A TSC Company
BLUEBIRD

WHITE PAPER

DOCUMENTO TÉCNICO DE SEGURIDAD EN COMPUTACIÓN MÓVIL DE BLUEBIRD

Impulsando las mejores prácticas de seguridad en computación móvil con Bluebird

Las iniciativas móviles están a la vanguardia de las prioridades estratégicas de la mayoría de las empresas en la actualidad. Este aumento de la movilidad organizativa se traduce en un mayor número de usuarios que acceden y utilizan dispositivos en diversas ubicaciones, incluidos entornos remotos. Si bien esto potencia una mayor productividad y eficiencia de su personal, los equipos de TI y seguridad se enfrentan al creciente reto de proteger un número cada vez mayor de terminales y garantizar la seguridad de los datos críticos en una gran variedad de dispositivos.

Las organizaciones que buscan proteger sus dispositivos móviles, como smartphones empresariales, tabletas y computadoras móviles especializadas, pueden lograrlo implementando las sólidas mejores prácticas de seguridad en computación móvil de Bluebird.

Para subrayar la importancia crítica de la seguridad a nivel de dispositivo en el ámbito móvil, consideremos las siguientes estadísticas relevantes:

- Una encuesta de Gartner de 2024 indica que el 63 % de las organizaciones globales han adoptado total o parcialmente una estrategia de confianza cero[1], lo que subraya un cambio significativo en la industria hacia una protección integral de dispositivos, incluyendo todos los activos de computación móvil, dentro de las redes empresariales.

- Un Informe Global de Amenazas Móviles de 2025 reveló que más del 50 % de los dispositivos móviles funcionan en sistemas operativos obsoletos en cualquier momento, lo que crea vulnerabilidades significativas.[2]

- Según Forbes, las brechas de seguridad aumentaron un 72 % en 2023 en comparación con 2021, con IBM reportando un ciclo medio de vida de 292 días.[3]

Estadísticas de seguridad para dispositivos móviles

Adopción del modelo Zero Trust

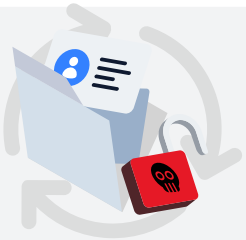
63 %

de las organizaciones han implementado una estrategia de confianza cero

Sistemas operativos móviles desactualizados

50 %▲

de los dispositivos móviles funcionan con sistemas operativos obsoletos



Tiempo de detección de brechas

292 días

Ciclo de vida promedio de una brecha

1. **Encuesta de Gartner:** https://www.gartner.com/en/newsroom/press-releases/2024-04-22-gartner-survey-reveals-63-percent-of-organizations-worldwide-have-implemented-a-zero-trust-strategy
2. **Informe global sobre amenazas móviles 2025 (Zimperium):** https://lp.zimperium.com/hubfs/Reports/2025%20Global%20Mobile%20Threat%20Report.pdf
3. **Estadísticas globales sobre ciberseguridad:** https://www.varonis.com/blog/cybersecurity-statistics

Estas cifras ilustran de forma contundente por qué integrar todos los dispositivos móviles en una estrategia de seguridad holística es fundamental, no solo para proteger datos invaluables, sino también para evitar que se conviertan en el eslabón más débil de la cadena de defensa de su organización.

Bluebird: Una postura proactiva en seguridad

Proteger los dispositivos y los datos sensibles es fundamental para garantizar flujos de trabajo fluidos y fomentar un rendimiento empresarial sólido. Bluebird mitiga activamente los riesgos y vulnerabilidades de seguridad integrando múltiples capas de protección en nuestros dispositivos y soluciones. Cada componente de nuestra oferta —desde el diseño de hardware hasta el software y servicios integrales— está meticulosamente diseñado para defenderse contra amenazas de seguridad comunes como malware, phishing, fallos criptográficos y diseño inseguro, todo ello sin comprometer la productividad ni la accesibilidad esenciales.

A medida que las empresas se interconectan cada vez más, sus redes y datos valiosos son más susceptibles a accesos no autorizados y diversas vulnerabilidades de seguridad. Bluebird aborda estos riesgos adhiriéndose a los principios fundamentales de ciberseguridad e implementando un enfoque de defensa en profundidad a lo largo de nuestra arquitectura y procesos de diseño. Gracias a nuestra tecnología innovadora y altamente configurable, Bluebird capacita a las organizaciones para lograr un equilibrio óptimo entre objetivos operativos críticos y posturas de seguridad robustas.

Aprendiendo de las vulnerabilidades para construir soluciones seguras

Bluebird analiza y aprende continuamente de vulnerabilidades pasadas de dispositivos móviles, desde métodos de ataque históricos hasta descubrimientos más recientes. Esta visión continua impulsa nuestro compromiso con el desarrollo de soluciones de seguridad más inteligentes y resilientes, diseñadas específicamente para afrontar los complejos desafíos actuales de la informática móvil.

Cada vez que se identifica una nueva vulnerabilidad, el equipo dedicado de Bluebird toma medidas rápidas para preparar y desplegar un parche. Este proceso se basa en un riguroso sistema de clasificación basado en la lista de Vulnerabilidades y Exposiciones Comunes (CVE), que es gestionado diligentemente por la Base de Datos Nacional de Vulnerabilidades. A cada vulnerabilidad o amenaza se le asigna un nivel de gravedad — que va de 0,1 (bajo) a 10 (crítico) según el Sistema Común de Puntuación de Vulnerabilidades (CVSS) — detallando las acciones esenciales que las empresas deben tomar para su protección.

Bluebird también supervisa de cerca el Open Web Application Security Project (OWASP), que proporciona información y reportes anuales sobre las principales vulnerabilidades móviles. Por ejemplo, al abordar vulnerabilidades clave como

Lista CVE*

*CVE: Vulnerabilidades y exposiciones comunes

CVSS*

*CVSS: Sistema común de puntuación de vulnerabilidades

OWASP*

*OWASP: Proyecto de Seguridad de Aplicaciones Web Abiertas

SDLC*

*SDLC: Ciclo de vida del desarrollo de software

el control de acceso defectuoso y los fallos de inyección, Bluebird se asegura de que todas las principales vulnerabilidades móviles se analicen a fondo. Nuestro ecosistema holístico, que abarca tanto el hardware como el software de nuestros dispositivos, está diseñado para abordar de manera integral las vulnerabilidades móviles existentes. Nuestros dispositivos se someten a exhaustivas fases de pruebas de seguridad, que incluyen rigurosas evaluaciones de seguridad internas (análisis de código estático y dinámico), así como pruebas de penetración independientes realizadas por terceros. Estas pruebas externas garantizan la solidez de nuestros controles de seguridad, ya que los evaluadores de penetración simulan los intentos reales de los hackers de eludir las distintas capas de protección.

Los dispositivos Bluebird se desarrollan siguiendo estrictamente un Ciclo de Vida de Desarrollo de Software (SDLC) exigido por la empresa. Esto garantiza que todo el software Bluebird esté diseñado y probado siguiendo estrictas directrices de seguridad integradas en nuestro SDLC. La estricta implementación del principio de menor privilegio y controles robustos de la Interfaz de Programación de Aplicaciones (API) impide que usuarios no autorizados accedan a dispositivos. Además, las pruebas exhaustivas de aplicaciones de extremo a extremo mejoran consistentemente la seguridad. Bluebird está comprometido a ampliar continuamente nuestro portafolio de características de seguridad a medida que surjan nuevas amenazas.

Bluebird rastrea diligentemente las vulnerabilidades y amenazas de Android™ mediante el monitoreo de CVE y OWASP. Colaboramos con los proveedores y aprovechamos nuestra experiencia interna para proporcionar los parches adecuados, garantizando que todos los dispositivos móviles estén protegidos contra amenazas críticas y de menor riesgo mediante nuestros mecanismos integrales de actualización de seguridad.

Bluebird garantiza que cada vulnerabilidad móvil crítica sea analizada a fondo, y que todo nuestro ecosistema —que abarca tanto el hardware como el software de nuestros dispositivos— está diseñado para abordar proactivamente las vulnerabilidades móviles existentes.

Simplifique la gestión del ciclo de vida del dispositivo con las soluciones BOS ™ de Bluebird

Basándose en décadas de investigación y desarrollo, así como en el conocimiento de innumerables casos de uso empresariales, la suite Business Optimizing Solution (BOS™) de Bluebird ofrece un conjunto completo de herramientas empresariales diseñadas para maximizar la productividad de los usuarios móviles y minimizar las complejidades de TI a lo largo del ciclo de vida de los dispositivos. Esta suite incluye numerosas soluciones creadas para simplificar y optimizar la gestión del ciclo de vida de los dispositivos móviles, desde la integración hasta la seguridad robusta y mucho más. Las soluciones BOS™ de Bluebird mejoran la capacidad de su equipo de TI para responder a las amenazas de seguridad nuevas y emergentes con características como:

- **Principio del menor privilegio:**
Más allá de limitar el acceso a los dispositivos, Bluebird mejora aún más este principio al detectar cualquier escalada de privilegios para llamadas al sistema, aplicación o componente, asegurando un control granular.

- **Defensa en profundidad:**
El enfoque en capas de Bluebird para la seguridad garantiza que los datos permanezcan completamente seguros, tanto en movimiento como en reposo. Nuestra arquitectura protege cada capa de un dispositivo móvil de vulnerabilidades y las analiza para proporcionar una protección integral y un verdadero enfoque de "defensa en profundidad". Bluebird ofrece una protección superior frente a multitud de amenazas de seguridad, reduciendo el riesgo y prolongando la vida útil de sus dispositivos. Esto incluye protección respaldada por hardware del almacenamiento de firmware para asegurar que el sistema operativo y el cargador de arranque no se modifiquen, así como comunicaciones seguras de punta a punta.

- **Soporte de seguridad ampliado para el sistema operativo:**
Bluebird ofrece un soporte de seguridad ampliado para el sistema operativo, lo que garantiza que sus dispositivos reciban actualizaciones de seguridad oportunas durante años, maximizando su vida útil.

- **BOS NEST™ para actualizaciones OTA (Over the Air):**
Nuestra herramienta de gestión de movilidad empresarial BOS NEST™ permite controlar y programar actualizaciones de dispositivos de forma remota, alineándose con los requerimientos de seguridad y flexibilidad operativa del negocio.

- **Soporte para cumplimiento normativo:**
Con el compromiso de Bluebird con la correcta aplicación de parches de seguridad y actualizaciones, las organizaciones obtienen tranquilidad al saber que sus dispositivos pueden ayudarlas a cumplir con regulaciones en constante cambio, como la Ley de Portabilidad y Responsabilidad del Seguro Médico (HIPAA) o la Certificación del Modelo de Madurez en Ciberseguridad (CMMC).

- **BOS™ Kiosk / Enterprise Launcher:**
Evite interrupciones operativas y proteja la productividad de la plantilla personalizando las interfaces de usuario y el acceso a los dispositivos: especifique a qué aplicaciones pueden acceder los usuarios, desactive las funciones no deseadas de los dispositivos e inicie automáticamente las aplicaciones necesarias.

- **BOS™ Power Manager:**
Supervise de forma centralizada el estado y la salud de las baterías en toda la flota de dispositivos, permitiendo una gestión proactiva y reduciendo tiempos de inactividad inesperados.

- **BOS™ Device Finder:**
Localice rápidamente dispositivos perdidos o extraviados mediante señales BLE, mejorando la recuperación de activos y reduciendo tiempos de búsqueda.

- **Mensajería segura:**
Facilite canales de comunicación seguros entre el personal, garantizando el intercambio protegido de información sensible dentro del entorno operativo.

Mayor confianza en la seguridad de los dispositivos móviles

Bluebird se adhiere rigurosamente a los pilares fundamentales de la ciberseguridad, proporcionando confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de las acciones con nuestros productos. Bluebird cuenta con la confianza de sectores críticos, como la seguridad pública, los servicios de emergencia y diversos clientes gubernamentales y empresariales de todo el mundo. Bluebird mantiene un firme compromiso con las mejores prácticas de seguridad y colabora con expertos del sector para garantizar que nuestros dispositivos cumplan con estrictas normas de seguridad, lo que en conjunto genera confianza en los usuarios respecto a la seguridad de los dispositivos.

Confianza reforzada con un entorno de ejecución confiable (TEE)

Un mecanismo clave que las organizaciones utilizan para proteger las operaciones criptográficas y el material sensible es el Entorno de Ejecución Confiable (TEE). Este entorno opera de forma aislada del Entorno de Ejecución Enriquecida (REE) del dispositivo, donde residen el sistema operativo principal y las aplicaciones. Dentro del TEE, el código se ejecuta con un alto nivel de confianza, ya que su entorno está completamente aislado del resto del sistema. Cualquier amenaza detectada en el REE no puede afectar al TEE. Incluso si el REE se ve comprometido, los datos dentro del TEE permanecen seguros.

Bluebird proporciona una capa adicional de seguridad a los TEE de las organizaciones, integrando funciones como nuestro quiosco BOS™ / Enterprise Launcher. Por ejemplo, nuestro Enterprise Launcher permite a los administradores controlar qué usuarios tienen acceso a entornos específicos, asegurando que los datos sensibles o confidenciales permanezcan seguros. Al seguir de forma constante las mejores prácticas de TEE (que están integradas en todos los dispositivos Bluebird recientemente producidos), los TEE están fuertemente protegidos frente a nuevas y emergentes amenazas de seguridad.

Computadoras Móviles

Solución RFID

Tabletas Empresariales*

Programa proactivo de pruebas de seguridad de Bluebird

Bluebird adopta un enfoque proactivo en materia de seguridad. En lugar de limitarnos a reaccionar a amenazas de seguridad, realizamos regularmente pruebas internas de seguridad, incluyendo intentos de identificar vulnerabilidades de código o debilidades del sistema dentro de nuestros propios dispositivos. Una vez identificadas, Bluebird rectifica rápidamente el problema, corrigiendo los fallos o creando una actualización de seguridad específica para eliminar la vulnerabilidad. Esto reduce significativamente la probabilidad de que los ciberdelincuentes identifiquen y aprovechen las vulnerabilidades, lo que de otro modo podría tener consecuencias devastadoras para las empresas.

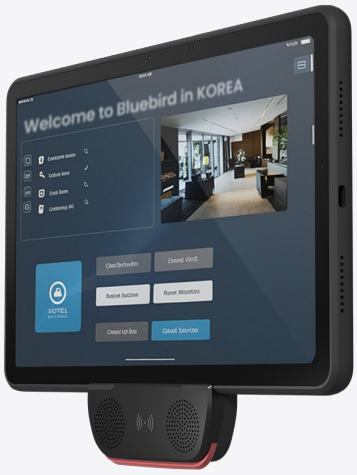
Refuerce la seguridad en computación móvil con Bluebird

Durante casi tres décadas, Bluebird ha sido líder en innovación en dispositivos móviles empresariales y estamos comprometidos a proporcionar a las organizaciones soluciones de seguridad integrales diseñadas según las mejores prácticas del sector. Todo nuestro catálogo de soluciones de seguridad está meticulosamente diseñado desde cero para ofrecer seguridad total sin comprometer la accesibilidad ni la escalabilidad. En materia de seguridad en dispositivos móviles, Bluebird ofrece protección y control inigualables.

Para obtener más información sobre cómo Bluebird protege sus dispositivos móviles con funciones de seguridad de primera clase, visite https://latam.tscprinters.com/en/mobile-computers

Terminales de Pago*

Quiosco Interactivo*



Automotriz*

*Disponibilidad limitada en EE. UU., Canadá y América Latina; por favor, contacte a su representante de ventas local.

Bluebird Inc. (Sede corporativa)

www.bluebirdcorp.com

Tel. +82-1577-0778 Fax. +82-2-6499-2242

06355, 3F, 115, Irwon ro, Gangnam gu, Seoul, Republic of Korea

Bluebird Alemania GmbH

EUROPE@bluebirdcorp.com

Tel. +49-6196-7761262, 06196-7761263

FAX. +49-6196-7761264

Ober der Röth 4, 65824 Schwalbach am Taunus, Germany

Bluebird Europe S.L.

bluebird.spain@bluebirdcorp.com

C/ José Abascal, 53, 6ª Planta, 28003, Madrid, Spain

Bluebird USA Inc.

bluebird.usa@bluebirdcorp.com

3775 Venture DR, BLDG E, Duluth, GA, 30096, USA

Bluebird América Latina

latam@bluebirdcorp.com

AV. Paseo de la Reforma 265, Edificio Axtel Piso 2, Cuauhtemoc, C.P. 06500, CDMX, Mexico

Bluebird India - Centro de Investigación y Desarrollo

2nd Floor, RPR Complex, Site No. A 52, Kamadhenu Nagar, B.Narayanapura, Mahadevapura, Bangalore, Karnataka, India

Bluebird Corea - Centro de Servicio r

TEL. +82-1660-3202

21315, #B-710, Bupyeong-daero 283, Bupyeong-gu, Incheon, Republic of Korea

Centro de Tecnología de Fabricación Bluebird

TEL. +82-1588-1380 FAX. +82-31-731-4341

13216, B 6F~8F, 531, Dunchon-daero, Jungwon-gu, Seongnam-si, Gyeonggi-do, Republic of Korea

SEDE CORPORATIVA
TSC Auto ID Technology Co., Ltd.
Tel: +886 2 2218 6789
E-mail: apac_sales@tscprinters.com

PLANTA DE LI ZE
TSC Auto ID Technology Co., Ltd.
Tel: +886 3 990 6677
E-mail: apac_sales@tscprinters.com

CHINA
Tianjin TSC Auto ID Technology Co., Ltd.
Tel: +86 22 5981 6661
E-mail: apac_sales@tscprinters.com

EMEA
TSC Auto ID Technology EMEA GmbH
Tel: +49 (0) 8106 37979 000
E-mail: emea_sales@tscprinters.com

AMÉRICAS
TSC Auto ID Technology America Inc.
Tel: +1 657 258 0808
E-mail: americas_sales@tscprinters.com

ASIA PACÍFICO
TSC Auto ID Technology Co., Ltd.
Tel: +886 2 2218 6789
E-mail: apac_sales@tscprinters.com

RUSIA
TSC Auto ID Technology EMEA GmbH
Tel: +7 495 646 3538
E-mail: emea_sales@tscprinters.com

MÉXICO
Oficina de Representación de TSC México
Tel: +1 52 (33) 3673 1406
E-mail: americas_sales@tscprinters.com

COREA
Oficina de Representación de TSC Corea
Tel: +82 2 852 3322
E-mail: apac_sales@tscprinters.com

ORIENTE MEDIO
TSC Auto ID Technology ME Ltd, FZE
Tel: +971 4 2533 069
E-mail: emea_sales@tscprinters.com

BRASIL
Oficina de Representación de TSC Brasil
Tel: +55 (11) 3554 7225
E-mail: americas_sales@tscprinters.com

INDIA
Oficina de Representación de TSC India
Tel: +91 2249 679 315
E-mail: apac_sales@tscprinters.com