Machine Translated by Google
RCMOS – Multidisciplinary Scientific Journal The Knowledge.
ISSN: 2675-9128. São Paulo-SP.

Year VII, v.2 2026 | Submission: 04/05/2026 | Accepted: 07/05/2026 | Publication: 10/05/2026

The convergence between cybersecurity and mobile applications in enterprise ecosystems.

The convergence between cybersecurity and mobile applications in enterprise ecosystems

The convergence between cybersecurity and mobile applications in business ecosystems

Adriano Souza Reis

Technologist in Information Technology Management (Uni-Anhanguera); Postgraduate in Artificial Intelligence, Mobile Application Development and Cybersecurity (Faculdade Iguaçu); Doctor Honoris Causa in Information Technology (UNISCECAP); Full Member of ABRASCI.

SUMMARY

The increasing adoption of mobile applications in the corporate environment has significantly transformed how organizations execute processes, share information, and support decision-making. The expansion of mobility has provided greater operational agility, but it has also expanded the surface area exposed to cyber threats, making information security a strategic requirement in software development for mobile devices. This article analyzes the relationship between mobile application development and cybersecurity in enterprise ecosystems, discussing the main risks associated with the use of mobile devices, as well as best practices for data protection, user authentication, secure communication, and continuous monitoring of corporate environments. The research is characterized as a systematic literature review, based on books, scientific articles, technical standards, and documents produced by internationally recognized institutions, considering publications available up to 2024. The results show that the protection of mobile applications depends on the integration of secure software architecture, cryptography, identity management, device governance, and continuous monitoring of technological environments. It can be concluded that mobile application security should be treated as an integral element of the software development process, incorporating security principles from the initial design phases and continuously monitoring the evolution of digital threats.

Keywords: Cybersecurity; Mobile Applications; Secure Development; Data Protection; Corporate Mobility.

ABSTRACT

The increasing adoption of mobile applications in corporate environments has significantly transformed the way organizations execute business processes, exchange information, and support decision-making. Although enterprise mobility has improved operational efficiency, it has also expanded the exposure to cyber threats, making information security a strategic requirement in mobile software development. This article analyzes the relationship between mobile application development and cybersecurity within enterprise ecosystems, discussing the main security risks associated with mobile devices and the best practices for data protection, user authentication, secure communication, and continuous monitoring of corporate environments. The study was conducted through a systematic literature review based on books, peer-reviewed scientific publications, technical standards, and reports issued by internationally recognized institutions, considering publications available up to 2024. The findings indicate that securing mobile applications requires the integration of secure software architecture, cryptography, identity management, device governance, and continuous security monitoring. It is concluded that mobile application security should be incorporated throughout the software development lifecycle, adopting security-by-design principles capable of reducing organizational exposure to emerging cyber threats.

Keywords: Cybersecurity; Mobile Applications; Secure Software Development; Data Protection;

This article is published in open access under the Creative Commons Attribution license, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Machine Translated by Google
IRCMOS – Multidisciplinary Scientific Journal The Knowledge.
ISSN: 2675-9128. São Paulo-SP.

Year VII, v.2 2026 | Submission: 04/05/2026 | Accepted: 07/05/2026 | Publication: 10/05/2026

Enterprise Mobility.

1 INTRODUCTION

Digital transformation has profoundly altered the way organizations develop their
Activities, they share information and manage business processes. The expansion of
cloud computing, mobile connectivity and the availability of smart devices
It allowed corporate applications to no longer be restricted to internal environments.
companies, becoming accessible in any location with an internet connection. This evolution
significantly increased operational flexibility, favoring remote work models,
On-site support, integrated logistics, and real-time decision-making.
The growth of corporate mobility represents one of the most relevant changes in this
process. Applications developed for smartphones and tablets have become integrated into routines
related to commercial management, logistics control, inventory monitoring, customer service
customer, financial operations and monitoring of industrial processes. As a consequence,
Mobile devices have ceased to function solely as communication tools and have taken on the role of...
strategic role within business ecosystems.
However, the expansion of mobility has also changed the information security landscape.
Unlike traditional workstations, which are typically protected by policies.
While centralized and corporate infrastructure allows mobile devices to operate in heterogeneous environments,
frequently connecting to public networks, personal devices, and various services in
cloud. This feature expands the attack surface available to malicious actors and requires
security approaches compatible with the distributed nature of these environments.
Schneier (2015) observes that technological evolution simultaneously expands opportunities for innovation
and challenges related to information protection. As new points of
As access points are incorporated into the organizational infrastructure, the number of vectors also increases.
susceptible to exploitation by cyberattacks. In mobile applications, this scenario becomes even more critical.
more complex due to the diversity of operating systems, manufacturers, configurations of
hardware and upgrade policies that exist in the market.
Among the most frequent threats are traffic interception attacks and exploitation of...
vulnerabilities in APIs, compromised credentials, installation of malicious applications,
social engineering, leakage of locally stored information, and exploitation of libraries.
Vulnerable third parties. The increasing use of personal devices in corporate activities.
This further exacerbates the situation, making it more difficult for companies to directly control the technological infrastructure.

This article is published in open access under the Creative Commons Attribution license, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Machine Translated by Google
RCMOS - Multidisciplinary Scientific Journal The Knowledge.
ISSN: 2675-9128. São Paulo-SP.

Year VII, v.2 2026 | Submission: 04/05/2026 | Accepted: 07/05/2026 | Publication: 10/05/2026

organizations.

In this context, an important change can be observed in the way application security is handled.
mobile is designed. Instead of focusing efforts exclusively on protecting the infrastructure of
As a network, organizations have begun to incorporate security mechanisms throughout all stages of the process.
software development. This approach, known as *Secure by Design,* considers that
requirements related to authentication, cryptography, session management, input validation,
API protection and continuous monitoring should be part of the application architecture from its inception.
design, reducing structural vulnerabilities and subsequent correction costs.

Another aspect that deserves highlighting refers to the strengthening of digital identity models.
Use of multifactor authentication, modern authorization protocols, management
A centralized set of identities and policies based on the principle of least privilege contributes to
to reduce risks associated with compromised credentials. In parallel, the adoption of the model
Zero Trust modifies the traditional logic of corporate security by assuming that no one...
The device, user, or connection should be considered trustworthy without ongoing validation.
regardless of their location on the network.

In addition to preventive measures, the importance of continuous environmental monitoring is growing.
Technological. Mobile device management tools, management platforms.
security events, AI-based solutions and automated mechanisms of
Incident response has come to play an essential role in identifying behaviors.
anomalous, allowing for faster responses to attempted intrusions or compromises.
of the devices.

Given this scenario, understanding the integration between mobile application development and
Cybersecurity has become a necessity for both researchers and professionals.
Those responsible for the development and management of corporate solutions. Information protection.
It has ceased to be an isolated activity within the technology field and has become a strategic requirement.
related to operational continuity, regulatory compliance, and preserving trust in
customers, partners and other stakeholders.

Thus, this article aims to analyze the convergence between cybersecurity and development.
of mobile applications in enterprise ecosystems, discussing the main risks associated with
Corporate mobility, contemporary secure development practices, and mechanisms
technological tools used to protect data, users, and systems in environments characterized by
High connectivity and the constant evolution of digital threats.

This article is published in open access under the Creative Commons Attribution license, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Machine Translated by Google
RCMOS - Multidisciplinary Scientific Journal The Knowledge.
ISSN: 2675-9128. São Paulo-SP.

Year VII, v.2 2026 | Submission: 04/05/2026 | Accepted: 07/05/2026 | Publication: 10/05/2026

2 METHODOLOGY

This research is characterized as a qualitative study, of an exploratory and descriptive nature. developed through a systematic literature review. This methodological strategy was chosen because it allows for the critical analysis of scientific knowledge related to application security. furniture, bringing together contributions from the areas of Software Engineering, Security and Information, Systems Architecture, Computer Networks and Technology Governance Information.

According to Gil (2019), exploratory research is appropriate when the objective is to expand Understanding a particular phenomenon and organizing available knowledge around a common theme. specific topic. In the context of cybersecurity, marked by constant technological evolution, the A systematic literature review makes it possible to identify trends, best practices, and challenges. emerging trends and convergences between different approaches proposed by researchers and organizations. international.

The literature review included books, peer-reviewed scientific articles, and standards. Technical and institutional documents published up to 2024 were prioritized. Indexed publications were given priority. in internationally recognized databases, such as IEEE Xplore, ACM Digital Library, SpringerLink, ScienceDirect, Scopus, and Google Scholar, as well as technical documents produced by organizations. such as OWASP, NIST and FIDO Alliance.

The selection criteria prioritized studies related to mobile application security, Secure Software Development Lifecycle, multifactor authentication, identity management, cryptography Applied, API protection, Mobile Device Management, Zero Trust, DevSecOps and monitoring continuous analysis of corporate environments. Publications lacking scientific basis were excluded. exclusively commercial materials and studies that did not adhere to the objectives of search.

After selecting the references, an analytical and comparative reading of the works was carried out, organizing them. The content is divided into five thematic areas: attack surface in mobile environments, development Software security, cryptographic mechanisms, identity management, and continuous monitoring of applications. This organization made it possible to establish relationships between different approaches present in literature, promoting a critical analysis of the factors that influence application security. Furniture used in corporate environments.

Although the literature review does not involve empirical research in specific organizations, The methodology adopted is considered to provide a consistent basis for understanding the current state of scientific knowledge on the subject, identifying widely recognized good practices, and discussing

This article is published in open access under the Creative Commons Attribution license, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Machine Translated by Google
RCMOS – Multidisciplinary Scientific Journal The Knowledge.
ISSN: 2675-9128. São Paulo-SP.

Year VII, v.2 2026 | Submission: 04/05/2026 | Accepted: 07/05/2026 | Publication: 10/05/2026

The main challenges faced by organizations in protecting their mobile ecosystems.

3. The Attack Surface in Corporate Mobile Environments

The consolidation of corporate mobility has profoundly modified the architecture of systems.
Information used by organizations. The ability to access business applications through
The use of smartphones and tablets has increased team productivity and reduced geographical barriers.
It has made administrative processes more agile. However, this same flexibility has expanded
significantly expands the attack surface of organizations, creating exploitation vectors for
malicious agents.

Unlike traditional workstations, mobile devices operate in environments
Highly dynamic. Over the course of a single day, the same device can connect to the network.
corporate, use 4G or 5G mobile connections, access public Wi-Fi networks and establish
communication with various cloud services. Each change of context alters the environment of
security increases the number of elements that need to be protected.

According to Stallings (2018), information security should consider not only the mechanisms
technological factors employed in protecting the systems, but also the environment in which these systems operate.
They operate. In mobile applications, this premise becomes particularly relevant due to the high
heterogeneity of devices, operating systems, manufacturers, and software versions present
in the corporate environment.

Among the factors contributing to this increase in attack surface area, the adoption of... stands out.
Bring Your Own Device (BYOD) model, in which employees use personal devices to
accessing institutional resources. Although this practice reduces investments in infrastructure and increases
Operational flexibility also makes it difficult to uniformly apply corporate policies.
Security. Private equipment often has different configurations and applications.
installed without organizational control and with different levels of operating system updates,
increasing exposure to vulnerabilities.

Another relevant aspect concerns the networks used when accessing corporate applications.
Users on the go often connect via public networks.
available at airports, hotels, restaurants, shopping centers and other major locations.
circulation. When these networks have insufficient protection mechanisms, they become
environments conducive to traffic interception attacks, access point spoofing and
credential capture.

As described by Tanenbaum and Wetherall (2011), *Man-in-the-Middle* type attacks allow

This article is published in open access under the Creative Commons Attribution license, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Machine Translated by Google
RCMOS - Multidisciplinary Scientific Journal The Knowledge.
ISSN: 2675-9128. São Paulo-SP.

Year VII, v.2 2026 | Submission: 04/05/2026 | Accepted: 07/05/2026 | Publication: 10/05/2026

that an intruder intercepts communication between two systems without the users noticing.
The existence of this intermediation. If the cryptographic mechanisms employed are inadequate.
Whether or not they exist, confidential information can be captured during transmission.
compromising financial data, authentication credentials, and strategic information of
organization.

Local storage of information also represents a significant risk factor. Several
Mobile applications retain temporary data to allow offline operation and reduce data consumption.
bandwidth or improve user experience. When these records remain stored
without adequate encryption mechanisms, devices can be lost, stolen, or compromised.
They may expose sensitive information related to the organization's activities.

In addition to threats related to the communication environment, the fragmentation of ecosystems
Mobile devices pose additional challenges to secure development. In the Android system, for example,
Different manufacturers offer customized versions of the operating system, with cycles
distinct from security updates. As a result, many devices remain for
long periods without receiving fixes for known vulnerabilities, widening the window of
exposure to attacks.

Another factor frequently exploited by malicious actors relates to obtaining privileges.
elevated levels through procedures such as *rooting* or *jailbreaking.* These modifications remove
Restrictions imposed by manufacturers compromise fundamental isolation mechanisms between
applications. As a consequence, malicious applications can gain expanded access to resources.
from the device, compromising information stored by corporate applications and reducing
significantly reduced the effectiveness of the protections originally implemented.

Also worthy of attention is the growth of attacks targeting programming interfaces of
Applications (APIs). In modern architectures, mobile applications concentrate a large part of their...
Business logic on servers, communicating continuously through REST APIs or
GraphQL. Failures related to authentication, authorization, parameter validation, or limitation of
Requests can allow unauthorized access to corporate information, compromising the
integrity and confidentiality of the processed data.

The expansion of the software supply chain represents another significant risk factor.
Contemporary development utilizes a large number of open-source libraries.
Reusable components and third-party services. While these features accelerate development.
applications also increase the possibility of introducing vulnerabilities arising from
Compromised dependencies or outdated components. Recent attacks demonstrate that...
Exploiting the supply chain has become one of the most widely used strategies by groups.

This article is published in open access under the Creative Commons Attribution license, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Machine Translated by Google
RCMOS - Multidisciplinary Scientific Journal The Knowledge.
ISSN: 2675-9128. São Paulo-SP.

Year VII, v.2 2026 | Submission: 04/05/2026 | Accepted: 07/05/2026 | Publication: 10/05/2026

specialized in cybercrime.

Given this scenario, it is clear that the security of mobile applications cannot be limited to Protection of the device or network infrastructure. Recent literature recommends the adoption of models based on the Zero Trust principle, according to which no user, equipment or The connection should be considered trusted automatically. All access requests should be continuously verified, authenticated, and authorized according to the operational context. reducing the likelihood of lateral movement and compromise of corporate environments. Therefore, increasing business mobility demands that security be designed in a way that... integrated, simultaneously considering devices, users, applications, and infrastructure. communication, digital identity, and technology governance. Only this systemic approach is capable of responding to the complexity of contemporary mobile ecosystems and reducing risks. associated with digital transformation.

4. SECURITY-ORIENTED SOFTWARE ENGINEERING (SECURE BY DESIGN)

The increasing sophistication of cyber threats has significantly changed the way we... Enterprise applications are developed. Traditional models, in which security requirements They were incorporated only in the final stages of development, and proved insufficient in the face of... due to the increasing complexity of modern architecture. In response to this scenario, the... The concept of *Secure by Design* proposes incorporating security principles from the very beginning. initial stages of the software lifecycle.

According to Pressman and Maxim (2020), defects identified during the initial specification stages and architecture present a significantly lower cost than the vulnerabilities discovered after the System deployment in a production environment. In addition to the financial impact, vulnerabilities exploited in Corporate applications can compromise operational continuity and cause data leaks. strategic information and generate losses related to institutional reputation.

In this context, the secure development cycle, known as Secure Software Development. Software Lifecycle Management (SSDLC) extends traditional software engineering activities by incorporating... specific practices aimed at identifying, preventing, and mitigating vulnerabilities throughout the development process.

One of the first steps involves threat modeling . Before that... During the implementation of functionalities, development teams analyze the most relevant assets. From the application, they identify potential threat actors, assess existing vulnerabilities and They establish controls capable of reducing the identified risks. This approach allows for anticipation.

This article is published in open access under the Creative Commons Attribution license, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Machine Translated by Google
RCMOS – Multidisciplinary Scientific Journal The Knowledge.
ISSN: 2675-9128. São Paulo-SP.

Year VII, v.2 2026 | Submission: 04/05/2026 | Accepted: 07/05/2026 | Publication: 10/05/2026

safety issues before they are incorporated into the final product.

Another widely adopted principle refers to development based on the concept of privilege.
minimum. Mobile applications should only request the permissions strictly necessary to
How its features work. Unrestricted access to the camera, location, storage,
Contacts or microphones unnecessarily increase the attack surface and amplify the impacts.
resulting from any potential compromise of the application.

Source code protection is also an important component of the strategies of
Secure development. Obfuscation techniques make reverse engineering of applications more difficult.
distributed to users, reducing the possibility of extracting business rules and algorithms.
owners, credentials improperly embedded in the code, and internal mechanisms of
authentication. While they don't completely prevent app analysis, these techniques increase
significantly the effort required for its exploration.

The programming interfaces used by mobile applications deserve special attention during
development. APIs exposed to the internet often constitute the main point of
communication between mobile devices and corporate systems. Because of this, mechanisms
Robust authentication, authorization, input validation, and request *rate limiting.*
Event logging and recording should be integrated into the architecture of these interfaces, reducing related risks.
Injection attacks, privilege escalation, and unauthorized access.

The increasing use of external libraries also demands rigorous library management policies.
dependencies. A large part of modern applications incorporates open-source components.
Responsible for authentication, network communication, encryption, data persistence, and interface.
Graphics. Although these resources accelerate development, vulnerabilities discovered in these...
Libraries can compromise thousands of applications simultaneously. Therefore, it becomes...
It is essential to maintain up-to-date inventories of the dependencies used and to monitor vulnerabilities.
known and perform continuous updates of the components used.

In recent years, the concept of DevSecOps has further strengthened this integration between
development and security. Instead of treating security as the sole responsibility of
specialized teams, the model distributes this responsibility throughout the entire cycle of
development, incorporating automated checks directly into the integration pipelines and
continuous deliveries.

Static analysis tools *(Static Application Security Testing – SAST)* allow you to identify
Vulnerabilities are detected directly in the source code before the application is compiled.
Additionally, dynamic analysis mechanisms *(Dynamic Application Security Testing –*
DASTs evaluate the behavior of running software, identifying faults that can only be detected if...

This article is published in open access under the Creative Commons Attribution license, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Machine Translated by Google
RCMOS - Multidisciplinary Scientific Journal The Knowledge.
ISSN: 2675-9128. São Paulo-SP.

Year VII, v.2 2026 | Submission: 04/05/2026 | Accepted: 07/05/2026 | Publication: 10/05/2026

They manifest during their operation. The combined use of these approaches expands significantly improves the ability to identify vulnerabilities early.

Another practice that has recently gained relevance is the use of a Software Bill of Materials. (SBOM), a document that lists all the components used during the construction of application. This approach facilitates the management of the software supply chain, allowing quickly identify which applications use components affected by newly discovered vulnerabilities. discoveries and accelerating incident response processes.

Also noteworthy is the periodic performance of penetration tests and validation exercises. security. Unlike automated analyses, these activities simulate behavior. of malicious agents, allowing the identification of vulnerabilities arising from the interaction between different architectural components, configuration errors, or environment-related failures operational.

It can be observed, therefore, that safe development has ceased to represent a complementary step. from software engineering to becoming a structuring element of enterprise applications Contemporary. Incorporating security requirements from the system design stage reduces costs, increases application reliability, and strengthens organizations' ability to... To respond to the threats present in today's digital ecosystems.

5 Cryptographic Protocols for Data Protection in Applications

FURNITURE

Cryptography is one of the fundamental pillars of information security and plays an indispensable role in protecting mobile applications used in corporate environments. As Mobile devices have begun processing strategic information related to operations.

In the areas of finance, logistics, healthcare, e-commerce, and business management, it has become necessary to adopt mechanisms capable of guaranteeing confidentiality, integrity, authenticity, and non-repudiation during The entire data lifecycle.

According to Katz and Lindell (2020), contemporary cryptographic security does not depend It's not just about the robustness of the algorithms used, but about the correct implementation of the protocols. proper management of cryptographic keys and the integration of these mechanisms with the architecture of the application. Vulnerabilities related to certificate management, storage Inadequate key usage or incorrect use of cryptographic libraries can compromise Systems that employ mathematically sound algorithms.

In the context of mobile applications, protecting data in transit is one of the primary concerns.

This article is published in open access under the Creative Commons Attribution license, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Machine Translated by Google
RCMOS - Multidisciplinary Scientific Journal The Knowledge.
ISSN: 2675-9128. São Paulo-SP.

Year VII, v.2 2026 | Submission: 04/05/2026 | Accepted: 07/05/2026 | Publication: 10/05/2026

Layers of defense. Information exchanged between devices and corporate servers travels...
continuously through different communication infrastructures, including mobile networks, Wi-Fi connections
Public networks and cloud service providers. This diversity of environments increases the
possibility of traffic interception by malicious actors if appropriate mechanisms are not in place.
protection should not be employed.

In this scenario, the use of the Transport Layer Security (TLS) protocol has become established as
A basic requirement for modern enterprise applications. TLS version 1.3 reduced vulnerabilities.
present in previous implementations, it simplified the cryptographic trading process and
It provided gains in both performance and security. In addition to the confidentiality of
In communication, the protocol ensures authentication between client and server and mechanisms that preserve
the integrity of the transmitted messages.

However, the isolated use of TLS does not completely eliminate the risks associated with communication.
between mobile applications and corporate services. Several attacks exploit digital certificates.
fraudulent or inadequate validation mechanisms implemented by the applications themselves.
To reduce this possibility, many organizations adopt a technique known as *Certificate*
Pinning, which consists of the explicit validation of the server's cryptographic identity during the process.
Establishing the connection.

This approach prevents certificates issued by compromised certification authorities or
Certificates inserted locally by malicious applications are accepted by the application. Although the
Certificate Pinning requires greater control during digital certificate renewal processes, your
Its use significantly reduces the possibility of attacks based on interception of
communication.

Another relevant aspect concerns the protection of information stored locally in
mobile devices. In many situations, corporate applications need to maintain data
Temporary measures to ensure offline functionality, subsequent synchronization, or improved experience.
from the user. When this storage is unavoidable, it becomes essential to employ mechanisms.
robust encryption capable of protecting this information even in situations of loss or theft.
or device impairment.

The Advanced Encryption Standard (AES) algorithm, especially in key-based implementations.
256-bit architecture remains one of the top recommendations for protecting data at rest.
However, the literature highlights that the effectiveness of this mechanism depends directly on how...
Cryptographic keys are stored and managed. Key storage directly
Including code in application code or configuration files represents an inappropriate practice, as it facilitates...
Its extraction through reverse engineering.

This article is published in open access under the Creative Commons Attribution license, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Machine Translated by Google
RCMOS – Multidisciplinary Scientific Journal The Knowledge.
ISSN: 2675-9128. São Paulo-SP.

Year VII, v.2 2026 | Submission: 04/05/2026 | Accepted: 07/05/2026 | Publication: 10/05/2026

To reduce this risk, mobile operating systems provide protected environments designed for specifically for the secure storage of cryptographic credentials. On Android, this function is This function is performed by the Android Keystore, while iOS devices use Keychain Services. associated with the Secure Enclave. These components keep the keys isolated from the rest of the system. operational, significantly reducing the likelihood of compromise even in the face of malicious applications running on the device.

In addition to confidentiality, the integrity of the information must also be ensured. Algorithms Cryptographic tools designed for generating *hash* functions allow you to verify if A particular file or message underwent changes during its storage or transmission. However, historically used algorithms, such as MD5 and SHA-1, have vulnerabilities. known and are no longer recommended for applications that require high levels of security. Currently, the use of algorithms belonging to the SHA-2 or families is recommended. SHA-3, according to the specific needs of the application.

Another topic that has gained importance in recent years concerns the preparation of architectural designs. Cryptographic tools for the advancement of quantum computing. Although practical attacks against the algorithms While currently used methods do not yet represent an immediate risk to most organizations, Institutions responsible for international standardization have already begun the development process. and the adoption of algorithms resistant to quantum computing. This perspective reinforces the need for Flexible cryptographic architectures, capable of incorporating new standards as they are developed. officially established.

Therefore, it can be observed that the cryptographic protection of mobile applications depends on the combination of robust algorithms, correct implementation of protocols, secure key management and Continuous updating of the libraries used. Cryptography should be understood as an integral part of the application architecture and not an embedded add-on feature. only in the final stages of development.

6. Identity Management and Access Control in Mobile Applications

As mobile applications have begun to offer critical functionalities for organizations In both public and private sectors, identity management has become a central element of strategies. Information security. The simple use of credentials consisting of a username and password. proved insufficient to respond to the growth of threats related to account compromise, password reuse, and targeted automated attacks on corporate systems.

This article is published in open access under the Creative Commons Attribution license, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Machine Translated by Google
RCMOS - Multidisciplinary Scientific Journal The Knowledge.
ISSN: 2675-9128. São Paulo-SP.

Year VII, v.2 2026 | Submission: 04/05/2026 | Accepted: 07/05/2026 | Publication: 10/05/2026

Several studies demonstrate that compromised credentials remain among the top risks.
Vectors used for intrusions into corporate environments. Brute-force attacks,
Credential stuffing, social engineering, and *phishing* campaigns exploit recurring behaviors.
of users, such as password reuse and the adoption of predictable combinations. Because of this
In this scenario, organizations have begun to incorporate additional authentication mechanisms capable of...
significantly reduce the likelihood of unauthorized access.
Multifactor authentication (MFA) has established itself as one of the most effective measures in this context.
The principle consists of the simultaneous use of two or more independent factors for validation.
of the user's identity, combining information that he knows, possesses or represents.
Biologically, even if a password is compromised, the absence of other factors makes it more difficult.
essentially the exploitation of the credentials obtained by the attacker.
In mobile applications, the integration between multifactor authentication and biometric features has become...
particularly efficient due to the presence of native sensors incorporated into the devices
Modern technologies such as fingerprints, facial recognition, and other biometric mechanisms can be used.
used to validate the user's identity without the need for biometric data.
transmitted to corporate servers. In architectures compatible with FIDO standards.
Alliance, verification occurs locally on the device, preserving user privacy and
reducing the exposure of sensitive information.
In addition to authentication, the management of sessions established between mobile devices and
Corporate servers require specific protection mechanisms. Unlike applications
Traditional architectures based on persistent sessions, modern architectures often utilize
token-based authorization protocols, such as OAuth 2.0 and OpenID Connect, associated with
The use of JSON Web Tokens (JWT) when appropriate. These mechanisms allow control over...
Validity period of credentials, limiting granted privileges, and facilitating revocation processes.
access.

However, the literature also highlights that the use of JWT requires care related to...
token storage, expiration control, and protection against reuse attacks.
(replay attacks). The adoption of tokens with short expiration periods, associated with controlled renewal.
And by securely storing credentials, it significantly reduces these vulnerabilities.
Another key component relates to centralized identity management. Solutions for
Single Sign-On (SSO) allows users to authenticate only once to access different
corporate applications, simplifying the user experience and reducing the proliferation of credentials.
independent. From an administrative perspective, this approach facilitates the management of
Permissions, access auditing, and immediate revocation of authorizations when necessary.

This article is published in open access under the Creative Commons Attribution license, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Machine Translated by Google
RCMOS - Multidisciplinary Scientific Journal The Knowledge.
ISSN: 2675-9128. São Paulo-SP.

Year VII, v.2 2026 | Submission: 04/05/2026 | Accepted: 07/05/2026 | Publication: 10/05/2026

Privilege management should also follow the principle of least privilege .
according to which each user receives only the permissions strictly necessary for the performance of
their activities. This strategy significantly reduces the impacts resulting from
Account compromise and limits the lateral movement of attackers within the infrastructure.
corporate.

In recent years, traditional authentication models have begun to incorporate associated principles.
adaptive authentication. Instead of considering only username and password, these mechanisms analyze
Contextual factors such as geographic location, time of access, device used, address
IP address, historical behavior, and connection characteristics. Whenever unusual patterns are
Once identified, additional authentication mechanisms may be automatically required before...
Granting access.

This approach is strongly aligned with the principles of the Zero Trust model, in which...
Identity is no longer validated only at the initial moment of authentication and becomes...
Continuously reevaluated throughout the interaction between user and system. Thus, changes
Relevant behavior may result in preventative blocking, credential renewal, or...
Request for additional authentication factors.

Beyond the technological aspects, identity management also involves components
Organizational guidelines related to access governance. Clear policies for creating, periodically reviewing, and...
Revoking permissions helps reduce orphaned accounts, unauthorized access, and inconsistencies.
resulting from the movement of employees between different roles within the organization.

Thus, it can be observed that identity management represents a strategic layer of
Mobile application security. Its effectiveness depends on the integration of robust authentication,
Centralized credential management, continuous monitoring of user behavior.
and governance policies capable of keeping pace with the operational dynamics of organizations.
contemporary. These mechanisms, when implemented in an integrated manner, strengthen
significantly protect digital assets and reduce organizations' exposure to major [risks/criticisms].
threats related to credential compromise.

7. Continuous Monitoring, Incident Response, and Governance of MOBILE SECURITY

The adoption of preventive mechanisms represents only one dimension of security.
Information. In corporate environments characterized by high connectivity and constant
Given the evolution of digital threats, it is assumed that technical controls will be able to prevent all of them.

This article is published in open access under the Creative Commons Attribution license, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Machine Translated by Google
RCMOS - Multidisciplinary Scientific Journal The Knowledge.
ISSN: 2675-9128. São Paulo-SP.

Year VII, v.2 2026 | Submission: 04/05/2026 | Accepted: 07/05/2026 | Publication: 10/05/2026

Attempts at compromise became incompatible with the operational reality of organizations. In this context, the continuous monitoring of technological assets plays a crucial role. strategic in the early identification of incidents and in reducing the impacts resulting from attacks. cybernetics.

The contemporary concept of defense in depth presupposes the integrated use of Preventive, detective, and corrective mechanisms. In addition to implementing access controls, Robust encryption and authentication make it necessary to continuously monitor behavior. of applications, devices, and users, allowing the identification of changes that may indicate Attempts to exploit vulnerabilities or compromise corporate environments.

Among the technologies used for this monitoring, *mobile* platforms stand out. *Device Management* (MDM) and *Enterprise Mobility Management* (EMM). These solutions enable remotely administer devices used by the organization, establish security policies, control settings, restrict features that are incompatible with corporate guidelines and Apply updates in a centralized manner. In environments where devices coexist. institutional and personal equipment used in *Bring Your Own Device* (BYOD) policies . These tools play a fundamental role in standardizing the minimum requirements for security.

In addition to device administration, remote management allows you to perform procedures. Critical in situations of compromise, loss, or theft of equipment. Resources such as Remote blocking, revocation of digital certificates, selective removal of corporate information and Restoring security settings significantly reduces the risk of exposure. Confidential data.

Another essential component relates to monitoring the events produced by the companies themselves. Mobile applications. Authentication logs, configuration changes, failed access attempts. Authorization, permission changes, and communication failures constitute important sources of... information for identifying suspicious activities. When properly structured, this Records make it possible to reconstruct the sequence of events associated with an incident and to support... forensic investigation processes.

In this context, *Security Information and Event Management* (SIEM) platforms consolidate information from different sources within the technological infrastructure, allowing for correlation seemingly isolated events and identifying patterns consistent with ongoing attacks. A Integration between mobile applications, servers, network devices, and cloud services expands significantly improves the ability of security teams to detect anomalous behavior. before they produce significant impacts on organizational operations.

This article is published in open access under the Creative Commons Attribution license, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Machine Translated by Google
RCMOS – Multidisciplinary Scientific Journal The Knowledge.
ISSN: 2675-9128. São Paulo-SP.

Year VII, v.2 2026 | Submission: 04/05/2026 | Accepted: 07/05/2026 | Publication: 10/05/2026

In recent years, techniques based on artificial intelligence and machine learning have begun to...
complement these platforms through behavioral analysis of users and devices.
Models known as *User and Entity Behavior Analytics* (UEBA) allow for the establishment of profiles.
usage patterns considered normal for each user or piece of equipment, automatically identifying
significant deviations related to access time, geographic location, volume of
transactions or usage patterns of corporate resources.
Although these technologies do not replace the analysis performed by security teams, their
Using this method reduces the time needed to identify potentially malicious behavior.
and contributes to prioritizing events that require immediate investigation. In this way, the
The ability of organizations to respond quickly to incidents and minimize their impact.
operational.
Another frequently overlooked aspect concerns the management of updates to
software. Recently discovered vulnerabilities make rapid distribution of software indispensable.
Fixes for mobile applications and operating systems. Automated update processes.
Over-the-Air (OTA) allows for the centralized delivery of new versions of applications.
ensuring that devices remain protected against known vulnerabilities and reducing the
Persistence of vulnerable versions in operation.
Alongside monitoring activities, organizations should establish formal plans for
Incident response plans are compatible with their operational characteristics. These plans define
Responsibilities, communication procedures, incident classification criteria,
containment mechanisms, service recovery, and analysis of the root causes of the events.
identified. The existence of structured processes reduces response time and minimizes losses.
operational and promotes institutional learning resulting from incidents that have occurred.
Also noteworthy is the periodic performance of penetration tests, simulation exercises and
Information security maturity assessments. These initiatives allow for the validation of effectiveness.
From the controls implemented, identify vulnerabilities that have not yet been exploited and improve them.
Continuously improve organizational processes related to the protection of mobile applications.
From a corporate governance perspective, continuous monitoring should be understood
as a permanent activity integrated into institutional strategies. The constant evolution of
Digital threats require frequent updates to security policies and a review of mechanisms.
control, training of professionals and systematic monitoring of related indicators
to the protection of technological assets.
It can be observed, therefore, that the security of mobile applications does not depend exclusively on adoption.
not only advanced technologies, but also the ability of organizations to establish continuous processes of

This article is published in open access under the Creative Commons Attribution license, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Machine Translated by Google

Year VII, v.2 2026 | Submission: 04/05/2026 | Accepted: 07/05/2026 | Publication: 10/05/2026

Monitoring, incident response, and continuous improvement. Integration between tools.
Technology, governance, processes, and people are key elements for strengthening [the company/organization].
of cyber resilience in increasingly distributed and interconnected business ecosystems.

CONCLUSION

The increasing use of mobile applications has significantly changed operational dynamics.
of organizations, expanding the availability of corporate systems and favoring models of
Work is becoming increasingly flexible. At the same time, this transformation has increased complexity.
technological environments have expanded the surface area exposed to cyber threats, making the
Information security is a strategic requirement for the development and operation of these
applications.

The literature review demonstrated that protecting mobile ecosystems requires an approach...
multidimensional, involving secure software architecture, cryptography, management of
identity, protection of communication interfaces, continuous monitoring and governance of
Information security. These elements work in a complementary way and should be incorporated.
from the early stages of application development, reducing structural vulnerabilities and
increasing the capacity to respond to security incidents.

It was also found that traditional protection models based exclusively on the perimeter of the
Corporate networks no longer meet the needs imposed by enterprise mobility.
The use of distributed devices, cloud services, and hybrid environments requires mechanisms.
continuous authentication, contextual validation of accesses, and application of the principles associated with
Zero Trust model, in which users, devices, and connections are constantly evaluated before use.
granting or maintaining access privileges.

Another relevant aspect identified during the study refers to the growing importance of integration.
between software development and information security. Practices such as Secure by Design,
Secure Software Development Lifecycle, DevSecOps, and software supply chain management.
They demonstrate that vulnerability prevention should occur throughout the entire lifecycle.
development, reducing maintenance costs and increasing the reliability of applications.
corporate.

The results also show that continuous monitoring plays a key role in
Protection of mobile environments. Device management platforms, correlation systems.
of events, behavioral analyses based on artificial intelligence, and structured processes of
Incident response significantly enhances organizations' ability to identify

This article is published in open access under the Creative Commons Attribution license, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Machine Translated by Google

Year VII, v.2 2026 | Submission: 04/05/2026 | Accepted: 07/05/2026 | Publication: 10/05/2026

Detecting suspicious activities, containing attacks in their early stages, and reducing operational impacts.
arising from security events.
However, the effectiveness of these strategies also depends on organizational factors.
defining governance policies, the continuous updating of technological controls, the
Professional qualifications and user awareness remain key components.
indispensable for strengthening corporate security. Technology, by itself, does not eliminate
risks arise when it is not accompanied by consistent processes and an organizational culture geared towards
information protection.
Based on the evidence presented, it can be concluded that the convergence between the development of
Mobile applications and cybersecurity are essential elements for the sustainability of
Contemporary business ecosystems. The systematic incorporation of security requirements.
throughout the entire application lifecycle, it contributes to reducing vulnerabilities and strengthening the
user trust, ensuring compliance with regulatory requirements, and preserving the
continuity of organizational operations in a scenario characterized by the constant evolution of
digital threats.
As a perspective for future research, it is recommended that empirical studies be conducted.
involving organizations from different economic sectors, with the goal of evaluating the impacts
from the adoption of Zero Trust architectures, DevSecOps practices, passwordless *authentication*
authentication) and post-quantum cryptographic algorithms in mobile application security
corporate. Investigations of this nature may broaden scientific knowledge about the
The effectiveness of these approaches in real organizational environments.

REFERENCES

ASSOCIATION FOR COMPUTING MACHINERY (ACM). *ACM DigitalLibrary.* New York, 2024.

FIDO ALLIANCE. *FIDO2: Moving the World Beyond Passwords.* Mountain View, 2024.
GIL, Antonio Carlos. *Methods and Techniques of Social Research.* 7th ed. São Paulo: Atlas, 2019.
KATZ, Jonathan; LINDELL, Yehuda. *Introduction to Modern Cryptography.* 3rd ed. Boca Raton: CRC Press, 2020.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST). *Cybersecurity Framework 2.0.*
Gaithersburg, 2024.
NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST). *Secure Software Development Framework*
(SSDF): SP 800-218. Gaithersburg, 2022.
OPEN WEB APPLICATION SECURITY PROJECT (OWASP). *Mobile Application Security Testing Guide*
(MASTG). 2024.
PRESSMAN, Roger S.; MAXIM, Bruce R. *Software Engineering: A Practitioner's Approach.* 9. ed.
New York: McGraw-Hill, 2020.
SCHNEIER, Bruce. *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your*

This article is published in open access under the Creative Commons Attribution license, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Machine Translated by Google

Year VII, v.2 2026 | Submission: 04/05/2026 | Accepted: 07/05/2026 | Publication: 10/05/2026

World. New York: WW Norton, 2015.

STALLINGS, William. *Cryptography and Network Security: Principles and Practice.* 8. ed. Pearson, 2023.

TANENBAUM, Andrew S.; WETHERALL, David J. *Computer Networks.* 6. ed. Pearson, 2021.

This article is published in open access under the Creative Commons Attribution license, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.