Machine Translated by Google
RCMOS – Revista Científica Multidisciplinaria El Conocimiento.
ISSN: 2675-9128. São Paulo-SP.

Año VII, vol. 2, 2026 | Envío: 04/05/2026 | Aceptación: 07/05/2026 | Publicación: 10/05/2026

La convergencia entre la ciberseguridad y las aplicaciones móviles en los ecosistemas empresariales.

La convergencia entre la ciberseguridad y las aplicaciones móviles en los ecosistemas empresariales
La convergencia entre la ciberseguridad y las aplicaciones móviles en los ecosistemas empresariales

Adriano Souza Reis

Tecnólogo en Gestión de Tecnologías de la Información (Uni-Anhanguera); Posgrado en Inteligencia Artificial, Desarrollo de Aplicaciones Móviles y Ciberseguridad (Faculdade Iguaçu); Doctor Honoris Causa en Tecnologías de la Información (UNISCECAP); Miembro de pleno derecho de ABRASCI.

RESUMEN

La creciente adopción de aplicaciones móviles en el entorno corporativo ha transformado significativamente la forma en que las organizaciones ejecutan procesos, comparten información y apoyan la toma de decisiones. La expansión de la movilidad ha proporcionado mayor agilidad operativa, pero también ha aumentado la superficie expuesta a las ciberamenazas, convirtiendo la seguridad de la información en un requisito estratégico en el desarrollo de software para dispositivos móviles. Este artículo analiza la relación entre el desarrollo de aplicaciones móviles y la ciberseguridad en los ecosistemas empresariales, abordando los principales riesgos asociados al uso de dispositivos móviles, así como las mejores prácticas para la protección de datos, la autenticación de usuarios, la comunicación segura y la monitorización continua de los entornos corporativos. La investigación se caracteriza por ser una revisión sistemática de la literatura, basada en libros, artículos científicos, normas técnicas y documentos producidos por instituciones reconocidas internacionalmente, considerando publicaciones disponibles hasta 2024. Los resultados muestran que la protección de las aplicaciones móviles depende de la integración de una arquitectura de software segura, criptografía, gestión de identidades, gobernanza de dispositivos y monitorización continua de los entornos tecnológicos. Se puede concluir que la seguridad de las aplicaciones móviles debe tratarse como un elemento integral del proceso de desarrollo de software, incorporando principios de seguridad desde las fases iniciales de diseño y monitorizando continuamente la evolución de las amenazas digitales.

Palabras clave: Ciberseguridad; Aplicaciones móviles; Desarrollo seguro; Protección de datos; Movilidad corporativa.

ABSTRACTO

La creciente adopción de aplicaciones móviles en entornos corporativos ha transformado significativamente la forma en que las organizaciones ejecutan procesos de negocio, intercambian información y facilitan la toma de decisiones. Si bien la movilidad empresarial ha mejorado la eficiencia operativa, también ha incrementado la exposición a las ciberamenazas, convirtiendo la seguridad de la información en un requisito estratégico para el desarrollo de software móvil. Este artículo analiza la relación entre el desarrollo de aplicaciones móviles y la ciberseguridad en los ecosistemas empresariales, abordando los principales riesgos de seguridad asociados a los dispositivos móviles y las mejores prácticas para la protección de datos, la autenticación de usuarios, la comunicación segura y la monitorización continua de los entornos corporativos. El estudio se realizó mediante una revisión sistemática de la literatura, basada en libros, publicaciones científicas revisadas por pares, normas técnicas e informes de instituciones reconocidas internacionalmente, considerando publicaciones disponibles hasta 2024. Los resultados indican que la seguridad de las aplicaciones móviles requiere la integración de una arquitectura de software segura, criptografía, gestión de identidades, gobernanza de dispositivos y monitorización continua de la seguridad. Se concluye que la seguridad de las aplicaciones móviles debe incorporarse a lo largo de todo el ciclo de vida del desarrollo de software, adoptando principios de seguridad desde el diseño que permitan reducir la exposición de las organizaciones a las ciberamenazas emergentes.

Palabras clave: Ciberseguridad; Aplicaciones móviles; Desarrollo de software seguro; Protección de datos;

Este artículo se publica en acceso abierto bajo la licencia Creative Commons Attribution, que permite el uso, la distribución y la reproducción sin restricciones en cualquier medio, siempre que se cite correctamente la obra original.

Machine Translated by Google
IRCMOS – Revista Científica Multidisciplinaria El Conocimiento.
ISSN: 2675-9128. São Paulo-SP.

Año VII, vol. 2, 2026 | Envío: 04/05/2026 | Aceptado: 07/05/2026 | Publicación: 10/05/2026

Movilidad empresarial.

1. INTRODUCCIÓN

La transformación digital ha alterado profundamente la forma en que las organizaciones desarrollan sus
Actividades, comparten información y gestionan procesos de negocio. La expansión de
computación en la nube, conectividad móvil y disponibilidad de dispositivos inteligentes
Esto permitió que las aplicaciones corporativas ya no estuvieran restringidas a entornos internos.
empresas, haciéndose accesibles en cualquier lugar con conexión a Internet. Esta evolución
Mayor flexibilidad operativa, favoreciendo los modelos de trabajo remoto,
Asistencia in situ, logística integrada y toma de decisiones en tiempo real.

El crecimiento de la movilidad corporativa representa uno de los cambios más relevantes en este ámbito.
proceso. Las aplicaciones desarrolladas para teléfonos inteligentes y tabletas se han integrado en las rutinas.
Relacionado con la gestión comercial, el control logístico, el control de inventarios y el servicio al cliente.
cliente, operaciones financieras y monitoreo de procesos industriales. Como consecuencia,
Los dispositivos móviles han dejado de funcionar únicamente como herramientas de comunicación y han asumido el papel de...
rol estratégico dentro de los ecosistemas empresariales.

Sin embargo, la expansión de la movilidad también ha cambiado el panorama de la seguridad de la información.
A diferencia de las estaciones de trabajo tradicionales, que normalmente están protegidas por políticas.
Si bien la infraestructura centralizada y corporativa permite que los dispositivos móviles operen en entornos heterogéneos,
Conectarse frecuentemente a redes públicas, dispositivos personales y diversos servicios en
nube. Esta función amplía la superficie de ataque disponible para los actores maliciosos y requiere
Enfoques de seguridad compatibles con la naturaleza distribuida de estos entornos.

Schneier (2015) observa que la evolución tecnológica amplía simultáneamente las oportunidades de innovación y los desafíos
relacionados con la protección de la información. A medida que surgen nuevos puntos de
A medida que se incorporan los puntos de acceso a la infraestructura organizativa, también aumenta el número de vectores.
susceptibles de ser explotados mediante ciberataques. En las aplicaciones móviles, este escenario se vuelve aún más crítico.
más complejo debido a la diversidad de sistemas operativos, fabricantes, configuraciones de
Políticas de hardware y actualización existentes en el mercado.

Entre las amenazas más frecuentes se encuentran los ataques de interceptación de tráfico y la explotación de...
vulnerabilidades en las API, credenciales comprometidas, instalación de aplicaciones maliciosas,
Ingeniería social, filtración de información almacenada localmente y explotación de bibliotecas.
Terceros vulnerables. El uso cada vez mayor de dispositivos personales en las actividades empresariales.
Esto agrava aún más la situación, dificultando que las empresas controlen directamente la infraestructura tecnológica.

Este artículo se publica en acceso abierto bajo la licencia Creative Commons Attribution, que permite el uso, la distribución y la reproducción sin restricciones en cualquier medio, siempre que se cite correctamente la obra original.

Machine Translated by Google

Año VII, vol. 2, 2026 | Envío: 04/05/2026 | Aceptado: 07/05/2026 | Publicación: 10/05/2026

organizaciones.

En este contexto, se puede observar un cambio importante en la forma en que se gestiona la seguridad de las aplicaciones.
móvil está diseñado. En lugar de centrar los esfuerzos exclusivamente en proteger la infraestructura de
Como parte de una red, las organizaciones han comenzado a incorporar mecanismos de seguridad en todas las etapas del proceso.
desarrollo de software. Este enfoque, conocido como Seguro por Diseño, considera que
requisitos relacionados con la autenticación, criptografía, gestión de sesiones, validación de entrada,
La protección de la API y la monitorización continua deben formar parte de la arquitectura de la aplicación desde su concepción.
diseño, reduciendo las vulnerabilidades estructurales y los consiguientes costes de corrección.

Otro aspecto que merece ser destacado se refiere al fortalecimiento de los modelos de identidad digital.
Uso de autenticación multifactor, protocolos de autorización modernos, gestión
Un conjunto centralizado de identidades y políticas basado en el principio del mínimo privilegio contribuye a
para reducir los riesgos asociados con las credenciales comprometidas. Paralelamente, la adopción del modelo
Zero Trust modifica la lógica tradicional de la seguridad corporativa al asumir que nadie...
El dispositivo, el usuario o la conexión deben considerarse fiables sin necesidad de validación continua.
independientemente de su ubicación en la red.

Además de las medidas preventivas, la importancia del monitoreo ambiental continuo es cada vez mayor.
Tecnológico. Herramientas y plataformas de gestión de dispositivos móviles.
eventos de seguridad, soluciones basadas en IA y mecanismos automatizados de
La respuesta ante incidentes ha llegado a desempeñar un papel esencial en la identificación de comportamientos.
anómalo, lo que permite respuestas más rápidas ante intentos de intrusión o vulneración de la seguridad.
de los dispositivos.

Dado este escenario, es necesario comprender la integración entre el desarrollo de aplicaciones móviles y
La ciberseguridad se ha convertido en una necesidad tanto para investigadores como para profesionales.
Responsables del desarrollo y la gestión de soluciones corporativas. Protección de la información.
Ha dejado de ser una actividad aislada dentro del campo de la tecnología y se ha convertido en un requisito estratégico.
relacionado con la continuidad operativa, el cumplimiento normativo y la preservación de la confianza en
clientes, socios y demás partes interesadas.

Por lo tanto, este artículo tiene como objetivo analizar la convergencia entre la ciberseguridad y el desarrollo.
de aplicaciones móviles en ecosistemas empresariales, analizando los principales riesgos asociados con
Movilidad corporativa, prácticas y mecanismos de desarrollo seguro contemporáneos
herramientas tecnológicas utilizadas para proteger datos, usuarios y sistemas en entornos caracterizados por
Alta conectividad y la constante evolución de las amenazas digitales.

Este artículo se publica en acceso abierto bajo la licencia Creative Commons Attribution, que permite el uso, la distribución y la reproducción sin restricciones en cualquier medio, siempre que se cite correctamente la obra original.

Machine Translated by Google
RCMOS – Revista Científica Multidisciplinaria El Conocimiento.
ISSN: 2675-9128. São Paulo-SP.

Año VII, vol. 2, 2026 | Envío: 04/05/2026 | Aceptación: 07/05/2026 | Publicación: 10/05/2026

2. METODOLOGÍA

Esta investigación se caracteriza por ser un estudio cualitativo, de carácter exploratorio y descriptivo. desarrollado a través de una revisión sistemática de la literatura. Se eligió esta estrategia metodológica. porque permite el análisis crítico del conocimiento científico relacionado con la seguridad de las aplicaciones. muebles, reuniendo contribuciones de las áreas de Ingeniería de Software, Seguridad y Información, arquitectura de sistemas, redes informáticas y gobernanza tecnológica Información.

Según Gil (2019), la investigación exploratoria es apropiada cuando el objetivo es ampliar Comprender un fenómeno en particular y organizar el conocimiento disponible en torno a un tema común. tema específico. En el contexto de la ciberseguridad, marcada por la constante evolución tecnológica, la Una revisión sistemática de la literatura permite identificar tendencias, mejores prácticas y desafíos. Tendencias emergentes y convergencias entre diferentes enfoques propuestos por investigadores y organizaciones. internacional.

La revisión bibliográfica incluyó libros, artículos científicos revisados por pares y normas. Se priorizaron los documentos técnicos e institucionales publicados hasta 2024. Se dio prioridad a las publicaciones indexadas. en bases de datos reconocidas internacionalmente, como IEEE Xplore, ACM Digital Library, SpringerLink, ScienceDirect, Scopus y Google Scholar, así como documentos técnicos producidos por organizaciones. como OWASP, NIST y la Alianza FIDO.

Los criterios de selección priorizaron los estudios relacionados con la seguridad de las aplicaciones móviles, Secure Ciclo de vida del desarrollo de software, autenticación multifactor, gestión de identidades, criptografía Aplicación, protección de API, gestión de dispositivos móviles, confianza cero, DevSecOps y monitorización Análisis continuo de entornos corporativos. Se excluyeron las publicaciones que carecían de base científica. materiales y estudios exclusivamente comerciales que no se adhirieron a los objetivos de buscar.

Tras seleccionar las referencias, se realizó una lectura analítica y comparativa de las obras, organizándolas. El contenido se divide en cinco áreas temáticas: superficie de ataque en entornos móviles, desarrollo Seguridad del software, mecanismos criptográficos, gestión de identidades y monitoreo continuo de aplicaciones. Esta organización hizo posible establecer relaciones entre diferentes enfoques presentes en literatura que promueve un análisis crítico de los factores que influyen en la seguridad de las aplicaciones. Mobiliario utilizado en entornos corporativos.

Aunque la revisión de la literatura no incluye investigación empírica en organizaciones específicas, Se considera que la metodología adoptada proporciona una base consistente para comprender el estado actual de conocimiento científico sobre el tema, identificando buenas prácticas ampliamente reconocidas y discutiendo

Este artículo se publica en acceso abierto bajo la licencia Creative Commons Attribution, que permite el uso, la distribución y la reproducción sin restricciones en cualquier medio, siempre que se cite correctamente la obra original.

Machine Translated by Google
RCMOS – Revista Científica Multidisciplinaria El Conocimiento.
ISSN: 2675-9128. São Paulo-SP.

Año VII, vol. 2, 2026 | Envío: 04/05/2026 | Aceptación: 07/05/2026 | Publicación: 10/05/2026

Los principales retos a los que se enfrentan las organizaciones para proteger sus ecosistemas móviles.

3. La superficie de ataque en entornos móviles corporativos

La consolidación de la movilidad corporativa ha modificado profundamente la arquitectura de los sistemas.
Información utilizada por las organizaciones. La capacidad de acceder a las aplicaciones empresariales a través de
El uso de teléfonos inteligentes y tabletas ha aumentado la productividad de los equipos y reducido las barreras geográficas.
Ha hecho que los procesos administrativos sean más ágiles. Sin embargo, esta misma flexibilidad se ha expandido.
amplía significativamente la superficie de ataque de las organizaciones, creando vectores de explotación para
agentes maliciosos.

A diferencia de las estaciones de trabajo tradicionales, los dispositivos móviles funcionan en entornos
Altamente dinámico. En el transcurso de un solo día, el mismo dispositivo puede conectarse a la red.
corporativo, usar conexiones móviles 4G o 5G, acceder a redes Wi-Fi públicas y establecer
comunicación con varios servicios en la nube. Cada cambio de contexto altera el entorno de
La seguridad aumenta el número de elementos que necesitan ser protegidos.

Según Stallings (2018), la seguridad de la información no solo debe considerar los mecanismos.
factores tecnológicos empleados para proteger los sistemas, pero también el entorno en el que operan estos sistemas.
Funcionan. En las aplicaciones móviles, esta premisa se vuelve particularmente relevante debido a la alta
heterogeneidad de dispositivos, sistemas operativos, fabricantes y versiones de software presentes
en el entorno corporativo.

Entre los factores que contribuyen a este aumento de la superficie de ataque, destaca la adopción de...
El modelo Bring Your Own Device (BYOD), en el que los empleados utilizan dispositivos personales para
acceder a los recursos institucionales. Aunque esta práctica reduce las inversiones en infraestructura y aumenta
La flexibilidad operativa también dificulta la aplicación uniforme de las políticas corporativas.
Seguridad. Los equipos privados suelen tener diferentes configuraciones y aplicaciones.
instalados sin control organizativo y con diferentes niveles de actualizaciones del sistema operativo,
mayor exposición a las vulnerabilidades.

Otro aspecto relevante se refiere a las redes utilizadas para acceder a las aplicaciones corporativas.
Los usuarios que se desplazan suelen conectarse a través de redes públicas.
Disponible en aeropuertos, hoteles, restaurantes, centros comerciales y otros lugares importantes.
circulación. Cuando estas redes tienen mecanismos de protección insuficientes, se convierten en
entornos propicios para ataques de interceptación de tráfico, suplantación de puntos de acceso y
captura de credenciales.

Como describen Tanenbaum y Wetherall (2011), los ataques de tipo "hombre en el medio" permiten

Este artículo se publica en acceso abierto bajo la licencia Creative Commons Attribution, que permite el uso, la distribución y la reproducción sin restricciones en cualquier medio, siempre que se cite correctamente la obra original.

Machine Translated by Google
RCMOS – Revista Científica Multidisciplinaria El Conocimiento.
ISSN: 2675-9128. São Paulo-SP.

Año VII, vol. 2, 2026 | Envío: 04/05/2026 | Aceptado: 07/05/2026 | Publicación: 10/05/2026

que un intruso intercepte la comunicación entre dos sistemas sin que los usuarios se den cuenta.
La existencia de esta intermediación. Si los mecanismos criptográficos empleados son inadecuados.
Independientemente de su existencia, la información confidencial puede ser interceptada durante la transmisión.
comprometer datos financieros, credenciales de autenticación e información estratégica de
organización.

El almacenamiento local de información también representa un factor de riesgo significativo. Varios
Las aplicaciones móviles conservan datos temporales para permitir el funcionamiento sin conexión y reducir el consumo de datos.
ancho de banda o mejorar la experiencia del usuario. Cuando estos registros permanecen almacenados
Sin mecanismos de cifrado adecuados, los dispositivos pueden perderse, ser robados o verse comprometidos.
Podrían revelar información sensible relacionada con las actividades de la organización.

Además de las amenazas relacionadas con el entorno de comunicación, la fragmentación de los ecosistemas
Los dispositivos móviles plantean desafíos adicionales para el desarrollo seguro. En el sistema Android, por ejemplo,
Diferentes fabricantes ofrecen versiones personalizadas del sistema operativo, con ciclos
distinto de las actualizaciones de seguridad. Como resultado, muchos dispositivos siguen siendo
largos períodos sin recibir correcciones para vulnerabilidades conocidas, ampliando la ventana de
exposición a ataques.

Otro factor frecuentemente explotado por actores maliciosos tiene que ver con la obtención de privilegios.
niveles elevados a través de procedimientos como rootear o jailbreaking. Estas modificaciones eliminan
Las restricciones impuestas por los fabricantes comprometen los mecanismos de aislamiento fundamentales entre
aplicaciones. Como consecuencia, las aplicaciones maliciosas pueden obtener un mayor acceso a los recursos.
desde el dispositivo, comprometiendo la información almacenada por las aplicaciones corporativas y reduciendo
Redujo significativamente la eficacia de las medidas de protección implementadas originalmente.

También merece atención el aumento de los ataques dirigidos a las interfaces de programación de
Aplicaciones (API). En las arquitecturas modernas, las aplicaciones móviles concentran una gran parte de su...
Lógica empresarial en servidores que se comunican continuamente a través de API REST o
GraphQL. Fallos relacionados con la autenticación, autorización, validación de parámetros o limitación de
Las solicitudes pueden permitir el acceso no autorizado a información corporativa, comprometiendo la
integridad y confidencialidad de los datos procesados.

La expansión de la cadena de suministro de software representa otro factor de riesgo significativo.
El desarrollo contemporáneo utiliza un gran número de bibliotecas de código abierto.
Componentes reutilizables y servicios de terceros. Estas características aceleran el desarrollo.
Las aplicaciones también aumentan la posibilidad de introducir vulnerabilidades derivadas de
Dependencias comprometidas o componentes obsoletos. Los ataques recientes demuestran que...
La explotación de la cadena de suministro se ha convertido en una de las estrategias más utilizadas por los grupos.

Este artículo se publica en acceso abierto bajo la licencia Creative Commons Attribution, que permite el uso, la distribución y la reproducción sin restricciones en cualquier medio, siempre que se cite correctamente la obra original.

Machine Translated by Google

Año VII, vol. 2, 2026 | Envío: 04/05/2026 | Aceptación: 07/05/2026 | Publicación: 10/05/2026

Especializado en ciberdelincuencia.

Dado este escenario, está claro que la seguridad de las aplicaciones móviles no puede limitarse a Protección del dispositivo o de la infraestructura de red. La literatura reciente recomienda la adopción de modelos basados en el principio de Confianza Cero, según el cual ningún usuario, equipo o La conexión debe considerarse de confianza automáticamente. Todas las solicitudes de acceso deben ser Verificado, autenticado y autorizado continuamente según el contexto operativo. reduciendo la probabilidad de movimientos laterales y de que se vean comprometidos los entornos corporativos. Por lo tanto, la creciente movilidad empresarial exige que la seguridad se diseñe de manera que... Integrado, considerando simultáneamente los dispositivos, los usuarios, las aplicaciones y la infraestructura. Comunicación, identidad digital y gobernanza de la tecnología. Solo este enfoque sistémico es capaz de responder a la complejidad de los ecosistemas móviles contemporáneos y reducir los riesgos. asociado con la transformación digital.

4. INGENIERÍA DE SOFTWARE ORIENTADA A LA SEGURIDAD (SEGURIDAD DESDE EL DISEÑO)

La creciente sofisticación de las ciberamenazas ha cambiado significativamente la forma en que... Se desarrollan aplicaciones empresariales. Modelos tradicionales, en los que se requieren requisitos de seguridad. Se incorporaron únicamente en las etapas finales del desarrollo y resultaron insuficientes frente a... Debido a la creciente complejidad de la arquitectura moderna. En respuesta a este escenario, el... El concepto de "Seguridad desde el Diseño" propone incorporar principios de seguridad desde el principio. etapas iniciales del ciclo de vida del software.

Según Pressman y Maxim (2020), los defectos identificados durante las etapas de especificación inicial y la arquitectura presentan un costo significativamente menor que las vulnerabilidades descubiertas después de la Implementación del sistema en un entorno de producción. Además del impacto financiero, las vulnerabilidades explotadas en Las aplicaciones corporativas pueden comprometer la continuidad operativa y provocar fugas de datos. información estratégica y generar pérdidas relacionadas con la reputación institucional.

En este contexto, el ciclo de desarrollo seguro, conocido como Desarrollo de Software Seguro. La gestión del ciclo de vida del software (SSDLC) amplía las actividades tradicionales de ingeniería de software al incorporar... prácticas específicas destinadas a identificar, prevenir y mitigar vulnerabilidades en todo el país el proceso de desarrollo.

Uno de los primeros pasos consiste en la elaboración de modelos de amenazas . Antes de eso... Durante la implementación de las funcionalidades, los equipos de desarrollo analizan los activos más relevantes. A partir de la aplicación, identifican posibles actores de amenazas, evalúan las vulnerabilidades existentes y Establecen controles capaces de reducir los riesgos identificados. Este enfoque permite anticiparse a ellos.

Este artículo se publica en acceso abierto bajo la licencia Creative Commons Attribution, que permite el uso, la distribución y la reproducción sin restricciones en cualquier medio, siempre que se cite correctamente la obra original.

Machine Translated by Google
RCMOS – Revista Científica Multidisciplinaria El Conocimiento.
ISSN: 2675-9128. São Paulo-SP.

Año VII, vol. 2, 2026 | Envío: 04/05/2026 | Aceptado: 07/05/2026 | Publicación: 10/05/2026

cuestiones de seguridad antes de que se incorporen al producto final.

Otro principio ampliamente adoptado se refiere al desarrollo basado en el concepto de privilegio.
mínimo. Las aplicaciones móviles solo deben solicitar los permisos estrictamente necesarios para
Cómo funcionan sus funciones. Acceso sin restricciones a la cámara, ubicación, almacenamiento,
Los contactos o micrófonos aumentan innecesariamente la superficie de ataque y amplifican los impactos.
como resultado de cualquier posible vulneración de la aplicación.

La protección del código fuente también es un componente importante de las estrategias de
Desarrollo seguro. Las técnicas de ofuscación dificultan la ingeniería inversa de las aplicaciones.
distribuidos a los usuarios, reduciendo la posibilidad de extraer reglas y algoritmos de negocio.
propietarios, credenciales incrustadas incorrectamente en el código y mecanismos internos de
autenticación. Si bien no impiden por completo el análisis de aplicaciones, estas técnicas aumentan
significativamente el esfuerzo requerido para su exploración.

Las interfaces de programación utilizadas por las aplicaciones móviles merecen especial atención durante
desarrollo. Las API expuestas a Internet a menudo constituyen el punto principal de
comunicación entre dispositivos móviles y sistemas corporativos. Debido a esto, los mecanismos
Autenticación, autorización, validación de entrada y limitación de la tasa de solicitudes robustas.
El registro y la grabación de eventos deben integrarse en la arquitectura de estas interfaces, reduciendo así los riesgos asociados.
Ataques de inyección, escalada de privilegios y acceso no autorizado.

El uso cada vez mayor de bibliotecas externas también exige políticas rigurosas de gestión bibliotecaria.
dependencias. Gran parte de las aplicaciones modernas incorporan componentes de código abierto.
Responsable de la autenticación, la comunicación de red, el cifrado, la persistencia de datos y la interfaz.
Gráficos. Si bien estos recursos aceleran el desarrollo, se han descubierto vulnerabilidades en ellos...
Las bibliotecas pueden contener miles de aplicaciones simultáneamente. Por lo tanto, se vuelve...
Es fundamental mantener inventarios actualizados de las dependencias utilizadas y supervisar las vulnerabilidades.
Conocer y realizar actualizaciones continuas de los componentes utilizados.

En los últimos años, el concepto de DevSecOps ha fortalecido aún más esta integración entre
desarrollo y seguridad. En lugar de tratar la seguridad como la única responsabilidad de
equipos especializados, el modelo distribuye esta responsabilidad a lo largo de todo el ciclo de
desarrollo, incorporando comprobaciones automatizadas directamente en las canalizaciones de integración y
entregas continuas.

Las herramientas de análisis estático (Pruebas de seguridad de aplicaciones estáticas – SAST) le permiten identificar
Las vulnerabilidades se detectan directamente en el código fuente antes de que se compile la aplicación.
Además, mecanismos de análisis dinámico (Pruebas de seguridad de aplicaciones dinámicas –
Las pruebas DAST evalúan el comportamiento del software en ejecución, identificando fallos que solo pueden detectarse si...

Este artículo se publica en acceso abierto bajo la licencia Creative Commons Attribution, que permite el uso, la distribución y la reproducción sin restricciones en cualquier medio, siempre que se cite correctamente la obra original.

Machine Translated by Google

Año VII, vol. 2, 2026 | Envío: 04/05/2026 | Aceptación: 07/05/2026 | Publicación: 10/05/2026

Se manifiestan durante su funcionamiento. El uso combinado de estos enfoques amplía
Mejora significativamente la capacidad de identificar vulnerabilidades de forma temprana.
Otra práctica que ha cobrado relevancia recientemente es el uso de una lista de materiales de software.
(SBOM), un documento que enumera todos los componentes utilizados durante la construcción de
aplicación. Este enfoque facilita la gestión de la cadena de suministro de software, permitiendo
Identificar rápidamente qué aplicaciones utilizan componentes afectados por vulnerabilidades recién descubiertas.
descubrimientos y aceleración de los procesos de respuesta ante incidentes.
También cabe destacar la realización periódica de pruebas de penetración y ejercicios de validación.
seguridad. A diferencia de los análisis automatizados, estas actividades simulan el comportamiento.
de agentes maliciosos, lo que permite la identificación de vulnerabilidades derivadas de la interacción entre
diferentes componentes arquitectónicos, errores de configuración o fallos relacionados con el entorno.
operacional.
Por lo tanto, se puede observar que el desarrollo seguro ha dejado de representar un paso complementario.
desde la ingeniería de software hasta convertirse en un elemento estructurador de las aplicaciones empresariales
Contemporáneo. Incorporar los requisitos de seguridad desde la etapa de diseño del sistema reduce
reduce costos, aumenta la confiabilidad de las aplicaciones y fortalece la capacidad de las organizaciones para...
Para responder a las amenazas presentes en los ecosistemas digitales actuales.

5 protocolos criptográficos para la protección de datos en aplicaciones
MUEBLES

La criptografía es uno de los pilares fundamentales de la seguridad de la información y desempeña un papel indispensable en
la protección de las aplicaciones móviles utilizadas en entornos corporativos.
Los dispositivos móviles han comenzado a procesar información estratégica relacionada con las operaciones.
En los ámbitos de las finanzas, la logística, la sanidad, el comercio electrónico y la gestión empresarial, se ha vuelto necesario adoptar
mecanismos capaces de garantizar la confidencialidad, la integridad, la autenticidad y el no repudio durante
Todo el ciclo de vida de los datos.

Según Katz y Lindell (2020), la seguridad criptográfica contemporánea no depende
No se trata solo de la robustez de los algoritmos utilizados, sino de la correcta implementación de los protocolos.
gestión adecuada de las claves criptográficas y la integración de estos mecanismos con la arquitectura
de la aplicación. Vulnerabilidades relacionadas con la gestión y el almacenamiento de certificados.
El uso inadecuado de claves o el uso incorrecto de bibliotecas criptográficas pueden comprometer la seguridad.
Sistemas que emplean algoritmos matemáticamente sólidos.
En el contexto de las aplicaciones móviles, la protección de los datos en tránsito es una de las principales preocupaciones.

Este artículo se publica en acceso abierto bajo la licencia Creative Commons Attribution, que permite el uso, la distribución y la reproducción sin restricciones en cualquier medio, siempre que se cite correctamente la obra original.

Machine Translated by Google

Año VII, vol. 2, 2026 | Envío: 04/05/2026 | Aceptado: 07/05/2026 | Publicación: 10/05/2026

Capas de defensa. La información intercambiada entre dispositivos y servidores corporativos viaja...
de forma continua a través de diferentes infraestructuras de comunicación, incluidas las redes móviles y las conexiones Wi-Fi.
Redes públicas y proveedores de servicios en la nube. Esta diversidad de entornos aumenta la
Posibilidad de interceptación del tráfico por parte de agentes maliciosos si no se implementan los mecanismos adecuados.
No se debe emplear ningún tipo de protección.

En este escenario, el uso del protocolo Transport Layer Security (TLS) se ha consolidado como
Un requisito básico para las aplicaciones empresariales modernas. La versión 1.3 de TLS redujo las vulnerabilidades.
presente en implementaciones anteriores, simplificó el proceso de comercio criptográfico y
Proporcionó mejoras tanto en el rendimiento como en la seguridad. Además de la confidencialidad de
En la comunicación, el protocolo garantiza la autenticación entre cliente y servidor y mecanismos que preservan
la integridad de los mensajes transmitidos.

Sin embargo, el uso aislado de TLS no elimina por completo los riesgos asociados a la comunicación.
entre aplicaciones móviles y servicios corporativos. Varios ataques explotan los certificados digitales.
Mecanismos de validación fraudulentos o inadecuados implementados por las propias aplicaciones.
Para reducir esta posibilidad, muchas organizaciones adoptan una técnica conocida como Certificado.
El anclaje consiste en la validación explícita de la identidad criptográfica del servidor durante el proceso.
Estableciendo la conexión.

Este enfoque impide que los certificados emitidos por autoridades de certificación comprometidas o
Los certificados insertados localmente por aplicaciones maliciosas son aceptados por la aplicación. Aunque la
El anclaje de certificados requiere un mayor control durante los procesos de renovación de certificados digitales, su
Su uso reduce significativamente la posibilidad de ataques basados en la interceptación de
comunicación.

Otro aspecto relevante se refiere a la protección de la información almacenada localmente en
dispositivos móviles. En muchas situaciones, las aplicaciones corporativas necesitan mantener datos.
Medidas temporales para garantizar la funcionalidad sin conexión, la sincronización posterior o una mejor experiencia de usuario.
del usuario. Cuando este almacenamiento es inevitable, se vuelve esencial emplear mecanismos.
Un cifrado robusto capaz de proteger esta información incluso en casos de pérdida o robo.
o deterioro del dispositivo.

El algoritmo Estándar de Cifrado Avanzado (AES), especialmente en implementaciones basadas en claves.
La arquitectura de 256 bits sigue siendo una de las principales recomendaciones para proteger los datos en reposo.
Sin embargo, la literatura destaca que la efectividad de este mecanismo depende directamente de cómo...
Las claves criptográficas se almacenan y gestionan. Almacenamiento de claves directamente
Incluir código en el código de la aplicación o en los archivos de configuración representa una práctica inapropiada, ya que facilita...
Su extracción mediante ingeniería inversa.

Este artículo se publica en acceso abierto bajo la licencia Creative Commons Attribution, que permite el uso, la distribución y la reproducción sin restricciones en cualquier medio, siempre que se cite correctamente la obra original.

Machine Translated by Google
RCMOS - Revista Científica Multidisciplinaria El Conocimiento.
ISSN: 2675-9128. São Paulo-SP.

Año VII, vol. 2, 2026 | Envío: 04/05/2026 | Aceptado: 07/05/2026 | Publicación: 10/05/2026

Para reducir este riesgo, los sistemas operativos móviles proporcionan entornos protegidos diseñados para específicamente para el almacenamiento seguro de credenciales criptográficas. En Android, esta función es Esta función la realiza el Almacén de claves de Android, mientras que los dispositivos iOS utilizan los Servicios de llavero. Asociados al Enclave Seguro. Estos componentes mantienen las claves aisladas del resto del sistema. operativo, reduciendo significativamente la probabilidad de compromiso incluso frente a aplicaciones maliciosas que se ejecutan en el dispositivo.

Además de la confidencialidad, también debe garantizarse la integridad de la información. Algoritmos Las herramientas criptográficas diseñadas para generar funciones hash le permiten verificar si Un archivo o mensaje en particular sufrió cambios durante su almacenamiento o transmisión. Sin embargo, los algoritmos utilizados históricamente, como MD5 y SHA-1, presentan vulnerabilidades. conocidos y ya no se recomiendan para aplicaciones que requieren altos niveles de seguridad. Actualmente, se recomienda el uso de algoritmos pertenecientes a SHA-2 o familias similares. SHA-3, según las necesidades específicas de la aplicación.

Otro tema que ha cobrado importancia en los últimos años se refiere a la elaboración de diseños arquitectónicos. Herramientas criptográficas para el avance de la computación cuántica. Aunque los ataques prácticos contra los algoritmos Si bien los métodos utilizados actualmente aún no representan un riesgo inmediato para la mayoría de las organizaciones, Las instituciones responsables de la normalización internacional ya han comenzado el proceso de desarrollo. y la adopción de algoritmos resistentes a la computación cuántica. Esta perspectiva refuerza la necesidad de Arquitecturas criptográficas flexibles, capaces de incorporar nuevos estándares a medida que se vayan desarrollando. establecida oficialmente.

Por lo tanto, se puede observar que la protección criptográfica de las aplicaciones móviles depende de la combinación de algoritmos robustos, implementación correcta de protocolos, gestión segura de claves y Actualización continua de las bibliotecas utilizadas. La criptografía debe entenderse como una parte integral de la arquitectura de la aplicación y no una función adicional integrada. únicamente en las etapas finales de desarrollo.

6. Gestión de identidades y control de acceso en aplicaciones móviles

A medida que las aplicaciones móviles han comenzado a ofrecer funcionalidades críticas para las organizaciones Tanto en el sector público como en el privado, la gestión de la identidad se ha convertido en un elemento central de las estrategias. Seguridad de la información. El uso sencillo de credenciales que consisten en un nombre de usuario y una contraseña. demostró ser insuficiente para responder al crecimiento de las amenazas relacionadas con compromiso de cuentas, reutilización de contraseñas y ataques automatizados dirigidos a sistemas corporativos.

Este artículo se publica en acceso abierto bajo la licencia Creative Commons Attribution, que permite el uso, la distribución y la reproducción sin restricciones en cualquier medio, siempre que se cite correctamente la obra original.

Machine Translated by Google
RCMOS – Revista Científica Multidisciplinaria El Conocimiento.
ISSN: 2675-9128. São Paulo-SP.

Año VII, vol. 2, 2026 | Envío: 04/05/2026 | Aceptado: 07/05/2026 | Publicación: 10/05/2026

Diversos estudios demuestran que las credenciales comprometidas siguen estando entre los principales riesgos.
Vectores utilizados para intrusiones en entornos corporativos. Ataques de fuerza bruta,
El robo de credenciales, la ingeniería social y las campañas de phishing explotan comportamientos recurrentes.
de los usuarios, como la reutilización de contraseñas y la adopción de combinaciones predecibles. Debido a esto
En este escenario, las organizaciones han comenzado a incorporar mecanismos de autenticación adicionales capaces de...
reducir significativamente la probabilidad de acceso no autorizado.

La autenticación multifactor (MFA) se ha consolidado como una de las medidas más eficaces en este contexto.
El principio consiste en el uso simultáneo de dos o más factores independientes para la validación.
de la identidad del usuario, combinando la información que conoce, posee o representa.
Desde el punto de vista biológico, incluso si una contraseña se ve comprometida, la ausencia de otros factores dificulta aún más el acceso.
esencialmente, se trata de la explotación de las credenciales obtenidas por el atacante.

En las aplicaciones móviles, la integración entre la autenticación multifactor y las funciones biométricas se ha convertido en...
particularmente eficiente debido a la presencia de sensores nativos incorporados en los dispositivos
Se pueden utilizar tecnologías modernas como huellas dactilares, reconocimiento facial y otros mecanismos biométricos.
Se utiliza para validar la identidad del usuario sin necesidad de datos biométricos.
Transmitido a servidores corporativos. En arquitecturas compatibles con los estándares FIDO.
Alliance, la verificación se realiza localmente en el dispositivo, preservando la privacidad del usuario y
reducir la exposición de información sensible.

Además de la autenticación, la gestión de las sesiones establecidas entre dispositivos móviles y
Los servidores corporativos requieren mecanismos de protección específicos. A diferencia de las aplicaciones
Las arquitecturas tradicionales se basan en sesiones persistentes, las arquitecturas modernas a menudo utilizan
protocolos de autorización basados en tokens, como OAuth 2.0 y OpenID Connect, asociados con
El uso de JSON Web Tokens (JWT) cuando sea apropiado. Estos mecanismos permiten controlar...
Periodo de validez de las credenciales, limitación de los privilegios otorgados y facilitación de los procesos de revocación.
acceso.

Sin embargo, la literatura también destaca que el uso de JWT requiere cuidados relacionados con...
Almacenamiento de tokens, control de caducidad y protección contra ataques de reutilización.
(ataques de repetición). La adopción de tokens con períodos de vencimiento cortos, asociados a una renovación controlada.
Y al almacenar las credenciales de forma segura, reduce significativamente estas vulnerabilidades.
Otro componente clave se relaciona con la gestión centralizada de identidades. Soluciones para
El inicio de sesión único (SSO) permite a los usuarios autenticarse solo una vez para acceder a diferentes
aplicaciones corporativas, simplificando la experiencia del usuario y reduciendo la proliferación de credenciales.
independiente. Desde una perspectiva administrativa, este enfoque facilita la gestión de
Permisos, auditoría de acceso y revocación inmediata de autorizaciones cuando sea necesario.

Este artículo se publica en acceso abierto bajo la licencia Creative Commons Attribution, que permite el uso, la distribución y la reproducción sin restricciones en cualquier medio, siempre que se cite correctamente la obra original.

Machine Translated by Google
RCMOS - Revista Científica Multidisciplinaria El Conocimiento.
ISSN: 2675-9128. São Paulo-SP.

Año VII, vol. 2, 2026 | Envío: 04/05/2026 | Aceptado: 07/05/2026 | Publicación: 10/05/2026

La gestión de privilegios también debe seguir el principio del mínimo privilegio .
según el cual cada usuario recibe únicamente los permisos estrictamente necesarios para el desempeño de
sus actividades. Esta estrategia reduce significativamente los impactos resultantes de
Protege las cuentas y limita el movimiento lateral de los atacantes dentro de la infraestructura.
corporativo.

En los últimos años, los modelos de autenticación tradicionales han comenzado a incorporar principios asociados.
autenticación adaptativa. En lugar de considerar solo el nombre de usuario y la contraseña, estos mecanismos analizan
Factores contextuales como la ubicación geográfica, la hora de acceso, el dispositivo utilizado, la dirección
Dirección IP, comportamiento histórico y características de conexión. Siempre que se observen patrones inusuales.
Una vez identificados, es posible que se requieran automáticamente mecanismos de autenticación adicionales antes de...
Conceder acceso.

Este enfoque está plenamente alineado con los principios del modelo de Confianza Cero, en el que...
La identidad ya no se valida solo en el momento inicial de la autenticación y se convierte en...
Se reevalúa continuamente a lo largo de la interacción entre el usuario y el sistema. Por lo tanto, los cambios
El comportamiento pertinente puede dar lugar a un bloqueo preventivo, a la renovación de credenciales o...
Solicitud de factores de autenticación adicionales.

Más allá de los aspectos tecnológicos, la gestión de identidades también implica componentes
Directrices organizativas relacionadas con la gobernanza del acceso. Políticas claras para la creación, revisión periódica y...
Revocar los permisos ayuda a reducir las cuentas huérfanas, el acceso no autorizado y las inconsistencias.
como resultado del movimiento de empleados entre diferentes roles dentro de la organización.

Por lo tanto, se puede observar que la gestión de identidades representa una capa estratégica de
Seguridad de las aplicaciones móviles. Su efectividad depende de la integración de una autenticación robusta,
Gestión centralizada de credenciales, monitorización continua del comportamiento del usuario.
y políticas de gobernanza capaces de seguir el ritmo de la dinámica operativa de las organizaciones.
contemporáneos. Estos mecanismos, cuando se implementan de manera integrada, fortalecen
protegen significativamente los activos digitales y reducen la exposición de las organizaciones a los principales [riesgos/críticas].
amenazas relacionadas con el compromiso de credenciales.

7. Monitoreo continuo, respuesta a incidentes y gobernanza de SEGURIDAD MÓVIL

La adopción de mecanismos preventivos representa solo una dimensión de la seguridad.
Información. En entornos corporativos caracterizados por una alta conectividad y constante
Dada la evolución de las amenazas digitales, se supone que los controles técnicos podrán prevenirlas todas.

Este artículo se publica en acceso abierto bajo la licencia Creative Commons Attribution, que permite el uso, la distribución y la reproducción sin restricciones en cualquier medio, siempre que se cite correctamente la obra original.

Machine Translated by Google

Año VII, vol. 2, 2026 | Envío: 04/05/2026 | Aceptado: 07/05/2026 | Publicación: 10/05/2026

Los intentos de compromiso se volvieron incompatibles con la realidad operativa de organizaciones. En este contexto, el monitoreo continuo de los activos tecnológicos juega un papel crucial. estratégico en la identificación temprana de incidentes y en la reducción de los impactos derivados de los ataques. cibernética.

El concepto contemporáneo de defensa en profundidad presupone el uso integrado de Mecanismos preventivos, de detección y correctivos. Además de implementar controles de acceso, El cifrado y la autenticación robustos hacen necesario supervisar continuamente el comportamiento. de aplicaciones, dispositivos y usuarios, lo que permite la identificación de cambios que pueden indicar Intentos de explotar vulnerabilidades o comprometer entornos corporativos.

Entre las tecnologías utilizadas para esta monitorización, destacan las plataformas móviles . Gestión de dispositivos (MDM) y gestión de movilidad empresarial (EMM). Estas soluciones permiten administrar de forma remota los dispositivos utilizados por la organización, establecer políticas de seguridad, Controlar la configuración, restringir las funciones que sean incompatibles con las directrices corporativas y Aplicar actualizaciones de forma centralizada. En entornos donde coexisten dispositivos. Equipos institucionales y personales utilizados en las políticas de "Traiga su propio dispositivo" (BYOD) . Estas herramientas desempeñan un papel fundamental en la estandarización de los requisitos mínimos para seguridad.

Además de la administración de dispositivos, la gestión remota permite realizar procedimientos. Fundamental en situaciones de compromiso, pérdida o robo de equipos. Recursos como Bloqueo remoto, revocación de certificados digitales, eliminación selectiva de información corporativa y Restablecer la configuración de seguridad reduce significativamente el riesgo de exposición. Datos confidenciales.

Otro componente esencial se refiere al seguimiento de los eventos producidos por las propias empresas. Aplicaciones móviles. Registros de autenticación, cambios de configuración, intentos de acceso fallidos. La autorización, los cambios de permisos y los fallos de comunicación constituyen fuentes importantes de... información para identificar actividades sospechosas. Cuando está debidamente estructurada, esta Los registros permiten reconstruir la secuencia de eventos asociados con un incidente y brindar apoyo... procesos de investigación forense.

En este contexto, las plataformas de gestión de información y eventos de seguridad (SIEM) consolidan información de diferentes fuentes dentro de la infraestructura tecnológica, lo que permite la correlación eventos aparentemente aislados e identificación de patrones consistentes con ataques en curso. La integración entre aplicaciones móviles, servidores, dispositivos de red y servicios en la nube se expande. Mejora significativamente la capacidad de los equipos de seguridad para detectar comportamientos anómalos. antes de que produzcan impactos significativos en las operaciones de la organización.

Este artículo se publica en acceso abierto bajo la licencia Creative Commons Attribution, que permite el uso, la distribución y la reproducción sin restricciones en cualquier medio, siempre que se cite correctamente la obra original.

Machine Translated by Google
RCMOS - Revista Científica Multidisciplinaria El Conocimiento.
ISSN: 2675-9128. São Paulo-SP.

Año VII, vol. 2, 2026 | Envío: 04/05/2026 | Aceptado: 07/05/2026 | Publicación: 10/05/2026

En los últimos años, las técnicas basadas en inteligencia artificial y aprendizaje automático han comenzado a...
Complementar estas plataformas mediante el análisis del comportamiento de los usuarios y los dispositivos.
Los modelos conocidos como Análisis del Comportamiento de Usuarios y Entidades (UEBA, por sus siglas en inglés) permiten establecer perfiles.
patrones de uso considerados normales para cada usuario o pieza de equipo, identificando automáticamente
desviaciones significativas relacionadas con el tiempo de acceso, la ubicación geográfica y el volumen de
transacciones o patrones de uso de los recursos corporativos.
Aunque estas tecnologías no reemplazan el análisis realizado por los equipos de seguridad, su
El uso de este método reduce el tiempo necesario para identificar comportamientos potencialmente maliciosos.
y contribuye a priorizar los eventos que requieren una investigación inmediata. De esta manera, la
La capacidad de las organizaciones para responder rápidamente a los incidentes y minimizar su impacto.
operacional.
Otro aspecto que se pasa por alto con frecuencia se refiere a la gestión de las actualizaciones de
software. Las vulnerabilidades descubiertas recientemente hacen que la distribución rápida de software sea indispensable.
Correcciones para aplicaciones móviles y sistemas operativos. Procesos de actualización automatizados.
La actualización inalámbrica (OTA) permite la entrega centralizada de nuevas versiones de las aplicaciones.
garantizar que los dispositivos permanezcan protegidos contra vulnerabilidades conocidas y reducir la
Persistencia de versiones vulnerables en funcionamiento.
Además de las actividades de seguimiento, las organizaciones deben establecer planes formales para
Los planes de respuesta a incidentes son compatibles con sus características operativas. Estos planes definen
Responsabilidades, procedimientos de comunicación, criterios de clasificación de incidentes,
mecanismos de contención, recuperación del servicio y análisis de las causas fundamentales de los incidentes.
identificado. La existencia de procesos estructurados reduce el tiempo de respuesta y minimiza las pérdidas.
Es operativo y promueve el aprendizaje institucional derivado de los incidentes ocurridos.
También cabe destacar la realización periódica de pruebas de penetración, ejercicios de simulación y
Evaluaciones de madurez en seguridad de la información. Estas iniciativas permiten validar la eficacia.
A partir de los controles implementados, identifique las vulnerabilidades que aún no han sido explotadas y mejórelas.
Mejorar continuamente los procesos organizativos relacionados con la protección de las aplicaciones móviles.
Desde una perspectiva de gobierno corporativo, se debe entender el monitoreo continuo.
como una actividad permanente integrada en las estrategias institucionales. La constante evolución de
Las amenazas digitales requieren actualizaciones frecuentes de las políticas de seguridad y una revisión de los mecanismos.
control, formación de profesionales y seguimiento sistemático de los indicadores relacionados
para la protección de los activos tecnológicos.
Por lo tanto, se puede observar que la seguridad de las aplicaciones móviles no depende exclusivamente de su adopción.
no solo las tecnologías avanzadas, sino también la capacidad de las organizaciones para establecer procesos continuos de

Este artículo se publica en acceso abierto bajo la licencia Creative Commons Attribution, que permite el uso, la distribución y la reproducción sin restricciones en cualquier medio, siempre que se cite correctamente la obra original.

Machine Translated by Google
RCMOS – Revista Científica Multidisciplinaria El Conocimiento.
ISSN: 2675-9128. São Paulo-SP.

Año VII, vol. 2, 2026 | Envío: 04/05/2026 | Aceptado: 07/05/2026 | Publicación: 10/05/2026

Monitorización, respuesta ante incidentes y mejora continua. Integración entre herramientas.

La tecnología, la gobernanza, los procesos y las personas son elementos clave para fortalecer [la empresa/organización].

de la ciberresiliencia en ecosistemas empresariales cada vez más distribuidos e interconectados.

CONCLUSIÓN

El uso cada vez mayor de aplicaciones móviles ha cambiado significativamente la dinámica operativa.

de organizaciones, ampliando la disponibilidad de sistemas corporativos y favoreciendo modelos de

El trabajo es cada vez más flexible. Al mismo tiempo, esta transformación ha aumentado su complejidad.

Los entornos tecnológicos han ampliado la superficie expuesta a las amenazas cibernéticas, lo que hace que

La seguridad de la información es un requisito estratégico para el desarrollo y la operación de estos sistemas.

aplicaciones.

La revisión bibliográfica demostró que la protección de los ecosistemas móviles requiere un enfoque...

multidimensional, que involucra arquitectura de software segura, criptografía, gestión de

identidad, protección de las interfaces de comunicación, monitoreo continuo y gobernanza de

Seguridad de la información. Estos elementos funcionan de forma complementaria y deben incorporarse.

desde las primeras etapas del desarrollo de la aplicación, reduciendo las vulnerabilidades estructurales y

aumentar la capacidad de respuesta ante incidentes de seguridad.

También se descubrió que los modelos de protección tradicionales basados exclusivamente en el perímetro de la

Las redes corporativas ya no satisfacen las necesidades impuestas por la movilidad empresarial.

El uso de dispositivos distribuidos, servicios en la nube y entornos híbridos requiere mecanismos.

autenticación continua, validación contextual de accesos y aplicación de los principios asociados con

Modelo de confianza cero, en el que los usuarios, los dispositivos y las conexiones se evalúan constantemente antes de su uso.

otorgar o mantener privilegios de acceso.

Otro aspecto relevante identificado durante el estudio se refiere a la creciente importancia de la integración.

entre el desarrollo de software y la seguridad de la información. Prácticas como Seguridad desde el diseño,

Ciclo de vida de desarrollo de software seguro, DevSecOps y gestión de la cadena de suministro de software.

Demuestran que la prevención de vulnerabilidades debe producirse a lo largo de todo el ciclo de vida.

desarrollo, reduciendo los costos de mantenimiento y aumentando la confiabilidad de las aplicaciones.

corporativo.

Los resultados también muestran que el monitoreo continuo juega un papel clave en

Protección de entornos móviles. Plataformas de gestión de dispositivos, sistemas de correlación.

de eventos, análisis de comportamiento basados en inteligencia artificial y procesos estructurados de

La respuesta a incidentes mejora significativamente la capacidad de las organizaciones para identificar

Este artículo se publica en acceso abierto bajo la licencia Creative Commons Attribution, que permite el uso, la distribución y la reproducción sin restricciones en cualquier medio, siempre que se cite correctamente la obra original.

Machine Translated by Google

Año VII, vol. 2, 2026 | Envío: 04/05/2026 | Aceptado: 07/05/2026 | Publicación: 10/05/2026

Detectar actividades sospechosas, contener los ataques en sus fases iniciales y reducir el impacto operativo.
derivados de incidentes de seguridad.

Sin embargo, la eficacia de estas estrategias también depende de factores organizativos.
definir políticas de gobernanza, la actualización continua de controles tecnológicos, la
La cualificación profesional y la concienciación del usuario siguen siendo componentes clave.
indispensable para fortalecer la seguridad corporativa. La tecnología, por sí sola, no elimina
Los riesgos surgen cuando no va acompañado de procesos consistentes y una cultura organizacional orientada hacia
protección de la información.

Con base en la evidencia presentada, se puede concluir que la convergencia entre el desarrollo de
Las aplicaciones móviles y la ciberseguridad son elementos esenciales para la sostenibilidad de
Ecosistemas empresariales contemporáneos. La incorporación sistemática de los requisitos de seguridad.
a lo largo de todo el ciclo de vida de la aplicación, contribuye a reducir las vulnerabilidades y fortalecer la
confianza del usuario, garantizando el cumplimiento de los requisitos reglamentarios y preservando la
continuidad de las operaciones organizativas en un escenario caracterizado por la constante evolución de
amenazas digitales.

Como perspectiva para futuras investigaciones, se recomienda realizar estudios empíricos.
involucrando a organizaciones de diferentes sectores económicos, con el objetivo de evaluar los impactos
desde la adopción de arquitecturas de confianza cero, prácticas DevSecOps, autenticación sin contraseña
autenticación) y algoritmos criptográficos post-cuánticos en la seguridad de aplicaciones móviles
corporativo. Las investigaciones de esta naturaleza pueden ampliar el conocimiento científico sobre el
La eficacia de estos enfoques en entornos organizacionales reales.

REFERENCIAS

ASOCIACIÓN DE MAQUINARIA INFORMÁTICA (ACM). Biblioteca Digital de la ACM. Nueva York, 2024.

FIDO ALLIANCE. FIDO2: Llevando el mundo más allá de las contraseñas. Mountain View, 2024.
GIL, Antonio Carlos. Métodos y Técnicas de Investigación Social. 7ª edición. São Paulo: Atlas, 2019.
KATZ, Jonathan; LINDELL, Yehuda. Introducción a la criptografía moderna. 3.ª ed. Boca Raton: CRC Press, 2020.

INSTITUTO NACIONAL DE ESTÁNDARES Y TECNOLOGÍA (NIST). Marco de Ciberseguridad 2.0. Gaithersburg, 2024.
INSTITUTO NACIONAL DE ESTÁNDARES Y TECNOLOGÍA (NIST). Marco de desarrollo de software seguro (SSDF): SP 800-218. Gaithersburg, 2022.
Proyecto Abierto de Seguridad de Aplicaciones Web (OWASP). Guía de Pruebas de Seguridad de Aplicaciones Móviles (MASTG). 2024.
PRESSMAN, Roger S.; MAXIM, Bruce R. Ingeniería de software: un enfoque práctico. 9.ª ed.
Nueva York: McGraw-Hill, 2020.
SCHNEIER, Bruce. Datos y Goliat: Las batallas ocultas para recopilar sus datos y controlar sus

Este artículo se publica en acceso abierto bajo la licencia Creative Commons Attribution, que permite el uso, la distribución y la reproducción sin restricciones en cualquier medio, siempre que se cite correctamente la obra original.

Machine Translated by Google

Año VII, vol. 2, 2026 | Envío: 04/05/2026 | Aceptado: 07/05/2026 | Publicación: 10/05/2026

Mundo. Nueva York: WW Norton, 2015.

STALLINGS, William. Criptografía y seguridad de redes: principios y práctica. 8.ª ed. Pearson, 2023.

TANENBAUM, Andrew S.; WETHERALL, David J. Redes de computadoras. 6.ª ed. Pearson, 2021.

Este artículo se publica en acceso abierto bajo la licencia Creative Commons Attribution, que permite el uso, la distribución y la reproducción sin restricciones en cualquier medio, siempre que se cite correctamente la obra original.