| Tipo de ataque | ¿Qué hace? | Ejemplo común | Cómo protegerte? |
|---|---|---|---|
| **Phishing** | Engaña a usuarios para robar datos | Email suplantando a tu banco. Entregas paquetes | Formación continua al personal |
| **Ransomware** | Secuestra tu información hasta que pagues | WannaCry, LockBit | Backups frecuentes + DRP |
| **Malware** | Software malicioso que se instala sin permiso | Troyanos, spyware | Antivirus actualizado y navegación segura |
| **DDoS** | Satura servidores y bota servicios | Ataques a sitios web gubernamentales | Firewall, CDN y monitoreo |
| **Ingeniería Social** | Manipula a las personas para obtener acceso | “Llamadas del soporte técnico” | Cultura organizacional en seguridad |
| **Man-in-the-Middle** | Intercepta comunicaciones | Red WiFi pública intervenida | VPN + HTTPS obligatorio |

WAFRA TRANSFORMATION

Ingrid Mora

# Top 10 países más atacados cibernéticamente (2024–2025)

| Ranking | País | Motivo de alta exposición |
|---|---|---|
| 1 | Japón | Infraestructura crítica, I+D, sector financiero |
| 2 | España | Gran digitalización, alto volumen de ransomware, ataques crecientes a PYMEs y e-commerce |
| 3 | Estados Unidos | Objetivo frecuente por su tamaño y relevancia global |
| 4 | Brasil | Alto uso de tecnología, sector financiero vulnerable |
| 5 | India | Aumento explosivo en ataques estatales y phishing |
| 6 | México | Digitalización rápida con baja protección en PYMEs |
| 7 | Australia | Grandes filtraciones en sectores salud y telecomunicaciones |
| 8 | Canadá | Objetivo de ransomware y ataques a gobiernos locales |
| 9 | Corea del Sur | Tensión geopolítica y ataques avanzados patrocinados por estados |
| 10 | Reino Unido | Aumento de ataques a bancos y gobiernos locales |

Ingrid Mora

WAFRA TRANSFORMATION

# Oferta vs Demanda en Ciberseguridad – Global

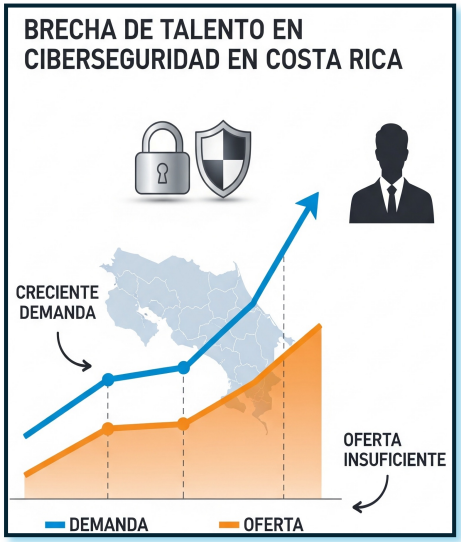
| Aspecto | Cantidad | Fuente |
|---|---|---|
| Profesionales activos (2025) | 5.5 millones | ISC² Workforce Study, 2025 |
| Profesionales requeridos (2025) | 10.2 millones | Cybersecurity Ventures, 2025 |
| **Brecha estimada (2025)** | **4.7 millones** | World Economic Forum / BCG, 2025 |

Ingrid Mora

# Oferta vs Demanda en Ciberseguridad – Costa Rica

| Aspecto | Cantidad / Porcentaje | Fuente |
|---|---|---|
| Profesionales activos (2025) | 1,600 | CINDE, 2022 |
| Nuevas vacantes creadas (2023) | 1,200 | MICITT – Indeed, 2023 |
| Vacantes estimadas por semana | 20+ | Reddit / Mercado laboral, 2025 |
| Medianas empresas que invierten en ciberseguridad (2025) | 100 % | DPL News, 2025 |
| **Factores que limitan la oferta de talento especializado** | Bajo nivel de inglés, brechas digitales, formación desconectada | CRHoy / PROCOMER / CINDE, 2025 |

WAFRA



# Principales ciberataques hacia usuarios móviles

| Ataque | ¿Qué hace? | Cómo llega? | Cómo protegerse? | Sistema afectado |
|---|---|---|---|---|
| **Smishing** | Phishing por SMS o mensajería instantánea. Busca robar contraseñas o datos bancarios. | Mensajes de texto, WhatsApp, Telegram | No hacer clic en enlaces sospechosos ni compartir datos | **Android / iOS** |
| **Aplicaciones maliciosas** | Instalan malware, roban información o activan micrófono/cámara. | Descargas fuera de tiendas oficiales o en tiendas con escaso control | Usar solo Google Play o App Store | **Principalmente Android** |
| **Malware móvil** | Controla el dispositivo, accede a tus datos y puede espiarte. | Archivos adjuntos, páginas engañosas, redes WiFi falsas | Antivirus móvil, cuidado al navegar | **Principalmente Android** |
| **Spyware** | Monitorea ubicación, llamadas, mensajes o redes sociales en secreto. | Instalado por terceros (parejas, empleados, etc.) | Revisar permisos, apps ocultas, rendimiento extraño | **Android / iOS (con jailbreak)** |
| **Redes WiFi falsas (Evil Twin)** | Finge ser una red confiable para robar datos cuando te conectas. | Lugares públicos (cafés, aeropuertos) | VPN, no conectarse a redes abiertas | **Android / iOS** |
| **Rogue Apps (Apps falsas)** | Se hacen pasar por apps legítimas para engañar al usuario. | Descargas engañosas o tiendas oficiales con escaso control | Verificar desarrollador, reseñas, permisos excesivos | **Principalmente Android** |
| **Ataques vía Bluetooth** | Intercepta datos o accede a tu dispositivo sin que lo notes. | Cercanía física + Bluetooth activado | Apagar Bluetooth si no se usa | **Android / iOS** |

WAFRA TRANSFORMATION

Ingrid Mora

# **Comparativo** entre **ISO/IEC 27001** y **ISO/IEC 27002** (versión 2022 para ambas)

Ingrid Mora

| Característica | ISO/IEC 27001:2022 | ISO/IEC 27002:2022 |
|---|---|---|
| **Enfoque principal** | Norma certificable que establece los **requisitos** para implementar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI). | Norma **de referencia** que proporciona **directrices y buenas prácticas** para implementar los controles de seguridad de la información. |
| **Propósito** | Servir de marco para auditar y certificar un SGSI. | Servir de guía para aplicar los controles listados en el Anexo A de la 27001. |
| **Contenido** | Incluye: contexto de la organización, liderazgo, planificación, soporte, operación, evaluación del desempeño, mejora y **Anexo A** con 93 controles. | Incluye descripción detallada de cada control, propósito, directrices de implementación y posibles atributos. |
| **Tipo de norma** | **Norma de requisitos** (obligaciones que deben cumplirse para certificarse). | **Norma de directrices** (no certificable por sí misma, complementa a la 27001). |
| **Certificación** | Sí, una organización puede certificarse. | No, es solo referencia técnica. |
| **Relación entre ambas** | La 27001 **remite** a la 27002 para entender y aplicar los controles del Anexo A. | La 27002 **explica** cómo implementar los controles que la 27001 menciona. |
| **Ejemplo práctico** | Dice **"debe implementar un control de gestión de accesos"**. | Explica **cómo** implementar ese control, con prácticas recomendadas, ejemplos y atributos. |

WAFRA TRANSFORMATION