UNIVERSIDAD TÉCNICA DE BABAHOYO

FACULTAD DE ADMINISTRACIÓN, FINANZAS E INFORMÁTICA.

INGENIERÍA EN SISTEMAS DE INFORMACIÓN

PREVIO A LA OBTENCION DEL TITULO DE INGENIERO EN SISTEMAS DE INFORMACIÓN

TEMA:

ANÁLISIS DE VULNERABILIDADES DE LAS APLICACIONES ANDROID UTILIZADAS EN GESTIÓN DE EMPRESAS

ESTUDIO DE CASO

JESUS ALEJANDRO PUTAN SANTILLAN

TUTOR:

ING.HUGO GUERRERO TORRES

AÑO 2023

PLANTEAMIENTO DEL PROBLEMA

La seguridad de la información es un tema sensible, de gran importancia para los usuarios móviles debido a que las aplicaciones que utilizan pueden contener información personal delicada que, en caso de ser filtrada por ciberdelincuentes, puede perjudicar la identidad del usuario, su dispositivo y la imagen y credibilidad de la empresa que brinda la aplicación. Las vulnerabilidades de seguridad en las aplicaciones móviles pueden variar dependiendo de la plataforma o la propia aplicación, y también hay preocupaciones acerca de posibles ataques desde el lado del servidor, el lado del cliente y las redes de comunicación.

El uso de aplicaciones Android inseguras puede tener graves consecuencias para la seguridad y privacidad de la empresa, así como para su productividad y reputación. Es importante que las organizaciones implementen medidas de seguridad sólidas para proteger sus dispositivos móviles y que fomenten el uso de aplicaciones seguras y confiables.

Las aplicaciones inseguras pueden permitir que los datos empresariales se filtren o se divulguen a terceros no autorizados, esto podría incluir información confidencial de la empresa, como datos financieros, información de clientes o datos de propiedad intelectual; así mismo, pérdida de productividad, las aplicaciones inseguras pueden ser propensas a fallos y problemas técnicos que pueden afectar la productividad de los empleados. Además, los empleados pueden perder tiempo y recursos al tratar de solucionar problemas técnicos o al tener que reinstalar o buscar alternativas para aplicaciones inseguras.

Una consecuencia grave de aplicaciones inseguras es la afectación a la empresa en cuanto al daño a la reputación, esto es, si los datos de la empresa se ven comprometidos debido al uso de aplicaciones inseguras, esto puede dañar la reputación de la empresa y la confianza de los clientes y socios comerciales.

Además de que implica responsabilidad legal, esto es si los datos de los clientes o de la empresa se ven comprometidos debido al uso de aplicaciones inseguras, la empresa puede ser considerada responsable legalmente y enfrentar sanciones o multas.

Uno de los problemas más significativos que enfrentan los usuarios de teléfonos móviles en Ecuador es la falta de acceso a teléfonos móviles de calidad y de bajo costo. Esto ha llevado a que muchos usuarios tengan que comprar dispositivos móviles baratos y de baja calidad que pueden tener problemas de seguridad y privacidad.

Según un informe del Banco Interamericano de Desarrollo (BID) publicado en el año 2019, solo el 54% de la población ecuatoriana tiene acceso a un teléfono móvil inteligente, y la mayoría de ellos son modelos de bajo costo. Además, la falta de inversión en infraestructura y tecnología de comunicaciones ha dejado a algunas zonas del país sin acceso a servicios de comunicación móvil confiables y de alta calidad.

Otro problema común en Ecuador es el robo de teléfonos móviles, que puede ser un riesgo significativo para los usuarios y sus datos personales. Según datos del Ministerio del Interior de Ecuador, se reportaron más de 100,000 robos de teléfonos móviles en el país en el año 2020.

Además, el uso de aplicaciones móviles inseguras y el phishing (ataques de suplantación de identidad) también son problemas frecuentes en Ecuador. En el año 2021, la Unidad de Investigación de Delitos Informáticos de la Policía Nacional de Ecuador reportó un aumento en los casos de phishing a través de aplicaciones de mensajería instantánea.

OBJETIVOS

Objetivo general:

Realizar un análisis de vulnerabilidades de las aplicaciones Android utilizadas en gestión de empresas.

Objetivos específicos:

- Identificar y evaluar herramientas que permitan descubrir vulnerabilidades en aplicaciones Android
- Identificar las vulnerabilidades de las aplicaciones Android utilizadas en la gestión de empresas comerciales.
- Recomendar las mejores prácticas entorno a la calidad de software para producir aplicaciones móviles confiables.

JUSTIFICACIÓN

En los actuales momentos en que vive la tecnología resulta importante y justificable el realizar un caso de estudio que tenga relación con analizar las vulnerabilidades de las aplicaciones Android que son utilizadas por la gestión comercial de las empresas comúnmente aplicaciones las solemos encontrar en la Play Store sin embargo también representan riesgos potenciales que deben ser analizados.

En el mundo se mueven billones de dólares a causa de la seguridad de la información cada año y es importante que se fije la mirada también a las aplicaciones móviles porque son un contacto directo entre el usuario y la empresa y las debilidades que estas puedan tener podrían representar graves acontecimientos tanto para los clientes como para las organizaciones que las utilizan.

Android se ha caracterizado por permitir cierta inyección de códigos maliciosos en sus aplicaciones que muchas empresas a propósito las incluyen y también estas son vulneradas por terceros ya sea por malware o códigos maliciosos que sin querer el usuario descarga al visitar algún sitio inseguro, En este sentido es importante este tipo de investigación técnica como lo es un caso de estudio porque reúne criterios y documentación que permiten analizar de distintas maneras situaciones críticas de las tecnologías móviles y estas puedan ser luego consultadas por más técnicos.

El uso de aplicaciones Android en la gestión de empresas se ha vuelto cada vez más común en la era digital. Estas aplicaciones son utilizadas por empresas para una amplia variedad de tareas, como la gestión de finanzas, la comunicación interna, el seguimiento de pedidos y la gestión de relaciones con los clientes, entre otras. Sin embargo, el uso de aplicaciones móviles también presenta desafíos en términos de seguridad y privacidad.

La vulnerabilidad de las aplicaciones móviles es una preocupación creciente debido a los riesgos de seguridad asociados con ellas. Los dispositivos móviles son vulnerables a una variedad de ataques, como el malware y la suplantación de identidad, lo que puede comprometer la seguridad de la información empresarial confidencial y la privacidad de los usuarios.

El análisis de vulnerabilidades de las aplicaciones Android utilizadas en la gestión de empresas es un tema de investigación importante porque ayuda a identificar los riesgos asociados con el uso de estas aplicaciones y desarrollar estrategias para minimizar estos riesgos. Este análisis puede incluir la identificación de vulnerabilidades conocidas y desconocidas en el código de la aplicación, la evaluación de los permisos requeridos por la aplicación y la identificación de las posibles brechas de seguridad.

Este caso de estudio también puede contribuir a la creación de mejores prácticas de seguridad para el desarrollo de aplicaciones móviles empresariales. Al comprender las vulnerabilidades comunes en las aplicaciones móviles, los desarrolladores pueden tomar medidas preventivas para asegurar que sus aplicaciones sean seguras y confiables.

LÍNEA DE INVESTIGACIÓN

Este documento de caso de estudio, tiene relación con la línea de investigación de Sistemas de información y comunicación, emprendimiento e innovación, ya que es un tema relacionado los sistemas de información desplegados en forma de aplicaciones para teléfonos inteligentes o tablets enfocados a empresas; así mismo, esta línea de investigación permite encarrilar el estudio de caso que se relaciona con la seguridad de los sistemas Operativos Android que utilizan los dispositivos móviles y los especialistas en esta profesión de ingenieros en sistemas de información requieren comprender elementos fundamentales que están vinculados con las comunicaciones y redes asociados a todo componente de software.

MARCO CONCEPTUAL

Las Empresas y Las Aplicaciones Móviles

En el mundo empresarial actual, las aplicaciones móviles han tenido un impacto importante. Según las investigaciones de García (2019), estas aplicaciones se han convertido en herramientas fundamentales para mejorar la productividad y la eficiencia de las empresas, además de incrementar la satisfacción y la lealtad de los clientes. Las aplicaciones móviles también pueden contribuir a la toma de decisiones empresariales al permitir el análisis de datos en tiempo real.

Según el estudio llevado a cabo por Molina-Castillo, F. J., Sánchez-Fernández, J., y Gázquez-Abad, J. C. (2016), las empresas que incluyen aplicaciones móviles en su estrategia de negocio pueden obtener una ventaja competitiva importante. Estas aplicaciones pueden facilitar a las empresas el acceso a nuevos mercados y clientes, así como mejorar la relación con los clientes actuales.

No obstante, es crucial tener en cuenta los obstáculos vinculados a la introducción de aplicaciones móviles en las empresas. En consonancia con el estudio llevado a cabo por González-Serrano, L. A., González-Serrano, M. H., y Fernández-Villacañas Marín, C. (2019), estos obstáculos implican cuestiones como la protección y privacidad de los datos, la integración con otros sistemas empresariales y la gestión del cambio organizacional.

> *Las aplicaciones móviles se han convertido en una herramienta importante en el entorno empresarial actual, ya que pueden mejorar la productividad y la eficiencia, así como aumentar la satisfacción del cliente y la fidelidad. Además, las empresas que adoptan las aplicaciones móviles pueden obtener una ventaja competitiva significativa al llegar a nuevos mercados y mejorar la relación con los clientes existentes. Sin embargo, a pesar de sus beneficios, la implementación de aplicaciones móviles en las*

empresas también presenta desafíos, como la seguridad y privacidad de los datos, la integración con otros sistemas empresariales y la gestión del cambio organizacional.

Las empresas y las aplicaciones móviles tienen una relación estrecha y compleja que puede ser beneficiosa si se implementa adecuadamente. Se requiere una cuidadosa planificación y gestión para maximizar los beneficios y minimizar los desafíos asociados con la implementación de aplicaciones móviles en el entorno empresarial.

Las Aplicaciones Móviles y Su Relación Con La Competitividad

Las aplicaciones móviles pueden ser una herramienta clave para mejorar la competitividad de las empresas. Según Molina-Castillo, Sánchez-Fernández, y Gázquez-Abad (2016), las empresas que adoptan las aplicaciones móviles como parte de su estrategia de negocio pueden obtener una ventaja competitiva significativa al llegar a nuevos mercados y clientes, así como mejorar la relación con los clientes existentes. Además, García (2019) señala que las aplicaciones móviles pueden mejorar la productividad y la eficiencia de las empresas, así como la toma de decisiones empresariales mediante el análisis de datos en tiempo real.

Sin embargo, también es importante considerar los desafíos asociados con la implementación de aplicaciones móviles en las empresas. Según González-Serrano, González-Serrano y Fernández-Villacañas Marín (2019), los desafíos incluyen la seguridad y la privacidad de los datos, la integración con otros sistemas empresariales y la gestión del cambio organizacional.

Las aplicaciones móviles pueden mejorar la competitividad de las empresas al permitirles llegar a nuevos mercados y mejorar la relación con los clientes existentes, además de mejorar la productividad y eficiencia y facilitar la toma de decisiones

empresariales en tiempo real. Sin embargo, su implementación también puede presentar desafíos, como la seguridad y privacidad de los datos, la integración con otros sistemas empresariales y la gestión del cambio organizacional.

La Aceptación De Aplicaciones Móviles A Nivel Regional

Un estudio de mercado realizado por eMarketer en 2021 revela que el uso de aplicaciones móviles en Sudamérica continúa en aumento y se espera que alcance los 250 millones de usuarios en 2022 (eMarketer, 2021). Además, según el reporte de App Annie de 2020, Brasil y México son los dos principales mercados de aplicaciones móviles en la región, seguidos de Argentina, Colombia y Chile (App Annie, 2020).

Por lo que se estima un crecimiento cada vez mayor y el uso seguramente como ya lo está haciendo, superará al de las PC, por lo que todo debe apuntar al uso y desarrollo de app móviles

Los Límites De La Transformación Tecnológica

La transformación tecnológica puede tener límites y desafíos importantes que deben ser considerados por las organizaciones. Según Lacity y Willcocks (2019), algunos de estos límites incluyen la resistencia al cambio por parte de los empleados, la complejidad y el costo de implementar nuevas tecnologías, la falta de habilidades y conocimientos técnicos por parte del personal y la necesidad de adaptarse a la cultura y los procesos existentes de la organización.

Además, según Chui, Manyika y Miremadi (2019), la transformación tecnológica también puede tener impactos negativos en la sociedad, como la creación de nuevas brechas económicas y sociales, el aumento del desempleo debido a la automatización y la falta de protección de la privacidad y los datos personales de los usuarios.

Aunque la transformación tecnológica puede ofrecer beneficios significativos para las organizaciones, también es importante considerar sus límites y desafíos, así como su impacto en la sociedad.

Según el informe "The State of Application Modernization" (2021), cerca del 70% de las organizaciones ya utilizan entre una y cuatro aplicaciones, lo que indica una mayor inversión en la transformación digital. Las decisiones de adopción de aplicaciones móviles se basan principalmente en la satisfacción del cliente y la eficiencia y satisfacción del empleado. Sin embargo, también hay organizaciones que han tomado esta decisión debido a la falta de modernización, lo que ha afectado la consecución de sus objetivos y la escalabilidad de los servicios críticos.

Lo anterior indica una creciente inversión en la transformación digital. Las decisiones de adopción de aplicaciones móviles se basan principalmente en la satisfacción del cliente y la eficiencia y satisfacción del empleado. No obstante, algunas organizaciones han optado por adoptar aplicaciones móviles debido a la falta de modernización, lo que ha afectado la consecución de sus objetivos y la escalabilidad de los servicios críticos.

Cómo Hacer Una Transición Hacia Aplicaciones Móviles De Forma Segura

La transición hacia aplicaciones móviles de forma segura es un tema cada vez más importante debido al aumento del uso de dispositivos móviles en todo el mundo. Según Hussain et al. (2020), la seguridad de las aplicaciones móviles es esencial para garantizar la protección de los datos y la privacidad de los usuarios. Kim et al. (2019) destacan la necesidad de examinar las vulnerabilidades comunes de las aplicaciones móviles y discutir soluciones para abordarlas.

En este contexto, Noor et al. (2020) presentan una revisión sistemática de la literatura existente sobre las preocupaciones de seguridad y privacidad en el desarrollo de aplicaciones

móviles, identificando una serie de riesgos de seguridad y privacidad, como la fuga de datos y la falta de autenticación de usuarios, y proponen soluciones para abordarlos. Krasnova et al. (2021) presentan una serie de pautas para el diseño de aplicaciones móviles seguras dirigidas a desarrolladores, enfatizando la importancia de la autenticación de usuarios, el cifrado de datos y la gestión de permisos de usuario para garantizar la seguridad de las aplicaciones móviles.

> *La transición hacia aplicaciones móviles de forma segura es un tema de creciente importancia que requiere la atención de desarrolladores y usuarios por igual, y se necesitan soluciones para abordar las vulnerabilidades y riesgos asociados con las aplicaciones móviles.*

Las Aplicaciones Android Utilizadas En La Gestión De Las Empresas

De acuerdo con Calvo-Flores, Cepeda-Carrión y García-Villalonga (2017), las aplicaciones móviles Android son cada vez más populares en la gestión empresarial debido a su portabilidad y facilidad de uso. Estas aplicaciones pueden mejorar la eficiencia y la productividad de las empresas al permitir el acceso a la información y recursos empresariales en cualquier momento y lugar. Fernández-Cardador y Pérez-López (2018) destacan que las aplicaciones móviles también pueden ser útiles para la gestión de relaciones con los clientes y la recopilación de datos para la toma de decisiones empresariales, incluyendo áreas como la gestión de inventarios y finanzas.

Sin embargo, según Villarreal-Castañeda y Ortiz-García (2017), es crucial que las empresas consideren la seguridad de la información y la privacidad de los datos en el desarrollo y la implementación de aplicaciones móviles empresariales. Es necesario evaluar la seguridad de las aplicaciones antes de implementarlas y tomar medidas adicionales de seguridad, como la autenticación de usuarios y el cifrado de datos.

Fortaleciendo estas ideas, aunque las aplicaciones móviles Android pueden ser beneficiosas para la gestión empresarial, es importante que las empresas consideren la seguridad de la información y la privacidad de los datos al utilizarlas.

Además, las aplicaciones móviles Android pueden ser una herramienta valiosa para la gestión empresarial, mejorando la eficiencia y la productividad, y facilitando la toma de decisiones. Sin embargo, es importante que las empresas consideren la seguridad de la información y la privacidad de los datos al implementar aplicaciones móviles en su gestión.

Como Afecta De Modo General La Inseguridad En Las Aplicaciones A Las Organizaciones

La inseguridad en las aplicaciones móviles puede tener un impacto significativo en las organizaciones. Según un estudio realizado por Kaur y Singh (2021), las vulnerabilidades de seguridad en las aplicaciones móviles pueden resultar en la pérdida de datos confidenciales de la empresa, el robo de información y la interrupción del negocio. Además, estas vulnerabilidades pueden poner en peligro la privacidad y seguridad de los usuarios de la aplicación, lo que puede afectar negativamente la reputación de la empresa y la confianza del cliente en la marca.

De acuerdo con Kim, Yoon y Lee (2019), las consecuencias de la inseguridad en las aplicaciones móviles pueden ser aún más graves en el caso de las aplicaciones empresariales, ya que estas pueden contener información sensible y confidencial. La exposición de esta información a personas no autorizadas puede resultar en pérdidas financieras, problemas legales y daños en la imagen de la empresa.

Fortaleciendo lo antes mencionado, la inseguridad en las aplicaciones móviles puede tener un impacto significativo en las organizaciones, incluyendo la pérdida de datos confidenciales, el robo de información, la interrupción del negocio y la pérdida de confianza del cliente.

Por lo tanto, es crucial que las empresas adopten medidas de seguridad adecuadas para proteger sus aplicaciones móviles y la información que contienen.

Vulnerabilidades De Android Que Afectan A Las Empresas

Las vulnerabilidades de Android son una preocupación importante para las empresas, ya que según la investigación de Gutiérrez y Segovia (2018), estas vulnerabilidades pueden permitir que los atacantes accedan a información confidencial de las empresas, como datos financieros y de clientes.

Además, el estudio de Huertas (2019) señala que estas vulnerabilidades pueden interrumpir las operaciones comerciales y reducir la productividad de los empleados, lo que puede tener un impacto negativo en la continuidad del negocio y en las finanzas de las empresas.

Por lo tanto, es crucial que las empresas tomen medidas proactivas para abordar las vulnerabilidades de seguridad en las aplicaciones móviles y reducir los riesgos asociados.

Las vulnerabilidades de Android pueden tener un impacto significativo en la seguridad, la productividad y la continuidad del negocio de las empresas. Es importante que las empresas tomen medidas proactivas para protegerse de estas vulnerabilidades, incluyendo la actualización regular de sus sistemas operativos y aplicaciones, así como la implementación de medidas de seguridad adicionales, como firewalls y software antivirus.

Estructura Android Y Modelo De Seguridad

Android es un sistema operativo móvil desarrollado por Google que se basa en el núcleo de Linux. El modelo de seguridad de Android se basa en el principio de "defensa en profundidad", que incluye múltiples capas de protección para garantizar la seguridad del sistema y los datos del usuario (Chin, Chen & Li, 2019).

El modelo de seguridad de Android se compone de cuatro niveles: el nivel del kernel, el nivel del espacio de usuario, el nivel de aplicaciones y el nivel de permisos (Barrera & Lindqvist, 2020). El nivel del kernel es la capa más baja del sistema y está a cargo de gestionar los recursos del hardware y las interacciones con el software. El nivel del espacio de usuario incluye la mayoría de las aplicaciones del sistema y se encarga de la gestión de los procesos y la memoria. El nivel de aplicaciones se encarga de ejecutar las aplicaciones de usuario, mientras que el nivel de permisos gestiona los permisos de las aplicaciones y los servicios que tienen acceso a los datos y recursos del sistema.

El modelo de seguridad de Android también incluye medidas de seguridad adicionales, como la verificación de la firma de las aplicaciones, la implementación de políticas de permisos y el cifrado de datos. Además, Google publica regularmente actualizaciones de seguridad para el sistema operativo y las aplicaciones para abordar las vulnerabilidades y mejorar la seguridad del sistema (Calleja, Urueña & Brizuela, 2019).

> *El modelo de seguridad de Android se basa en múltiples capas de protección para garantizar la seguridad del sistema y los datos del usuario. Además, incluye medidas de seguridad adicionales y actualizaciones regulares para abordar las vulnerabilidades y mejorar la seguridad del sistema.*
>
> *Para este cado de estudio, este componente de texto resulta muy aportante, ya que en necesario conocer su estructura para proporcionar criterios de seguridad.*

> *En su arquitectura, Android tiene un ciclo de desarrollo destinado a reforzar las vulnerabilidades en la seguridad de los dispositivos móviles. Este ciclo incluye cuatro etapas: 1- una revisión del diseño, 2 - una prueba de penetración, 3- una revisión del código y 4 -una respuesta a incidentes.*

Vulnerabilidad.

Las vulnerabilidades en aplicaciones móviles pueden tener su origen en múltiples factores, como la falta de pruebas exhaustivas de seguridad, la falta de atención a las actualizaciones y parches de seguridad, y la inclusión de código malicioso o vulnerabilidades en bibliotecas de terceros. Según el estudio realizado por Arshad et al. (2020), las vulnerabilidades más comunes en aplicaciones móviles incluyen la falta de verificación de autenticidad, la falta de cifrado de datos, la inyección de SQL, la divulgación de información confidencial y la explotación de debilidades en la autenticación.

Además, según el estudio realizado por Chang et al. (2021), la popularidad de las aplicaciones móviles también puede contribuir a la aparición de vulnerabilidades, ya que los atacantes pueden verlas como objetivos atractivos para la explotación. Es importante que las empresas y desarrolladores de aplicaciones móviles implementen medidas proactivas para abordar estas vulnerabilidades, incluyendo la realización de pruebas de seguridad regulares, la atención a las actualizaciones y parches de seguridad, y la implementación de políticas de seguridad sólidas durante el proceso de desarrollo.

> *Fortaleciendo la idea de los textos antes mencionados, el origen de las vulnerabilidades en las aplicaciones móviles se debe a varios factores, como la falta de pruebas adecuadas durante el desarrollo, la falta de actualizaciones y parches de seguridad, y la falta de conciencia por parte de los usuarios sobre las amenazas de seguridad.*

Así mismo, en cuanto a la seguridad en la gestión empresarial, es importante que las organizaciones tomen medidas proactivas para protegerse de estas vulnerabilidades, como asegurarse de que sus aplicaciones móviles sean desarrolladas y probadas adecuadamente antes de su implementación, implementar medidas de seguridad adicionales, como firewalls y software antivirus, y educar a sus empleados sobre las amenazas de seguridad en las aplicaciones móviles y cómo evitarlas. Esto ayudará a proteger la información confidencial y la propiedad intelectual de la empresa, así como a garantizar la continuidad del negocio.

MARCO METODOLOGICO

En el contexto de esta investigación plasmada como caso de estudio análisis de vulnerabilidades de las aplicaciones Android utilizadas en gestión de empresas, es crucial seleccionar una metodología de investigación adecuada que aborde el problema de estudio y cumpla con los objetivos de investigación.

Las metodologías comunes incluyen el estudio de casos, las entrevistas con expertos y el análisis de documentos relacionados con las vulnerabilidades de las aplicaciones Android. Además, se utilizará una metodología cualitativa para obtener datos y percepciones de expertos que no son medibles en muchos casos.

Esta investigación cualitativa, porque se enfocará en comprender y describir fenómenos complejos y subjetivos, tales como percepciones, valores, creencias, experiencias y comportamientos humanos, desde la perspectiva de los participantes en el estudio.

En lugar de recoger datos numéricos o estadísticos, esta investigación cualitativa se centra en el análisis de datos textuales y visuales, como transcripciones de entrevistas, observaciones, diarios y documentos, con el fin de identificar patrones, temas y relaciones entre los datos. Los métodos utilizados en la investigación cualitativa incluyen entrevistas, grupos focales, observación participante, análisis de contenido y análisis de discurso, entre otros; esta metodología es muy útil para explorar cómo la tecnología afecta a las empresas el uso sobre una tecnología en particular.

Como técnica de recopilación de datos se presenta en este caso de estudio, el instrumento entrevista, aplicable a expertos, que serán 3 en total como población para esta investigación, con un perfil de técnicos en Sistemas o Afines, con experiencia en asuntos de desarrollo de software y gestión de empresas; esto con la finalidad de comparar los resultados

obtenidos, analizar y discutir las contribuciones de expertos relacionados con la investigación bibliográfica.

Las preguntas realizadas a los entrevistados fueron las siguientes:

Pregunta 1. Describa las formas comunes en las que una App móvil puede afectar a la gestión operativa de una empresa, cuando este software es operado por clientes y tiene problemas de vulnerabilidad

Pregunta 2. Con la finalidad de conocer las mejores prácticas, si usted es un desarrollador de Aplicaciones móviles que estrategias utiliza para brindarle protección.

Pregunta 3. Desde el punto de vista de un asesor informático, que recomendaciones le brindaría a una organización, si esta se ve afectada por alguna aplicación móvil insegura.

RESULTADOS

Luego de realizar las entrevistas a los expertos, reflejadas ampliamente en (Anexo 1) especialistas en sistemas y tecnologías, todos conocedores del tema relacionado al presente caso de estudio; por lo que cada pregunta del cuestionario además está relacionada con alguno de los objetivos planteados en este documento; es así que el cuestionamiento de: **Describa las formas comunes en las que una App móvil puede afectar a la gestión operativa de una empresa, cuando este software es operado por clientes y tiene problemas de vulnerabilidad**; Responde el **Profesional 1**: Las posibles consecuencias de tener vulnerabilidades en la seguridad de una aplicación móvil. Estas vulnerabilidades pueden permitir que los atacantes roben información confidencial de los usuarios, expongan datos almacenados en la aplicación a terceros, accedan a áreas restringidas de la aplicación, distribuyan malware y realicen ataques de denegación de servicio. Es importante tener en cuenta

la seguridad de las aplicaciones móviles para proteger la información privada y confidencial de los usuarios y de la empresa.

Profesional 2: Que las aplicaciones móviles inseguras pueden poner en riesgo la infraestructura de la empresa, ya que los atacantes pueden utilizarlas para realizar ataques contra sistemas críticos de la empresa. Además, estas aplicaciones también pueden exponer la propiedad intelectual de la empresa a posibles robos por parte de los atacantes, lo que puede afectar su competitividad. Es importante tener en cuenta la seguridad de las aplicaciones móviles para proteger la infraestructura y los datos confidenciales de la empresa.

Profesional 3:

que las aplicaciones móviles inseguras pueden ser utilizadas para interrumpir el servicio de la empresa, mediante ataques de denegación de servicio que impiden a los usuarios acceder a los servicios y a la empresa realizar operaciones críticas. Esto puede provocar una pérdida significativa de ingresos y dañar la reputación de la empresa. Es importante tomar medidas de seguridad adecuadas para evitar estas situaciones y garantizar la continuidad del servicio.

En relación a la pregunta: Con la finalidad de conocer las mejores prácticas, si usted es un desarrollador de Aplicaciones móviles que estrategias utiliza para brindarle protección.? Responde el Ing. Saltos lo siguiente: la importancia de implementar medidas de autenticación y autorización seguras en las aplicaciones móviles, como contraseñas fuertes, autenticación multifactor y token de autenticación de sesión. Estas medidas aseguran que los usuarios que acceden a la aplicación sean quienes dicen ser y tengan los permisos adecuados para acceder a los recursos y datos de la aplicación. También se menciona la importancia de encriptar los datos de la aplicación de forma adecuada según la naturaleza operativa.

Profesional 1: es importante realizar pruebas de seguridad regulares en las aplicaciones móviles para detectar y corregir vulnerabilidades y debilidades en la seguridad. Estas pruebas

pueden incluir pruebas de penetración, pruebas de vulnerabilidad y auditorías de seguridad. Es fundamental tener en cuenta la seguridad de las aplicaciones móviles para garantizar la protección de los datos confidenciales y la continuidad del servicio.

Profesional 2:

Tomaría las medidas de seguridad y de funcionalidad que me han requerido

En relación a: **Basado en vuestra experiencia, que herramientas permiten un análisis para detectar una posible falla y poder garantizar una usabilidad adecuada** Responde Profesional 1, lo siguiente: las técnicas para asegurar la seguridad de las aplicaciones móviles es el análisis estático de código, que consiste en revisar el código fuente de la aplicación para identificar posibles vulnerabilidades de seguridad. Se pueden utilizar herramientas automatizadas para buscar patrones de código comunes que se sabe que son inseguros, como el uso de funciones de cifrado débiles o la falta de validación de entrada de datos. Esta técnica ayuda a identificar posibles vulnerabilidades de seguridad en la etapa de desarrollo de la aplicación.

Profesional 2: la revisión de diseño y arquitectura es una técnica para identificar posibles vulnerabilidades de seguridad en una aplicación móvil. Esta técnica consiste en revisar el diseño y la arquitectura de la aplicación para evaluar cómo maneja la autenticación, el almacenamiento de datos, el cifrado y otras funciones de seguridad. La revisión de diseño y arquitectura ayuda a identificar posibles vulnerabilidades de seguridad en la etapa de planificación y diseño de la aplicación.

Profesional 3: La prueba de usuario final es una técnica que implica realizar pruebas con usuarios reales para detectar posibles vulnerabilidades en una aplicación móvil. Estas pruebas pueden incluir pruebas de seguridad de la interfaz de usuario, como intentar acceder a funciones restringidas o manipular la entrada de datos para provocar comportamientos inesperados. La prueba de usuario final es útil para identificar posibles vulnerabilidades que pueden ser pasadas por alto en pruebas automatizadas o revisiones de código.

Desde el punto de vista de un asesor informático, que recomendaciones le brindaría a una organización, si esta se ve afectada por alguna aplicación móvil insegura.? Responde el **Profesional 1**: Aislar la App: esta técnica implica limitar el acceso de la aplicación móvil a los recursos y datos del dispositivo y de la red. Esto puede incluir el uso de técnicas como la virtualización, contenedores y aislamiento de red para reducir la superficie de ataque y limitar el impacto de las posibles brechas de seguridad.

Identificar la causa raíz: es importante investigar y comprender las causas del problema para tomar medidas preventivas en el futuro. Esto puede incluir realizar un análisis forense en la aplicación para determinar cómo se produjo la brecha de seguridad y tomar medidas para corregir las debilidades detectadas.

Profesional 2: se pueden implementar medidas de seguridad adicionales, como el uso de herramientas de monitoreo y análisis de seguridad para detectar y prevenir futuros ataques, la implementación de actualizaciones de seguridad y parches, y la formación del personal sobre las mejores prácticas de seguridad. También se debe establecer un plan de respuesta a incidentes para manejar rápidamente cualquier brecha de seguridad que ocurra en el futuro.

Profesional 3: Detener el uso de la aplicación pues si la aplicación se encuentra en uso, es importante detener el uso de la misma inmediatamente para evitar que se produzcan más daños.

DISCUSION DE RESULTADOS

Para fortalecer este documento, se han tomado los resultados de las entrevistas y se los ha contrastado con la teoría relacionada en el marco conceptual, es así que:

Los ingenieros Profesional 1, Profesional 2 y Profesional 3, coinciden en que las aplicaciones móviles inseguras pueden tener graves consecuencias para la gestión operativa de una empresa. Estas vulnerabilidades pueden permitir que los atacantes roben información confidencial, expongan datos a terceros, accedan a áreas restringidas, distribuyan malware y realicen ataques de denegación de servicio, lo que puede poner en riesgo la infraestructura de la empresa, la propiedad intelectual, la continuidad del servicio y la reputación de la empresa. Por lo tanto, es crucial tomar medidas de seguridad adecuadas para proteger la información privada y confidencial de los usuarios y de la empresa, garantizar la continuidad del servicio y evitar situaciones que puedan afectar negativamente a la empresa.

> *En concordancia con el marco conceptual, además se indica que, las vulnerabilidades de Android pueden tener un impacto significativo en la seguridad, la productividad y la continuidad del negocio de las empresas. Es importante que las empresas tomen medidas proactivas para protegerse de estas vulnerabilidades, incluyendo la actualización regular de sus sistemas operativos y aplicaciones, así como la implementación de medidas de seguridad adicionales, como firewalls y software antivirus.*

Los expertos, Profesional 1 y 3 destacan la importancia de implementar medidas de autenticación y autorización seguras, encriptar los datos de la aplicación y realizar pruebas regulares de seguridad para detectar y corregir vulnerabilidades en las aplicaciones móviles. Estas medidas son fundamentales para garantizar la protección de los datos confidenciales y la

continuidad del servicio. Por otro lado, el Profesional 3 indica que seguiría las medidas de seguridad y funcionalidad requeridas.

> *Vinculando estos resultados con el componente teórico del marco conceptual se tiene que: es importante que las organizaciones adopten medidas proactivas para protegerse de vulnerabilidades en las aplicaciones móviles, como desarrollar y probar adecuadamente las aplicaciones, implementar medidas de seguridad adicionales y educar a los empleados sobre las amenazas de seguridad en las aplicaciones móviles. Estas medidas ayudarán a proteger la información confidencial y la propiedad intelectual de la empresa, así como a garantizar la continuidad del negocio.*

Por último, Los Profesional 1 y 2 recomiendan medidas proactivas para protegerse de futuras vulnerabilidades, como el aislamiento de la aplicación móvil, identificación de la causa raíz, implementación de herramientas de monitoreo y análisis de seguridad, actualizaciones de seguridad y parches, formación del personal en seguridad y establecimiento de un plan de respuesta a incidentes. Por otro lado, el Profesional 3 indica la importancia de detener inmediatamente el uso de la aplicación afectada.

> *Para fortalecer esta idea, se ha tomado del marco conceptual el componente relacionado con la competitividad: Las aplicaciones móviles pueden mejorar la competitividad de las empresas al permitirles llegar a nuevos mercados y mejorar la relación con los clientes existentes, además de mejorar la productividad y eficiencia y facilitar la toma de decisiones empresariales en tiempo real. Sin embargo, tener una aplicación con funcionamiento riesgoso, pone vulnerable cualquier funcionamiento o desarrollo comercial, porque lo que se desea es estar con disponibilidad operativa siempre.*

CONCLUSIONES

Las vulnerabilidades que se han identificado son la inyección de código malicioso, la fuga de datos sensibles, los problemas de autenticación, las vulnerabilidades en la red, los problemas de seguridad en el almacenamiento local y los ataques de phishing. Los desarrolladores deben tomar medidas para proteger sus aplicaciones y los usuarios deben tomar medidas para proteger sus dispositivos y datos personales.

Las aplicaciones móviles inseguras pueden tener graves consecuencias para la gestión operativa de una empresa; estas vulnerabilidades pueden permitir que los atacantes roben información confidencial, expongan datos a terceros, accedan a áreas restringidas, distribuyan malware y realicen ataques de denegación de servicio, lo que puede poner en riesgo la infraestructura de la empresa; así mismo las vulnerabilidades de Android pueden tener un impacto significativo en la seguridad, la productividad y la continuidad del negocio de las empresas.

Se destaca la importancia de implementar medidas de autenticación y autorización seguras, encriptar los datos de la aplicación y realizar pruebas regulares de seguridad para detectar y corregir vulnerabilidades en las aplicaciones móviles; es fundamentar para garantizar la protección de los datos confidenciales y la continuidad de los servicios.

En las organizaciones el componente relacionado con la competitividad de las empresas requiere de mejorar la productividad y eficiencia y facilitar la toma de decisiones empresariales en tiempo real. Sin embargo, tener una aplicación con funcionamiento riesgoso, pone vulnerable cualquier funcionamiento o desarrollo comercial, porque lo que se desea es estar con disponibilidad operativa siempre.

La inseguridad en las aplicaciones móviles puede tener un gran impacto en las organizaciones, incluyendo la pérdida de datos y daños a la reputación. La estructura de la

arquitectura del sistema operativo Android indica que las capas inferiores son más susceptibles a tener más vulnerabilidades y el ciclo de desarrollo de Android se enfoca en fortalecer las debilidades en seguridad.

RECOMENDACIONES

Se recomienda a los Gerentes de Tecnologías, implementar medidas de seguridad adecuadas, que protejan la información privada y confidencial de los usuarios y la infraestructura de la empresa, esto inicialmente con una política bien estructurada y socializada.

Realizar pruebas de seguridad regulares, por lo que es importante realizar pruebas de seguridad regulares para identificar vulnerabilidades en la seguridad de una aplicación móvil y corregirlas antes de que se conviertan en problemas graves; podría usar la herramienta OWASP ZAP para detectar vulnerabilidades en aplicaciones web y móviles. La herramienta puede utilizarse para realizar pruebas de penetración, escanear vulnerabilidades y realizar pruebas de seguridad en general.

Además, se recomienda capacitar al personal en seguridad de aplicaciones móviles, es crucial que el personal de la empresa es decir los desarrolladores estén capacitado en seguridad de aplicaciones móviles para que puedan identificar y responder adecuadamente a las posibles amenazas.

Seleccionar cuidadosamente aplicaciones de terceros, es decir, que es necesario tener cuidado al seleccionar aplicaciones de terceros y verificar que cumplen con los requisitos de seguridad necesarios antes de implementarlas en la empresa.

Además, es necesario educar a los usuarios finales sobre las mejores prácticas de seguridad en las aplicaciones móviles, como la importancia de no compartir información

confidencial y de usar contraseñas seguras. También es importante fomentar una cultura de seguridad en la organización y asegurarse de que todos los empleados estén informados sobre las políticas de seguridad de la empresa en cuanto al uso de aplicaciones móviles.

Es importante también recomendar a los gerentes de tecnologías, tomar como buenas prácticas el asegurarse de que las actualizaciones se implementen regularmente en las aplicaciones móviles para garantizar que cualquier vulnerabilidad conocida se aborde y se solucione. Además, se deben monitorear y auditar regularmente las aplicaciones móviles para identificar y abordar cualquier problema de seguridad que pueda surgir.

REFERENCIAS BIBLIOGRAFICAS

App Annie. (2020). The State of Mobile 2021. Retrieved from https://www.appannie.com/en/go/state-of-mobile-2021/

Arshad, M., et al. (2020). A systematic literature review on mobile application security testing. Journal of Information Security and Applications, 52, 102515.

Barrera, D., & Lindqvist, U. (2020). A survey of the security landscape of mobile devices using Android. ACM Computing Surveys (CSUR), 53(5), 1-36.

Calleja, D. F., Urueña, M., & Brizuela, C. (2019). Android operating system security: An up-to-date review. Computers & Security, 81, 353-373.

Calvo-Flores, M. D., Cepeda-Carrión, G., & García-Villalonga, F. J. (2017). Aplicaciones móviles y su impacto en la gestión empresarial. Revista de Investigación Académica, 1(56), 1-11.

Chang, C. H., et al. (2021). An empirical study of mobile application vulnerabilities in android and iOS platforms. IEEE Access, 9, 134759-134770.

Chin, Y. K., Chen, Y. L., & Li, Y. C. (2019). Enhancing the Security of Android Mobile Devices: A Review of Existing Approaches and Future Directions. IEEE Access, 7, 75894-75906.

Chui, M., Manyika, J., & Miremadi, M. (2019). What's now and next in analytics, AI, and automation. McKinsey Quarterly, 1-11.

Díaz-Gómez, E., & Sánchez-García, A. (2017). Vulnerabilidades en aplicaciones móviles y su impacto en la seguridad empresarial. Revista de Investigación Académica, 1(54), 1-11.

eMarketer. (2021, March 1). South America Mobile Users 2021: Trends and Forecast for 5 Countries and 9 Subregions. Retrieved from https://www.emarketer.com/content/south-america-mobile-users-2021

Fernández-Cardador, A., & Pérez-López, R. (2018). Aplicaciones móviles y su impacto en la gestión empresarial. Revista Electrónica de Investigación en Administración, 20(1), 1-15.

García, R. (2019). Mobile apps in business management. Journal of Business Research, 100, 485-493.

Gartner. (2020). Gartner Survey Reveals 70% of Organizations Have Invested or Plan to Invest in Customer Experience Technology. Retrieved from https://www.gartner.com/en/newsroom/press-releases/2020-10-14-gartner-survey-reveals-70--of-organizations-have-invested-or-plan-to-invest-in-customer-experience-technology

González-Serrano, L. A., González-Serrano, M. H., & Fernández-Villacañas Marín, C. (2019). Impact of mobile apps on business strategies. International Journal of Information Management, 48, 62-70.

Gutiérrez, A., & Segovia, J. (2018). Análisis de vulnerabilidades y amenazas en dispositivos móviles con sistema operativo Android. Revista de Investigación Académica, 1(55), 1-15.

Huertas, F. J. (2019). Análisis de las vulnerabilidades en dispositivos móviles Android. Revista Digital del CEI, 20(1), 1-10.

Hussain, A., Asad, M., Khan, M. A., & Khan, R. H. (2020). Securing Mobile Applications: A Systematic Literature Review. IEEE Access, 8, 8349-8371.

Kaur, H., & Singh, S. (2021). Security vulnerabilities in mobile applications: A review. International Journal of Advanced Intelligence Paradigms, 14(2), 107-124.

Kim, D. J., Yoon, C., & Lee, J. (2019). A survey of enterprise mobile application security challenges and solutions. Computers & Security, 85, 16-30.

Kim, D., Yoon, J., & Lee, K. (2019). Mobile Application Security: A Survey. IEEE Access, 7, 110922-110939.

Krasnova, H., Kovrigin, S., & Veltri, N. F. (2021). Guidelines for Secure Mobile App Development: Recommendations for Developers. In: MobileHCI '21: Proceedings of the 23rd International Conference on Human-Computer Interaction with Mobile Devices and Services, 1-13.

Lacity, M., & Willcocks, L. (2019). Beyond the hype: A guide to understanding and successfully implementing robotic process automation. The European Business Review, 67-70.

Molina-Castillo, F. J., Sánchez-Fernández, J., & Gázquez-Abad, J. C. (2016). Impact of mobile apps in competitive strategy. Journal of Business Research, 69(11), 4892-4897.

Noor, T. H., Al-Obeidat, F., Khasawneh, S., & Aboabdo, A. (2020). Security and privacy concerns in mobile application development: A systematic literature review. International Journal of Information Management, 52, 102050.

Villarreal-Castañeda, G. J., & Ortiz-García, J. J. (2017). Seguridad en aplicaciones móviles para la gestión empresarial. Revista de Investigación Académica, 1(55), 1-14.

Anexo 1

Diseño de Entrevista

Universidad Técnica de Babahoyo

Entrevista relacionada con: ANÁLISIS DE VULNERABILIDADES DE LAS APLICACIONES ANDROID UTILIZADAS EN GESTIÓN DE EMPRESAS

Nombre del Profesional: _____

Empresa:_____ Cargo: _____

1- **¿Describa las formas comunes en las que una App móvil puede afectar a la gestión operativa de una empresa, cuando este software es operado por clientes y tiene problemas de vulnerabilidad?**

2- **Con la finalidad de conocer las mejores prácticas, si usted es un desarrollador de Aplicaciones móviles que estrategias utiliza para brindarle protección.**

3- **Desde el punto de vista de un asesor informático, que recomendaciones le brindaría a una organización, si esta se ve afectada por alguna aplicación móvil insegura.?**