*Seguridad Digital*

Unidad para la Prevención y el Análisis Criminológico (UPAC) – Costa Rica +Segura

**La nueva delincuencia sin rostro:**
**Costa Rica ante el aumento de los delitos informáticos**

En Costa Rica, la digitalización de la vida cotidiana ha traído consigo una nueva realidad criminal: el aumento acelerado de los delitos informáticos. Solo en 2024 se registraron 10.040 denuncias relacionadas con cibercrimen, según datos del Organismo de Investigación Judicial (OIJ), Sección de Delitos Informáticos. Detrás de números fríos hay personas afectadas por estafas electrónicas, robo de identidad, accesos indebidos y manipulación de información personal. En un entorno donde la vida social, laboral y financiera transcurre frente a una pantalla, la seguridad digital dejó de ser opcional para convertirse en un componente clave de la seguridad ciudadana.

El ciberespacio se ha convertido en unos de los principales centro de operaciones de las personas; con acceder a un dispositivo electrónico y en segundos se pueden se ejecutan transferencias bancarias, educación, compras, citas médicas, trabajo remoto y hasta trámites estatales. Sin embargo, este ecosistema tecnológico también ha sido aprovechado por grupos criminales que, desde el anonimato, logran ganancias significativas con mínimos riesgos.

Hoy los delincuentes ya no necesitan armas ni violencia física para ejecutar un delito: basta un enlace fraudulento, un mensaje convincente o un acceso indebido a una contraseña. Las medidas básicas, pero de alto impacto, para evitar ser víctima de un ataque digital,

siendo la primera de ellas el uso de contraseñas fuertes y únicas, combinando letras, números y símbolos, y evitando repetir claves en distintas plataformas

La criminología y la ciberseguridad coinciden en que el eslabón más débil no es el sistema, sino el usuario. El OIJ advierte que gran parte de las estafas electrónicas se ejecutan mediante ingeniería social: manipulación psicológica para obtener información. Basta un enlace sospechoso para comprometer toda la información de un teléfono o computadora.

Se puede recomendar acciones como:

- Mantener los dispositivos actualizados, porque las actualizaciones corrigen vulnerabilidades de seguridad.

- No abrir enlaces sospechosos, verificados o enviados por desconocidos

- Evitar redes Wi-Fi públicas, ya que permiten capturar datos personales o credenciales

Las recomendaciones parecen sencillas, pero su incumplimiento explica gran parte de los casos de fraude digital. La seguridad digital es ya un componente de la seguridad ciudadana. Sin embargo, mientras los criminales evolucionan a gran velocidad, las políticas públicas no avanzan al mismo ritmo.

Tres aspectos preocupan desde la criminología:

1. Educación digital insuficiente. No existe una estrategia nacional permanente de alfabetización en ciberseguridad para niños, adultos y personas mayores, que son los más vulnerables a estafas telefónicas y phishing.

2. Falta de campañas estatales sostenidas. Las recomendaciones para seguridad digital existen, pero no llegan a la población con urgencia ni frecuencia. Se ha logrado demostrar que acciones básicas de prevención pueden reducir significativamente el riesgo individual

3. Acelerada evolución del cibercrimen. Los delitos informáticos no requieren presencia física, tienen baja trazabilidad y alta ganancia, lo cual los convierte en un delito atractivo para organizaciones criminales.

La digitalización llegó para quedarse; lo que falta es una cultura colectiva de autoprotección digital. La seguridad dejó de medirse solo en candados, cámaras o patrullas: hoy se mide también en contraseñas fuertes, navegación segura y criterio digital.

En un país donde más de 10 mil denuncias informáticas fueron interpuestas solo en un año, proteger datos es proteger la identidad, las finanzas y la integridad personal. La prevención, más que una opción, es una responsabilidad social. Ciberseguridad ciudadana en tiempos de hiperconexión y vulnerabilidad digital: La delincuencia sin rostro ya está aquí. La pregunta no es si intentarán atacarnos, sino qué tan preparados estaremos cuando ocurra.

**Fuentes Bibliográficas**


Organismo de Investigación Judicial. (2024). *Denuncias relacionadas con delitos informáticos*. Sección de Delitos Informáticos.

Cámara de Tecnologías de la Información y Comunicación (CAMTIC) & Organismo de Investigación Judicial. (2024). *Informe sobre ciberseguridad y filtración de datos en Costa Rica*.

Superintendencia General de Entidades Financieras. (2023). *Estadísticas de fraude financiero por canales digitales*. SUGEF.

Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones. (2023). *Programa Nacional de Ciberseguridad 2023-2027*. MICITT.