Además, es importante revisar previamente investigaciones que nos permitan sustentar nuestras ideas. Una vez realizadas estás recomendaciones, es importante realizar una conclusión personal sobre la importancia de nuestra labor en esta actividad y como ayudaría dentro del campo laboral o vida cotidiana, así como incorporar las referencias consultadas durante nuestra investigación realizada.

Justificación

En la actualidad, la tecnología es una herramienta fundamental, ya que gracias a ella mucho de los procesos hoy en día se realizan de forma automática y práctica. No obstante, es importante considerar que a medida que la sociedad se digitaliza, y se conecta a internet, aumenta la posibilidad de que los hackers y otros ciberdelincuentes accedan a datos e información confidencial. Por ello se vuelve es esencial contar con medidas de seguridad que nos protejan contra estos ataques, especialmente para las instituciones y organizaciones que manejan un mundo de información. Tomando esto en cuenta, las organizaciones deben desarrollar estrategias y planes que les permitan anticipar y responder rápidamente a posibles ataques maliciosos. Estas medidas deben evitar que alguien externo o interno puedan acceder, alterar, eliminar o utilizar datos sensibles de una organización. La seguridad informática se convierte así en una prioridad para garantizar la integridad de la información y proteger los intereses de la organización.

Desarrollo

Tabla de recomendaciones

	Amenazas humanas	Amenazas Lógicas	Amenazas Físicas	Vulnerabilidades de almacenamiento	Vulnerabilidades de Comunicación
Factor de riesgo	Acceso no vigilado en el área administrativa	Riesgos de red por la ubicación del servidor principal	Colegio carece de un dispositivo de detección de eventos naturales	Registro de entrada se realiza por medio de una libreta.	Servidor principal puede ocasionar problemas de comunicación y rendimiento debido a su ubicación.
Recomendaciones	Colocar sistemas de alarma en las áreas más vulnerables y en la entrada para evitar accesos no autorizados.	Centralizar el servidor principal en el centro de cómputo garantiza una mayor seguridad y reduce el riesgo de que cada nueva conexión se convierta en un punto de entrada potencial para un atacante.	Es fundamental instalar dispositivos de detección de eventos naturales, como sistemas de alerta para huracanes o sismos. Así mismo realizar copias de seguridad de datos importantes y proteger los equipos electrónicos de posibles daños físicos.	Se recomienda utilizar un sistema informático o una aplicación móvil donde los docentes puedan registrar su entrada de manera electrónica, además de implementar un sistema de copias de seguridad. Esto facilitaría la recuperación de datos anteriores, y protegería la información contra daños en los dispositivos electrónicos utilizados para el registro.	Implementar medidas para optimizar la conexión entre el servidor principal y el centro de cómputo. Además actualizar el hardware de red y el uso de tecnologías de conexión más avanzadas como fibra óptica en lugar de cableado de cobre.

Fuente de ataque e intrusión	El área administrativa del colegio actualmente carece de sistemas de alarma de seguridad al acceder, lo que podría permitir el acceso no autorizado y la potencial obtención de información confidencial para fines no autorizados.	La ubicación del servidor principal fuera del centro de cómputo implica la necesidad de mantener conexiones de red adicionales. Esto expande la superficie de ataque de la red, convirtiendo cada nueva conexión en un posible punto de entrada para un atacante.	Tomando en cuenta la ubicación de Veracruz, una de las amenazas físicas a las que se está expuesto son los huracanes, los cuales pueden causar vientos, lluvias e inundaciones lo que puede resultar en daños materiales y afectaciones a las infraestructuras. Esto es muy grave, sobre todo considerando que el colegio carece de un dispositivo de detección de eventos naturales, lo que aumenta la vulnerabili	El registro de la entrada de los docentes en una libreta puede parecer una tarea simple, pero en realidad conlleva una vulnerabilidad significativa. Existe el riesgo de pérdida de la libreta, lo que implicaría la pérdida de la información registrada. Además, recuperar datos de meses o años anteriores puede resultar difícil, especialmente si la libreta se llenó en algún momento y fue reemplazada por otra.	La calidad de la conexión entre el servidor principal y el centro de cómputo debe ser óptima, ya que de lo contrario podría generar problemas de comunicación o rendimiento. Esto afectaría la accesibilidad y la eficiencia de los servicios ofrecidos.

			dad de los equipos ante tales eventualidades.		
Factor de riesgo	Ataques dirigidos en la salida de emergencia.	Seguridad de la red Wi-Fi.	Equipos ubicados en planta baja conectados directamente al módem a través de cables.	Falta de almacenamiento en los equipos.	Dispositivos portátiles se conectan a través de Wi-Fi.
Recomendaciones	Contar con más de una salida de emergencia, no solo es crucial para en situaciones cómo sismos o incendios, sino que también reduce el riesgo de que los atacantes puedan aprovechar esta única salida de emergencia.	Una opción viable para disminuir el riesgo es utilizar conexiones por cable, considerando que son más seguras que las comunicaciones inalámbricas ya que poseen un menor riesgo de sufrir incidentes por falsos puntos de acceso donde la víctima se conecta a una red	Considerar la posibilidad de reubicar los equipos a áreas más elevadas y menos propensos a los deslizamientos de tierra.	Se recomienda capacitar al personal y a los estudiantes sobre como manejar adecuadamente los archivos y utilizar herramientas de almacenamiento en la nube para evitar la pérdida de datos.	Es recomendable colocar el enrutador Wi-Fi en una ubicación central y elevada para maximizar su alcance y reducir las interferencias. Además se pueden instalar repetidores o extensores de Wi-Fi en áreas donde la señal sea débil y mejorar la cobertura de la red inalámbrica en el segundo piso.

		abierta creada por el atacante y este último lo que hace es espiar su tráfico y robar sus datos. Sin embargo, también se considera que la redes WI-FI son más prácticas, por lo que otra opción sería generar múltiples redes inalámbricas que tengan diferentes accesos. Por ejemplo: una red para maestros que sea distinta a la red de los alumnos, así como utilizar un servidor RADIUS el cual sirve para una			

Fuente de ataque e intrusión	Existe el riesgo de que un posible atacante concentre sus esfuerzos en identificar y explotar esta única vía. Esto podría lograrse mediante ataques de denegación de servicio u otras técnicas que comprometan o interrumpan el sistema, dejando vulnerables a quienes dependen de ella en situaciones críticas.	Dado que contamos con dispositivos portátiles que se conectan a través de Wi-Fi, la seguridad de esta conexión se ve comprometida. Este tipo de conexión es más susceptible a ser interceptada o comprometida en comparación con las conexiones por cable, ya que los atacantes podrían intentar acceder a la red mediante técnicas como la suplantación de identidad y el descifrado de contraseñas débiles	Debido a la presencia de zonas montañosas en Veracruz, las fuertes lluvias pueden desencadenar deslizamientos de tierra, representando un riesgo para los equipos, especialmente aquellos ubicados en la planta baja que están conectados directamente al módem a través de cables.	Tomando en cuenta la falta de almacenamiento en los equipos, es más probable que ocurran errores al guardar los datos, lo que podría resultar en la pérdida de archivos importantes. Esto comprometería la disponibilidad de información sensible para el colegio.	Los equipos portátiles que se conectan a través de Wi-Fi pueden experimentar interferencias y alcances limitados, especialmente al considerar su ubicación en un segundo piso. Esto puede traducirse en conexiones inestables y problemas de rendimiento.

Factor de riesgo	Acceso físico a la información facilitado	Riesgo de malware y ataques por dispositivos con bajo almacenamiento	Tipo de extintores disponibles	Servidor espejo se encuentra ubicado en el centro de cómputo.	Presencia de un servidor espejo.
Recomendaciones	Se sugiere llevar un registro de las personas autorizadas que necesiten transportarlas en caso de extrema necesidad. Además, se pueden implementar sistemas de detección y prevención de intrusiones para fortalecer la seguridad de la red. Es fundamental realizar evaluaciones regulares de la red para eliminar cuentas inactivas y capacitar al personal en temas de ciberseguridad.	Es fundamental realizar un mantenimiento regular y una limpieza periódica de los dispositivos. Es recomendable almacenar únicamente los archivos esenciales en servicios de almacenamiento en la nube y mantener instaladas solo las aplicaciones que sean realmente necesarias.	Incluir el extintor de dióxido de carbono (tipo C). Este último es crucial, ya que no deja residuos y no conduce electricidad, lo que lo hace seguro para su uso en entornos con equipos electrónicos. Su ausencia podría representar un riesgo para la integridad de nuestros dispositivos en caso de un incendio.	Se recomienda revisar la configuración del servidor para asegurarse que coincida exactamente con la del servidor principal, incluyendo la configuración de hardware, software, redes y cualquier otro parámetro importante.	Implementar sistemas de monitoreo de la actividad de la red que pueda detectar patrones de tráfico anormales indicativos de un posible ataque DDoS. Además sería útil realizar pruebas periódicas de mitigación de DDoS para evaluar la eficacia de la medida implementada e identificar posibles áreas de mejora.

Fuente de ataque e intrusión	Los dispositivos portátiles son más susceptibles al acceso físico no autorizado, especialmente si se permite que sean transportados fuera del lugar de trabajo. Esto aumenta el riesgo de robo de datos, incluso por parte de los propios empleados, sobre todo si no se implementan las medidas de seguridad adecuadas.	Los equipos con bajo espacio de almacenamiento y rendimiento lento son más propensos a infecciones por malware y ataques cibernéticos. Esta vulnerabilidad se incrementa especialmente cuando los usuarios descargan e instalan software, parches de seguridad y actualizaciones sin precaución, lo que aumenta la probabilidad de instalar malware o software no autorizado.	Actualmente, contamos con dos extintores Clase A y uno Clase B ubicados en el piso principal. Sin embargo, considerando que nuestras instalaciones abarcan dos pisos, 18 salones, el centro de cómputo y la biblioteca, varias áreas quedan desprotegidas en caso de un incendio. Es importante destacar que los extintores disponibles son eficaces para combatir incendios que involucran materiales	Si el servidor espejo ubicado en el centro de cómputo no está configurado correctamente con el servidor principal, podrían surgir diferencias en los datos. Esto podría ocasionar inconsistencias en la información o incluso pérdida de datos.	La presencia de un servidor espejo aumenta la probabilidad a un ataque DDoS, el cual sobrecarga los recursos de red y agota la capacidad de procesamiento. Este tipo de ataque podría provocar una interrupción del servicio para los usuarios.

			combustibles comunes, como madera, papel, tela y plástico (tipo A), así como para extinguir incendios que implican líquidos inflamables o combustibles (tipo B). Sin embargo, esta selección de extintores no garantiza la protección adecuada de los dispositivos electrónicos.		
Factor de riesgo	El bajo rendimiento y poco almacenamiento de los dispositivos puede generar exposición a las amenazas internas.	Ataques de autenticación por contraseñas débiles.	Sólo se cuenta con una salida de emergencia en el edificio.	Falta de firewall en los dispositivos.	Centro de cómputo cuenta con 10 equipos de escritorio, 5 laptops y 1 servidor de espejo, todos ellos dependen de un servicio de internet con una

					capacidad de 20GB.
Recomendaciones	Es fundamental realizar una limpieza periódica eliminando archivos y aplicaciones innecesarios, gestionando las descargas de manera eficiente y, sobre todo, manteniendo actualizados tanto el software como el firmware de los dispositivos.	Las contraseñas son la primera barrera de protección contra accesos no autorizados. Por lo tanto, cuanto más segura sea la contraseña, mayor será la protección de la información. Se aconseja utilizar contraseñas que consten de al menos ocho a doce caracteres, que combinen letras, números y símbolos, y que incluyan palabras poco comunes o inusuales.	Agregar salidas de emergencia adicionales en puntos estratégicos para garantizar una evacuación segura, así como instalar sistemas de alerta temprana para mantener la seguridad de la infraestructura y de las personas en todo momento.	Instalar y configurar un firewall actualizado en la red de la organización, ya que este firewall actúa como una barrera de seguridad que controla y monitorea el tráfico de red, bloqueando cualquier intento de salida no autorizada.	Considerar actualizar el servicio de internet a uno con mayor capacidad de ancho de banda y opciones de alta velocidad que permitan cumplir con las necesidades de todos los dispositivos conectados. O bien, identificar y limitar el acceso a servicios y aplicaciones no esenciales que puedan consumir ancho de banda de manera innecesaria.

Fuente de ataque e intrusión	Los dispositivos con bajo rendimiento y poco espacio de almacenamiento pueden ser objeto de abuso por parte de empleados malintencionados. Estos dispositivos ofrecen una mayor oportunidad para el robo de datos confidenciales o la realización de actividades no autorizadas, aprovechando la falta de controles y la lentitud del sistema	Dado que los equipos utilizan credenciales de usuario y contraseña básicas, se vuelven vulnerables a los ataques de autenticación, tales como el SpoofingLooping, el Ip SplicingHijacking y el Net Flooding.	Depender únicamente de una sola salida de emergencia nos expone a un punto crítico. Si esta salida llegara a fallar o ser comprometida de alguna manera, toda la infraestructura o sistema podría volverse inaccesible.	La falta de un firewall puede ocasionar la salida no autorizada de datos sensibles de la organización, comprometiendo la confidencialidad de la información.	Considerando que el centro de cómputo cuenta con 10 equipos de escritorio, 5 laptops y 1 servidor espejo, depender de un servicio de internet con una capacidad limitada de 20 GB podría provocar una sobrecarga de red si no es capaz de soportar el tráfico generado por todos los dispositivos. Esto podría afectar la disponibilidad y el rendimiento de los servicios..
Factor de riesgo	Exposición a amenazas externas por acceso a redes sociales.	Dispositivos con versión gratuita del antivirus nod 32.	Ubicación del servidor principal.	Servidor utiliza el software Oracle Database en un sistema operativo Linux.	Ausencia de un firewall en los dispositivos.
Recomendaciones	Se recomienda adquirir líneas móviles específicas para los dispositivos,	Es crucial disponer de un antivirus capaz de detectar y eliminar malware	Considerar trasladar el servidor principal al centro de cómputo principal o	Es recomendable mantener actualizado tanto el software como el sistema operativo, así mismo se recomienda	Es necesario instalar y configurar un firewall de red para controlar y monitorear el tráfico de red entrante y

	las cuales deben tener restricciones en el acceso a redes sociales y contenido sensible. Estas restricciones pueden ser monitoreadas por un operador para garantizar la seguridad y el uso adecuado de los dispositivos.	de manera efectiva. Los antivirus de pago suelen garantizar una protección más completa y avanzada en comparación con las versiones gratuitas. Por ello, se sugiere optar por el plan de pago del antivirus NOD32 o explorar otras alternativas que ofrezcan versiones premium.	a un lugar más seguro dentro de las instalaciones. Además de implementar un sistema de respaldo de datos para garantizar que la información almacenada en el servidor está protegida y pueda recuperarse.	implementar herramientas que permitan analizar las vulnerabilidades para identificar puntos débiles en el servidor y la base de datos.	saliente, este debe de estar configurado para bloquear el tráfico no autorizado.
Fuente de ataque e intrusión	Tomando en cuenta que en los equipos no se tiene denegado el acceso a redes sociales, correo personal o WhatsApp, los empleados pueden exponerse a amenazas externas,	Debido a que se utiliza la versión gratuita del antivirus nod32 en todos los equipos, su capacidad de detección y limpieza	El servidor principal está expuesto a diversas amenazas físicas debido a su ubicación fuera del centro de cómputo principal. Riesgos	Contemplando que el servidor utiliza el software Oracle Database en un sistema operativo Linux, es importante considerar que puede contener vulnerabilidades de seguridad propias, como errores de programación e inyecciones de	La ausencia de un firewall habilitado expone nuestros sistemas a ataques que pueden agotar los recursos del sistema y causar interrupciones en los servicios.

	como perfiles falsos, ataques de ingeniería social o intentos de robo de identidad.	es inferior en comparación con las versiones comerciales. Esto puede resultar en una menor eficacia para detectar y eliminar malware, aumentando así el riesgo de infecciones y compromisos de seguridad.	como desastres naturales, incendios, robos o daños accidentales pueden provocar la pérdida de datos o la interrupción del servicio.	SQL. Estas vulnerabilidades podrían ser explotadas por atacantes para acceder o manipular los datos almacenados en la base de datos.	
Factor de riesgo		El servidor cuenta con un sistema de control descargado de internet, cuya fuente y origen son desconocidos.		Utilización de software de origen desconocido en el servidor 2.	
Recomendaciones		Para reducir el riesgo de comprometer la seguridad del servidor y la integridad de los		Es necesario realizar una investigación para determinar el origen y la fiabilidad del software instalado en el servidor 2, sobre todo verificar si es de una fuente	

		datos almacenados, es esencial realizar un escaneo exhaustivo del sistema de control descargado de internet mediante un antivirus confiable y actualizado. Además, se recomienda investigar la procedencia del sistema, buscando información sobre la reputación y la confiabilidad de la fuente.		confiable y si ha sido previamente evaluado por expertos en seguridad y privacidad.	
Fuente de ataque e intrusión		Dado que el Servidor 2 aloja un sistema de control descargado de internet, cuya		La utilización de software de origen desconocido en el Servidor 2 podría ocasionar fugas de datos o violaciones de privacidad. Esto	

		fuente y origen son desconocidos, existe el riesgo de que contenga malware como virus, troyanos o ransomware. Esto podría comprometer la seguridad del servidor y poner en riesgo la integridad de los datos almacenados.		puede ocurrir si el software recopila, almacena o transmite información de los alumnos sin el consentimiento adecuado.	

Conclusión

A través de la siguiente actividad tuvimos la oportunidad de seguir trabajando con las fuentes de vulnerabilidades y amenazas previamente identificadas. En esta ocasión nos enfocamos en encontrar y realizar las recomendaciones adecuadas para prevenir o evitar cualquier riesgo tanto en el colegio como en otras organizaciones. Este proceso nos permitió anticipar diferentes escenarios que podrían pasar y desarrollar posibles soluciones para cada uno de ellos.

Además remarcamos la importancia de realizar un análisis de vulnerabilidades y amenazas, con el fin de detectar y abordar posibles puntos débiles en los sistemas antes de que puedan ser explotados por atacantes o personas malintencionadas. Esta labor preventiva se vuelve crucial para proteger la integridad y seguridad de los dispositivos. En conclusión, la prevención de vulnerabilidades y amenazas es una inversión estratégica y esencial que ayuda a garantizar la seguridad de las organizaciones. Al reducir los riesgos relacionados con las amenazas cibernéticas actuales, se fortalece la seguridad y la vez se conserva la confianza de los usuarios.

Link GitHub: https://github.com/KathyaCh/Prevenci-n-de-Vulnerabilidades-y-Amenazas.git

Referencias

I. Admin_Miray. (2020, 8 octubre). La importancia del Firewall en entornos corporativos | Blog Miray. *Miray Consulting*. https://www.mirayconsulting.com/la-importancia-del-firewall-en-entornos-corporativos/#:~:text=Ejecuci%C3%B3n%20de%20software%20no%20autorizado&text=Tener%20un%20buen%20sistema%20de%20firewall%2C%20actualizado%20y%20constantemente%20revisado,terceros%20a%20la%20red%20corporativa.

II. *Cómo proteger correctamente la red WiFi de tu oficina*. (2023, 23 marzo). Tecnología Para los Negocios. https://ticnegocios.camaravalencia.com/servicios/tendencias/como-proteger-la-red-wifi-de-tu-oficina/

III. Conzultek. (s. f.). *Seguridad en endpoint: cómo evitar el robo de información en su empresa*. https://blog.conzultek.com/seguridad-endpoint-como-evitar-robo-de-informacion

IV. CoveriX. (2023, 28 diciembre). Los 5 mejores antivirus para empresas. *Coverix*. https://blog.coverix.mx/mejores-antivirus#:~:text=Seg%C3%BAn%20los%20resultados%20de%20las,McAfee%20Total%20Protection

V. *Detección y prevención de amenazas informáticas | Prey Blog*. (2022, 8 septiembre). https://preyproject.com/es/blog/deteccion-y-prevencion-de-amenazas-su-guia-para-mantenerse-a-salvo

VI. Duran, V., & Duran, V. (2023, 12 diciembre). Por qué es importante proteger tu empresa de un ciberataque. *Hillstone Networks*.

https://www.hillstonenet.lat/blog/notificacion-de-vulnerabilidad/por-que-es-importante-proteger-tu-empresa-de-un-ciberataque/

VII. Fernández, Y. (2021, 26 marzo). *Repetidor WiFi, qué es y cómo funciona*. Xataka. https://www.xataka.com/basics/repetidor-wifi-que-como-funciona

VIII. Gurusoft. (2024, 18 enero). *Tips para optimizar el espacio de almacenamiento de los dispositivos*. GuruSoft. https://guru-soft.com/tips-para-optimizar-el-espacio-de-almacenamiento-de-los-dispositivos/#:~:text=Elimina%20regularmente%20archivos%20y%20aplicaciones,actualizado%20de%20software%20y%20firmware.

IX. Lockbits. (2023b, abril 13). Ciberseguridad, ¿Por qué es tan importante? *Lockbits*. https://lockbits.cl/blog/ciberseguridad-por-que-es-importante/

X. Paus, L. (s. f.). *Conocimientos generales: ¿Cuál es la red de datos más segura, la cableada o la inalámbrica? – Seguridad de la información*. https://www.uv.mx/infosegura/general/conocimientos_wifi-6/#:~:text=Debido%20a%20esto%2C%20las%20conexiones,de%20seguridad%20que%20podr%C3%ADan%20aplicarse.

XI. *¿Por qué la ciberseguridad es tan importante?* (s. f.). https://www.ironhack.com/mx/blog/por-que-la-ciberseguridad-es-tan-importante

XII. *¿Qué es la protección con contraseña? | Seguridad de Microsoft*. (s. f.). https://www.microsoft.com/es-mx/security/business/security-101/what-is-password-protection#:~:text=Crea%20contrase%C3%B1as%20seguras%20que%20tengan,mismas%20contrase%C3%B1as%20en%20varias%20cuentas.

XIII. *Qué es un ataque DDOS y cómo proteger su sitio contra uno*. (s. f.). Amazon Web Services, Inc. https://aws.amazon.com/es/shield/ddos-attack-protection/

XIV. *Red de fibra óptica: ventajas y definición | Enel X*. (s. f.). Enel X. https://corporate.enelx.com/es/question-and-answers/advantages-of-fiber-optic#:~:text=Las%20ventajas%20del%20cable%20de,vida%20m%C3%A1s%20sostenible%20y%20circular.

XV. Solbyte. (2024, 15 abril). *Cómo Limitar o Bloquear el Uso de Redes Sociales en Móviles de Empresa*. Más IP. https://www.masip.es/blog/como-limitar-o-bloquear-el-uso-de-redes-sociales-en-moviles-de-empresa/

XVI. Ubiqo. (2021, 13 mayo). *Qué son las apps de origen desconocido - Evidence*. Evidence. https://www.evidence.com.mx/blog/que-son-las-apps-de-origen-desconocido/