Ciberdelitos en Costa Rica y la Criptografía como Herramienta de Defensa

Víctor Sibaja Reyes
Universidad Internacional San Isidro Labrador, Escuela de Ingeniería en Sistemas, San José, Costa Rica, victallisyslaw@gmail.com

Resumen – Este artículo examina la creciente amenaza de los ciberdelitos en Costa Rica, los tipos de delitos más comunes, las tendencias recientes y su impacto en la sociedad costarricense. Además, se analiza el papel crucial de la criptografía en la defensa contra estos delitos, al tiempo que se discuten las estrategias necesarias para asegurar que los ciberdelincuentes no queden impunes. Finalmente, se propone una serie de recomendaciones para mejorar la ciberseguridad en el país.

Palabras clave: Ciberdelitos, Costa Rica, Criptografía, Ciberseguridad, Delitos Informáticos, Protección de Datos, Fraude Cibernético, Legislación Cibernética.

I. INTRODUCCIÓN

El avance de la tecnología y el crecimiento del acceso a Internet han transformado la manera en que las sociedades modernas operan, proporcionando innumerables beneficios económicos y sociales. Sin embargo, este progreso también ha facilitado la aparición de nuevas formas de criminalidad, particularmente en el ciberespacio. Los ciberdelitos, definidos como actos ilegales realizados a través de medios electrónicos, han experimentado un incremento alarmante en todo el mundo. En Costa Rica, este fenómeno no es una excepción. A medida que el país ha avanzado en la digitalización de su economía y la adopción de nuevas tecnologías, también ha visto un aumento en la incidencia de ciberdelitos.

Este documento tiene como objetivo proporcionar un análisis exhaustivo de la situación de los ciberdelitos en Costa Rica, explorando los tipos de delitos más comunes, las tendencias actuales, y el impacto que tienen en la sociedad costarricense. Además, se destacará el papel fundamental que juega la criptografía como una herramienta en la defensa contra estas amenazas y se abordarán las medidas necesarias para garantizar que los ciberdelincuentes no operen con impunidad.

II. CIBERDELITOS EN COSTA RICA

A. Definición y Clasificación de Ciberdelitos

Los ciberdelitos abarcan una amplia gama de actividades delictivas que se realizan a través de medios electrónicos. En Costa Rica, estos delitos se clasifican generalmente en dos categorías principales: delitos dirigidos contra sistemas informáticos (como ataques de denegación de servicio, malware, y hackeo), y delitos en los que la tecnología es utilizada como una herramienta para perpetrar actividades ilegales (como el fraude, la extorsión, y el robo de identidad).

Entre los ciberdelitos más prevalentes en Costa Rica se encuentran:

1. **Robo de Identidad**: La obtención y uso fraudulento de la información personal de alguien, como números de seguridad social, datos bancarios, o información de tarjetas de crédito, para cometer fraude.
2. **Suplantación de Identidad (Phishing)**: Intentos fraudulentos de obtener información confidencial de las víctimas haciéndose pasar por una entidad confiable, generalmente a través de correos electrónicos o sitios web falsos.
3. **Extorsión**: El uso de amenazas o chantajes, muchas veces a través de ataques de ransomware, para obtener pagos o favores de las víctimas.
4. **Fraude Electrónico**: Cualquier actividad fraudulenta realizada a través de sistemas electrónicos, incluyendo estafas de inversión, fraudes de tarjetas de crédito, y esquemas de Ponzi digitales.
5. **Ciberterrorismo**: El uso de medios digitales para llevar a cabo actos de terror o daño a nivel nacional o internacional.

B. Estadísticas y comparaciones regionales.

Según el Instituto Costarricense sobre Drogas, Costa Rica se posiciona en el cuarto lugar en América Latina en cuanto al uso de Internet para actividades ilícitas, precedida por Brasil, México y Colombia. Esta posición refleja la creciente sofisticación de los ciberdelincuentes en el país y la necesidad de reforzar las estrategias de ciberseguridad.

Entre 2016 y 2019, el número de denuncias relacionadas con ciberdelitos en Costa Rica se duplicó, reflejando un patrón de aumento similar al observado en otras naciones de la región.

En 2020, por ejemplo, se registraron más de 7,000 denuncias de ciberdelitos, siendo el fraude cibernético y el phishing los delitos más reportados. Este incremento coincide con el mayor acceso a Internet y la creciente adopción de servicios en línea en el país, asimismo debido a la pandemia.

La proyección de esta tendencia hasta agosto de 2024 muestra un panorama preocupante:

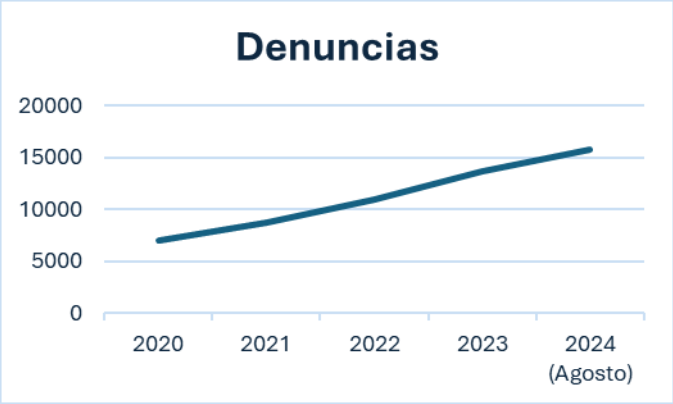

Fig 1. Fuente del OIJ muestra aumento constante en el número de denuncias por ciberdelitos, con un crecimiento anual estimado del 25%.

En cuanto a la distribución de los tipos de ciberdelitos, las estimaciones para agosto de 2024 revelan que:

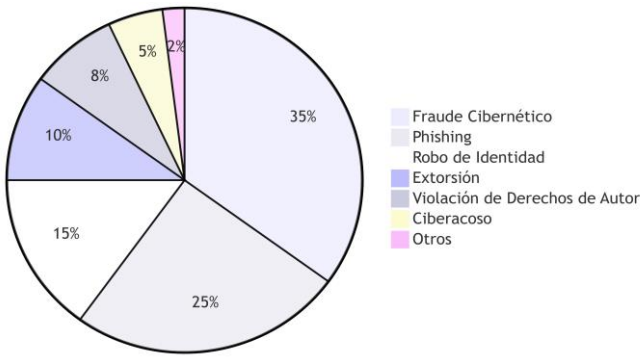

Fig 2. Fuente del OIJ muestra una distribución estimada de los tipos de ciberdelitos en Costa Rica para agosto de 2024. Las proporciones se basan en las tendencias actuales y las proyecciones para el futuro.

C. Casos relevantes

Uno de los casos más destacados de ciberdelito en Costa Rica fue el ataque de ransomware sufrido por el Ministerio de Hacienda en 2019. Este ataque paralizó varios sistemas críticos durante días, afectando la recaudación de impuestos y la gestión financiera del país. El incidente subrayó la vulnerabilidad de las infraestructuras críticas a los ataques cibernéticos y la necesidad de mejorar las medidas de ciberseguridad en el sector público.

III. TENDENCIAS E IMPACTO DE LOS CIBERDELITOS

A. Crecimiento del Uso de Internet y su Correlación con el Ciberdelito

Costa Rica ha experimentado un crecimiento significativo en la penetración de Internet en los últimos años. Según datos de la Unión Internacional de Telecomunicaciones (UIT), más del 72% de la población costarricense tiene acceso a Internet, lo que ha fomentado el desarrollo de la economía digital y el comercio electrónico en el país. Sin embargo, este crecimiento también ha proporcionado un terreno fértil para el aumento de los ciberdelitos.

Las autoridades han observado que a medida que más personas acceden a servicios en línea, como la banca electrónica y las plataformas de comercio electrónico, también aumenta la exposición a riesgos cibernéticos. Los ciberdelincuentes han aprovechado esta expansión, desarrollando métodos más sofisticados para explotar las vulnerabilidades de los sistemas y engañar a los usuarios desprevenidos.

B. Impacto Económico y Social

El impacto de los ciberdelitos en Costa Rica no se limita a pérdidas financieras directas, aunque estas son significativas. Según estimaciones, las pérdidas anuales debidas al fraude cibernético en el país podrían superar los $50 millones USD. Sin embargo, el daño va más allá de lo económico; los ciberdelitos también causan graves daños a la reputación de las empresas y erosionan la confianza de los consumidores en el entorno digital.

Además, el costo de recuperar la información perdida, reparar los sistemas comprometidos, y la inversión en medidas de ciberseguridad puede ser considerable, especialmente para pequeñas y medianas empresas. Estas compañías a menudo carecen de los recursos para implementar medidas de protección avanzadas, lo que las hace más vulnerables a los ataques.

C. Legislación Vigente

Costa Rica ha realizado esfuerzos significativos para

actualizar su marco legal en respuesta a la creciente amenaza de los ciberdelitos. Las principales leyes que abordan este tema incluyen:

1. Ley de Protección de la Persona frente al Tratamiento de sus Datos Personales (Ley N° 8968)
2. Ley de Delitos Informáticos y Conexos (Ley N° 9048)
3. Ley sobre Registro, Secuestro y Examen de Documentos Privados e Intervención de las Comunicaciones (Ley N° 7425)

D. Desafíos en la Aplicación de la Ley

A pesar de contar con un marco legal, Costa Rica enfrenta varios desafíos en la aplicación efectiva de estas leyes:

1. Jurisdicción: Muchos ciberdelitos son cometidos desde fuera del país, dificultando la persecución legal.
2. Evidencia Digital: La recolección y presentación de evidencia digital presenta desafíos técnicos y legales.
3. Capacitación: Existe una necesidad de capacitar a jueces y fiscales en temas de ciberdelincuencia.
4. Cooperación Internacional: La naturaleza transnacional de los ciberdelitos requiere una mayor cooperación entre países.

IV. LA CRIPTOGRAFÍA COMO HERRAMIENTA CONTRA LOS CIBERDELITOS

A. Principios Básicos de la Criptografía

La criptografía es la ciencia de proteger la información a través de técnicas de codificación y cifrado, asegurando que solo las partes autorizadas puedan acceder a los datos protegidos. Existen varios métodos de criptografía, incluyendo la criptografía simétrica, la criptografía asimétrica, y los algoritmos de hash, cada uno de los cuales tiene aplicaciones específicas en la ciberseguridad.

1. Criptografía Simétrica: Utiliza una única clave para cifrar y descifrar la información, lo que requiere que ambas partes compartan esa clave de manera segura.
2. Criptografía Asimétrica: Utiliza un par de claves – una pública y una privada – donde la clave pública se utiliza para cifrar los datos y la clave privada para descifrarlos.
3. Algoritmos de Hash: Generan un resumen fijo de los datos, que es único para cada conjunto de información y se utiliza para verificar la integridad de los datos.

B. Aplicaciones en la Ciberseguridad

La criptografía juega un papel crucial en diversas áreas de la ciberseguridad. Algunas de las aplicaciones más importantes incluyen:

1. Protección de la Confidencialidad de la Información: Los métodos criptográficos aseguran que solo las partes autorizadas puedan leer la información transmitida, lo que es esencial en las comunicaciones sensibles, como las transacciones bancarias.
2. Integridad de los Datos: Los algoritmos de hash se utilizan para verificar que los datos no hayan sido alterados durante la transmisión, lo que protege contra ataques de manipulación.
3. Autenticación y Verificación de Identidades: La criptografía asimétrica se utiliza para verificar la identidad de los usuarios, asegurando que solo los usuarios legítimos puedan acceder a los sistemas.
4. Firmas Digitales: Estas aseguran que los documentos electrónicos no hayan sido modificados y que el remitente es quien dice ser, lo que es fundamental para el cumplimiento de contratos y la legalidad de transacciones electrónicas.

C. Rol de los Abogados en la Ciberseguridad

Los abogados desempeñan un papel crucial en la intersección entre la tecnología y la ley, especialmente en el ámbito de la ciberseguridad. Con el aumento de los ciberdelitos, es fundamental que los profesionales legales comprendan y apliquen principios de criptografía en su práctica. Esto no solo mejora la protección de la información sensible de sus clientes, sino que también fortalece la integridad de los procesos legales en el entorno digital.

D. Aplicaciones Prácticas de la Criptografía para Abogados

1. Protección de Comunicaciones Cliente-Abogado:
    - Implementación de sistemas de correo electrónico cifrado para garantizar la confidencialidad de las comunicaciones con los clientes.
    - Uso de plataformas de mensajería segura con cifrado de extremo a extremo para discusiones sensibles.
2. Manejo Seguro de Documentos:
    - Utilización de sistemas de gestión de documentos con cifrado incorporado para proteger archivos confidenciales.
    - Implementación de firmas digitales para autenticar y verificar la integridad de documentos legales.
3. Evidencia Digital:
    - Aplicación de técnicas criptográficas para preservar la cadena de custodia de la evidencia digital, asegurando su admisibilidad en los tribunales.
    - Uso de funciones hash para verificar la integridad de los archivos digitales

presentados como evidencia.

4. Contratos Inteligentes:
    - Comprensión y aplicación de principios criptográficos en la creación y ejecución de contratos inteligentes basados en blockchain.
5. Protección de Datos de Clientes:
    - Implementación de sistemas de almacenamiento cifrado para proteger la información personal y financiera de los clientes.
    - Uso de técnicas de anonimización y pseudonimización de datos para cumplir con regulaciones de protección de datos.

E. Desafíos y Limitaciones

A pesar de sus beneficios, la criptografía no es una panacea. Existen desafíos significativos en su implementación, incluyendo la gestión segura de claves, la necesidad de actualizaciones constantes para contrarrestar nuevas amenazas, y la posibilidad de errores humanos en la configuración de los sistemas criptográficos. Además, los avances en la computación cuántica podrían poner en riesgo algunos de los métodos criptográficos actuales, lo que subraya la necesidad.

V. GARANTIZAR QUE LOS CIBERDELINCUENTES NO QUEDEN IMPUNES

Para disuadir la actividad delictiva en el ciberespacio, es crucial que los ciberdelincuentes no queden impunes. Sin embargo, la investigación y persecución de estos delitos presentan desafíos únicos. Los delincuentes pueden operar desde cualquier parte del mundo, utilizando técnicas sofisticadas de anonimato y encriptación para ocultar sus identidades y evadir la detección. Por lo tanto, es imperativo desarrollar nuevas estrategias y herramientas para combatir los ciberdelitos, asegurando que los perpetradores sean llevados ante la justicia.

Algunas medidas importantes incluyen:

1. Fortalecimiento de la cooperación internacional
2. Mejora de las capacidades de investigación digital
3. Implementación de programas de capacitación continua para las fuerzas del orden
4. Establecimiento de unidades especializadas en ciberdelitos
5. Fomento de la colaboración público-privada en la lucha contra el cibercrimen

VI. RECOMENDACIONES Y CONCLUSIONES

Para mejorar la ciberseguridad en Costa Rica y combatir eficazmente los ciberdelitos, se proponen las siguientes recomendaciones:

1. Actualización continua del marco legal para abordar las nuevas formas de ciberdelitos.
2. Inversión en tecnología y capacitación para las fuerzas del orden.
3. Fomento de la cooperación internacional en la lucha contra el cibercrimen.
4. Implementación de programas de educación en ciberseguridad para el público general.
5. Establecimiento de un centro nacional de ciberseguridad.

Asimismo, dentro la practica legal, podemos integrar la criptografía con recomendaciones como las siguientes:

1. Educación Continua:
    - Participación en programas de formación sobre ciberseguridad y criptografía aplicada al derecho.
    - Mantenimiento actualizado sobre las últimas tendencias y amenazas en ciberdelincuencia.

2. Adopción de Mejores Prácticas:
    - Implementación de políticas de seguridad de la información que incorporen principios criptográficos.
    - Realización de auditorías regulares de seguridad para evaluar y mejorar las prácticas de protección de datos.

3. Colaboración Interdisciplinaria:
    - Establecimiento de relaciones con expertos en ciberseguridad para asesoramiento técnico.
    - Participación en grupos de trabajo que aborden la intersección entre tecnología y derecho.

4. Desarrollo de Protocolos:
    - Creación de directrices claras para el manejo de información digital sensible.
    - Establecimiento de procedimientos para responder a incidentes de seguridad cibernética.

Los ciberdelitos representan una amenaza creciente para la seguridad y estabilidad de Costa Rica. La criptografía se presenta como una herramienta eficaz en la lucha contra estos delitos, pero es igualmente esencial garantizar que los ciberdelincuentes no queden impunes. La colaboración entre el gobierno, la sociedad y el sector privado es vital para abordar este desafío y proteger a la población de los peligros

que emanan del ciberespacio.

La integración de la criptografía en la práctica legal no solo mejora la seguridad de la información, sino que también posiciona a los abogados como líderes en la protección de los derechos digitales de sus clientes. Al adoptar estas prácticas, los profesionales legales pueden fortalecer su capacidad para enfrentar los desafíos de la era digital y contribuir significativamente a la lucha contra los ciberdelitos.

VII. REFERENCIAS

[1] Instituto Costarricense sobre Drogas. (2020). Estadísticas sobre el uso de Internet en Costa Rica.

[2] García, P. (2019). La Criptografía y su impacto en la ciberseguridad. Revista de Tecnología y Sociedad, 15(3), 45-58.

[3] Caja Costarricense de Seguro Social. (2021). Comunicado Oficial sobre Incidente de Ciberseguridad.

[4] Asamblea Legislativa de Costa Rica. (2011). Ley de Protección de la Persona frente al Tratamiento de sus Datos Personales (Ley N° 8968).

[5] Asamblea Legislativa de Costa Rica. (2012). Ley de Delitos Informáticos y Conexos (Ley N° 9048).

[6] Unión Internacional de Telecomunicaciones. (2020). Informe sobre el Desarrollo Mundial de las Telecomunicaciones/TIC.

[7] Ministerio de Ciencia, Tecnología y Telecomunicaciones de Costa Rica. (2020). Estrategia Nacional de Ciberseguridad.