2025

Centro de Respuestas a Incidentes Informáticos
CSIRT Académico UNAD

Lo que nos cuentan los datos

ANALISIS A LA INFORMACIÓN DEL SITIO WEB DATOS ABIERTOS RESPECTO A SEGURIDAD INFORMÁTICA

VIEM
Vicerrectoría de Innovación y Emprendimiento

ECBTI
Escuela de Ciencias Básicas, Tecnología e Ingeniería

Semillero de Investigación
Ceros y Unos

E-boletín Informativo CSIRT Académico UNAD

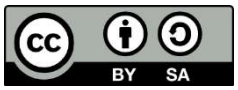
Medio de divulgación: Correo Electrónico, Sitio Web

Incluye: Noticias, alertas o informes relacionados con la disciplina de la ciberseguridad

Número treinta uno [31]
Abril de 2025

Universidad Nacional Abierta y a Distancia (UNAD)
Vicerrectoría de Innovación y Emprendimiento (VIEM)
Escuela de Ciencias Básicas Tecnología Ingeniería (ECBTI)
Maestría en Ciberseguridad
Especialización en Seguridad Informática
CSIRT Académico UNAD

Universidad Nacional Abierta y a Distancia
Calle 14 sur No. 14-23 | Bogotá D.C
Correo electrónico: csirt@unad.edu.co
Página web: https://csirt.unad.edu.co



Edición electrónica, financiada por la Universidad Nacional Abierta y a Distancia (UNAD)

Vicerrectoría de Innovación y Emprendimiento (VIEM)
Ing. Andrés Ernesto Salinas
Vicerrector

Escuela de Ciencias Básicas Tecnología e Ingeniería (ECBTI)
Ing. Claudio Camilo González Clavijo
Decano

Maestría en Ciberseguridad (ECBTI)
Ing. Sonia Ximena Moreno Molano
Líder Programa de Maestría en Ciberseguridad

Semillero de Investigación Ceros y Unos, adscrito al Grupo de Byte InDesign

Centro de Desarrollo Tecnológico CSIRT Académico UNAD
Ing. Luis Fernando Zambrano Hernández
Líder CSIRT Académico UNAD

Responsable de la Edición
Ing. Luis Fernando Zambrano Hernandez

Revisó
Ing. Hernando Peña Hidalgo
Analista CSIRT Académico UNAD

Estado legal:
Periodicidad: Mensual
ISSN: 2806-0164

Contenido

Introducción

La transformación digital que atraviesa la sociedad colombiana ha traído consigo un aumento exponencial en la incidencia y sofisticación de los delitos informáticos. Los datos oficiales públicos en el sitio https://www.datos.gov.co/ y encuestas aplicadas a la comunidad UNADISTA[1] evidencian que los incidentes asociados a la seguridad de la información no solo se han incrementado en número, sino que también se han diversificado en su tipología y alcance, afectando a usuarios, organizaciones y entidades públicas por igual. El análisis muestra patrones claros: el acceso abusivo a sistemas informáticos, la violación de datos personales y el daño informático constituyen la mayoría de los casos reportados. Estos delitos encuentran su marco normativo en la Ley 1273 de 2009, que estableció los cimientos jurídicos para la persecución penal de las conductas que atentan contra la integridad, confidencialidad y disponibilidad de la información. El crecimiento sostenido en la cantidad de incidentes, la concentración de casos en los principales centros urbanos, y la alta correlación entre población y frecuencia de delitos subrayan la necesidad de fortalecer las capacidades institucionales, tanto para la prevención como para la respuesta ante incidentes. Al mismo tiempo, la evidencia recopilada en las encuestas revela una brecha importante en la percepción y el conocimiento sobre los riesgos informáticos, lo que exige redoblar los esfuerzos en formación, sensibilización y cultura de ciberseguridad. Este panorama plantea un desafío multidimensional para las instituciones académicas, los entes públicos y privados, y la ciudadanía en general. Solo a través de un enfoque integral, que combine el cumplimiento normativo, la actualización tecnológica, la gestión efectiva de incidentes y la formación continua de la comunidad, será posible reducir la vulnerabilidad y construir entornos digitales más seguros y resilientes.

El presente boletín recoge y analiza los principales hallazgos obtenidos a partir de las fuentes oficiales y los ejercicios de diagnóstico institucional, con el objetivo de ofrecer una visión clara y fundamentada sobre la realidad de los delitos informáticos en Colombia, y servir de base para la toma de decisiones, el diseño de políticas y el fortalecimiento de la cultura de ciberseguridad en la Universidad Nacional Abierta y a Distancia – UNAD.

[1] https://datos.semillerocerosyunos.online/Analisis_Encuestas.html

Lo Que Nos Cuentan los Datos

Autores

Luis Fernando Zambrano Hernandez
Líder CSIRT Académico UNAD
Universidad Nacional Abierta y a Distancia
ORCID: 0000-0002-4690-3526

Javier Santiago García Sarmiento
Estudiante Ingeniería de Sistemas
Universidad Nacional Abierta y a Distancia
ORCID: 0000-0002-1667-3432

Nataly Guzmán Sáenz
Estudiante Ingeniería Multimedia
Universidad Nacional Abierta y a Distancia

Luna María Valentina Castillo Pineda
Estudiante Comunicación Social
Universidad Nacional Abierta y a Distancia

Yon Garzón Ávila
Docente de apoyo Evaluación del Aprendizaje
Universidad Nacional Abierta y a Distancia
ORCID: 0000-0003-0689-5821

Delito informático presentado con mayor frecuencia en términos de meses.

Según los registros oficiales publicados en el portal de datos abiertos del Gobierno Nacional (Datos, 2024). Se observa una tendencia ascendente sostenida en la cantidad de incidentes, especialmente a partir del año 2020, lo cual coincide con el incremento del uso de servicios digitales y la consolidación del trabajo y la educación remota tras la pandemia. Este aumento progresivo subraya la urgencia de fortalecer los mecanismos de prevención, respuesta y gestión de incidentes de ciberseguridad en las instituciones académicas y en el sector público y privado en general.

La Ley 1273 de 2009 (Congreso, 2009), marca un hito en la legislación colombiana, pues reconoce los delitos informáticos como una modalidad criminal diferenciada, tipificando conductas como el acceso abusivo a sistemas informáticos, la interceptación de datos informáticos, daño informático, uso de software malicioso, violación de datos personales, y suplantación de sitios web para capturar datos personales, entre otros. Esta ley no solo amplía el espectro de protección jurídica, sino que también impone la responsabilidad a las organizaciones de implementar políticas y procedimientos orientados a la

protección de la información y la infraestructura tecnológica.

Al relacionar la gráfica con el marco legal, se destaca que el crecimiento de los incidentes no es solamente un fenómeno estadístico, sino una señal de alerta que pone de manifiesto la sofisticación de las técnicas delictivas y la necesidad de evolucionar en las capacidades institucionales de prevención y respuesta

De acuerdo con los datos, los delitos más reportados corresponden a la técnica de Phising – Articulo 269I. Esta base de datos está compuesta por 7 columnas originalmente, donde se encuentra desde la fecha y hora del delito hasta el tipo de articulo infringido y la descripción de la conducta. También cuenta con el departamento y el municipio y por último la cantidad. En el momento que se realizó el análisis contaba con registros desde el 13 de mayo 2006 hasta septiembre 30 del 2024

Figura 1.
Total de delitos informáticos presentados por mes

Fuente. https://datos.semillerocerosyunos.online/Analisis_Delitos.html

Técnica de ataque de Pishing: El delito informático con mayor tasa de frecuencia es: Hurto por medio informático o semejantes, amparado por el articulo 269I de la ley 1273 del año 2009. Desde el día 13 de mayo del año 2006 hasta el día 13 de septiembre del año 2024, cuenta con un total de 179857 casos relacionados en la base de datos (Delitos informáticos), obtenida de los datos abiertos Colombia. Como dato curioso, en el año 2006, se registraron dos (2)

delitos informáticos, y uno de ellos, infringía el articulo 269I.

Año y mes con mayor frecuencia: Por otro lado, el mes con mayor frecuencia de este delito es: Julio con un total de 16457 casos, no obstante, el mes de mayo no se queda atrás con un total de 16180 casos. El año con mayor cantidad de hurtos por medios informáticos o semejantes es: 2023 con una tasa de 31095 casos, no obstante, el 2024 esta cerca de alcanzarlo, este año cuenta con 30399 casos registrados.

Capturas Policía Nacional: Por supuesto que este delito, cuenta con la mayor tasa de individuos capturados por la Policía Nacional por delitos informáticos, con un total de 1007 capturados, este valor es equivalente al 54% del total, en el periodo de tiempo registrado en la base de datos (Capturas Policía Nacional), tomada de datos abiertos, este periodo es de 5 años, desde Enero del 2010 hasta diciembre del 2015, de estos 1007 privados de la libertad, 761 son de género masculino y 226 de género femenino. Este delito se ubica en el top 1 de delitos informáticos por municipios, en Bogotá tiene un total de 54647 casos y en Medellín 13615.

Tasa de delitos informáticos por cada 10.000 personas por departamento en Colombia

El siguiente gráfico de dispersión muestra la relación entre el número total de delitos informáticos reportados por departamento y la tasa ajustada por cada 10.000 habitantes, con una línea de tendencia (regresión) que ayuda a visualizar la correlación entre ambas variables. El coeficiente de correlación de 0,79 indica una alta relación positiva: los departamentos con más población tienden a registrar mayor número de delitos informáticos tanto en cifras absolutas como en tasa ajustada, aunque existen excepciones notables.

Figure 2.
Tasa de delitos informáticos por departamento

Fuente. https://datos.semillerocerosyunos.online/Analisis_Delitos.html

En el costado derecho, se presenta una tabla con el número de delitos informáticos reportados y una estimación de la población por departamento. Bogotá D.C., Antioquia y Valle del Cauca lideran tanto en cantidad absoluta de delitos como en población, pero el uso de tasas permite identificar departamentos que, aun con menor población, pueden tener una incidencia proporcionalmente significativa de delitos informáticos.

Frecuencia delictiva con relación a los artículos planteados en la ley 1273 de 2009

El artículo 269I (Acceso abusivo a un sistema informático) es, con diferencia, el más infringido, acumulando 179,857 casos y representando cerca de la mitad de todos los delitos informáticos reportados (47,64% según el gráfico circular).

Figura 3.

Frecuencia delictiva con relación a la ley 1273 de2009

Fuente. https://datos.semillerocerosyunos.online/Analisis_Capturas.html

Esto evidencia que los ataques que buscan el acceso no autorizado a sistemas informáticos ya sea para exfiltrar información, controlar sistemas o causar daños constituyen la principal amenaza en el ecosistema digital colombiano. Le siguen, aunque a distancia, el artículo 269F (Violación de datos personales) con 66,151 registros (17,52%) y el artículo 269A (Daño informático) con 64,981 registros (17,21%). La alta frecuencia de estos delitos resalta la importancia de proteger la integridad y confidencialidad de la información personal y corporativa, así como la necesidad de robustecer las políticas de privacidad, la gestión de datos y los controles de acceso. Otros delitos relevantes incluyen hurto por medios informáticos (artículo 269G), interceptación de datos informáticos (artículo 269C) y el uso de software malicioso (artículo 269E), aunque su incidencia es menor en términos absolutos. La baja frecuencia de artículos como la suplantación de sitios web y la

obstrucción ilegítima de sistemas no debe subestimarse, pues muchas veces corresponden a técnicas sofisticadas o subreportadas, pero pueden tener un impacto severo en instituciones y ciudadanos.

Delitos informáticos reportados en datos abiertos por año (2006 - 2024) - Análisis de la tendencia temporal

El primer dato relevante es el crecimiento sostenido y acelerado en la cantidad de delitos informáticos reportados anualmente. Entre 2006 y 2015, las cifras muestran incrementos progresivos, pero relativamente bajos (de solo 2 casos en 2006 a 8.651 en 2015). A partir de 2016, la tendencia se vuelve ascendente de forma marcada, con incrementos anuales que superan los 10.000 casos, hasta alcanzar cifras superiores a los 60.000 delitos informáticos reportados por año a partir de 2021. En total, se registra una suma acumulada de 377.573 incidentes en el periodo 2006-2024.

Figura 4.
Delitos informáticos realizados por año

Fuente. https://datos.semillerocerosyunos.online/Analisis_Capturas.html

Especialmente llamativo es el salto observado en los años 2019-2021, cuando los delitos informáticos casi se triplican en un corto periodo de tiempo (de 21.279 en 2019 a 49.959 en 2020 y 52.224 en 2021). Esta aceleración coincide con la masificación de los servicios digitales, el crecimiento del comercio electrónico, el auge del teletrabajo y la educación virtual, impulsados por la pandemia de COVID-19.

Factores explicativos y contexto normativo

Este comportamiento está alineado con la evolución global del cibercrimen, tal como lo reportan entidades internacionales y académicas. El crecimiento de la digitalización, junto con la sofisticación de los atacantes, genera mayores oportunidades para la comisión de delitos informáticos. Por otra parte, la Ley 1273 de 2009 contribuyó significativamente a la visibilización y judicialización de estos delitos, pues brindó el marco legal necesario para que las víctimas y las autoridades reconocieran, reportaran y procesaran los incidentes de manera formal.

Los años recientes muestran una cierta estabilización en la curva (alrededor de 62.000 casos anuales), lo que puede deberse tanto a una madurez en los mecanismos de denuncia y detección, como a cambios en las estrategias de prevención, inversión en ciberseguridad, y mayor conciencia pública. Sin embargo, estas cifras siguen siendo preocupantes y reflejan que los riesgos y amenazas evolucionan constantemente.

Implicaciones para la gestión institucional y la política pública

Para entidades como la UNAD y su CSIRT académico, esta tendencia subraya la urgencia de fortalecer las capacidades de prevención, detección y respuesta a incidentes. La educación en buenas prácticas de seguridad, la actualización tecnológica, la vigilancia proactiva y la colaboración con organismos estatales y privados son fundamentales para contener la expansión del delito informático.

Capturas policiales por delitos informáticos en Colombia has el año 2015

La siguiente imagen expone que, hasta 2015, se registraron 1864 capturas relacionadas con delitos informáticos (abiertos, 2024), predominando claramente el artículo 269I (acceso abusivo a un sistema informático), con 1007 capturas, es decir, más del 54% del total. Le siguen el artículo 269A (daño informático) y el artículo 269G (hurto por medios informáticos y semejantes). Este patrón evidencia que las conductas más perseguidas y judicializadas están vinculadas a accesos no autorizados, manipulación y hurto de información, aspectos centrales de la Ley 1273. Así mismo, el predominio del artículo 269I refleja tanto la frecuencia de ataques de acceso abusivo como la capacidad de las autoridades para detectar y judicializar este tipo de conductas, lo cual puede asociarse a la clara definición del delito y a la mayor facilidad probatoria en comparación con otros delitos informáticos más

sofisticados, como el uso de software malicioso o la suplantación de sitios web, que presentan menos capturas.

Figura 5.
índice de capturas policiales por delitos informáticos

Fuente. https://datos.semillerocerosyunos.online/Analisis_Capturas.html

En cuanto a la distribución de género, se observa que el 79,9% de las capturas corresponden a hombres y solo el 20,01% a mujeres. Esto coincide con estudios globales sobre ciberdelincuencia, donde la brecha de género en la participación en este tipo de delitos sigue siendo considerable (EIGE, 2022).

El panel de descripción de conductas muestra la variedad de tipologías criminales abordadas por la ley, entre ellas la interceptación de datos, la obstrucción ilegítima de sistemas, la suplantación para captura de datos personales, el uso de software malicioso, y la transferencia no consentida de activos. Todas estas conductas están alineadas con la modernización del marco penal colombiano tras la promulgación de la Ley 1273, que adecuó el Código Penal a las exigencias de la economía digital y la protección de la información.

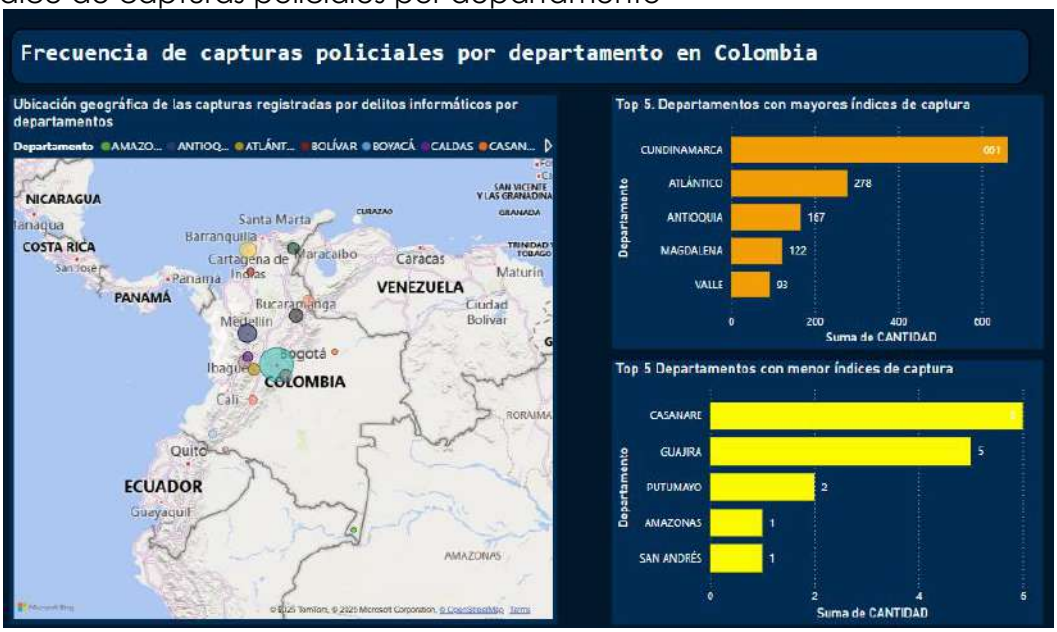
Frecuencia de capturas policiales por departamento

Foco Urbano y Zonas Vulnerables sin Vigilancia

La distribución de capturas relacionadas con delitos informáticos en Colombia muestra un sesgo significativo hacia las zonas urbanas, especialmente en ciudades grandes como Bogotá y Medellín. Con el 80% de las capturas concentradas en estos

centros, los departamentos menos poblados y con menor infraestructura quedan casi desprotegidos. Esto evidencia una clara brecha de recursos policiales y judiciales en la aplicación de la ley contra delitos digitales, lo que permite a los infractores operar con relativa impunidad en áreas rurales y menos desarrolladas. Para una respuesta eficaz, sería esencial fortalecer la ciberseguridad a nivel regional y mejorar la capacidad de respuesta policial en zonas periféricas.

Figura 6.
índice de capturas policiales por departamento



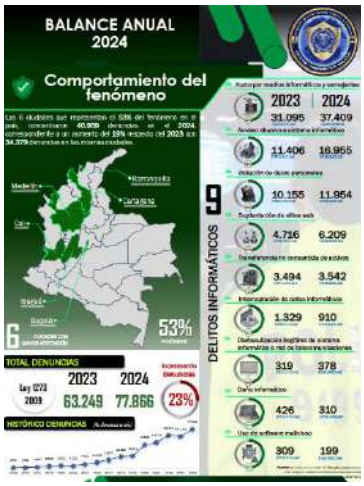
Fuente. https://datos.semillerocerosyunos.online/Analisis_Capturas.html

La marcada concentración de capturas en los departamentos de Cundinamarca (661), Atlántico (278), Antioquia (167), Magdalena (122) y Valle (93), indica que estas regiones no solo concentran mayores índices de denuncia y judicialización, sino probablemente también presentan una infraestructura tecnológica más desarrollada, un mayor volumen de transacciones digitales y una densidad poblacional significativa. Estos factores, en conjunto, elevan la exposición y el riesgo frente a los delitos informáticos. Esta concentración en los grandes centros urbanos y departamentos más poblados puede explicarse, además, por la mayor capacidad institucional de las autoridades en estas regiones, la existencia de equipos especializados en delitos informáticos y una mayor cultura de denuncia por parte de la ciudadanía y las empresas. No es casualidad que Cundinamarca, que incluye a Bogotá el epicentro económico, administrativo y tecnológico del país, lidere ampliamente el número de capturas.

Por otro lado, los departamentos con menor índice de capturas, como Casanare (6), Guajira (5), Putumayo (2), Amazonas (1) y San Andrés (1), reflejan realidades distintas: menor densidad poblacional, posibles brechas de acceso a la tecnología, limitaciones en la capacidad de las autoridades locales para investigar y judicializar delitos informáticos, y quizá una subrepresentación de incidentes debido a la baja cultura de denuncia o desconocimiento de los canales institucionales.

Este contraste territorial evidencia desafíos estructurales en la aplicación de la Ley 1273 de 2009, la cual, si bien ofrece un marco jurídico robusto para la persecución penal de los delitos informáticos, requiere del fortalecimiento de capacidades técnicas y humanas en los departamentos con menor índice de captura, así como de campañas de sensibilización sobre la importancia de denunciar y tratar adecuadamente los incidentes de ciberseguridad

Los Que Nos Muestra el CAI virtual al año 2024



El informe presenta el comportamiento, modalidades, operaciones relevantes y resultados estratégicos de la lucha contra los delitos informáticos en Colombia durante el año 2024. Se destaca un aumento del 23% en denuncias por delitos informáticos respecto a 2023, reflejando tanto el incremento del uso de tecnologías de la información como la sofisticación y expansión de las conductas ciberdelictivas.[2]

Figura 7.
Balance anual 2024 - CAI Virtual

Comportamiento del fenómeno

- Las principales ciudades afectadas (Bogotá, Medellín, Cali, Barranquilla, Ibagué, Cartagena) concentraron el 53% de las denuncias nacionales, alcanzando 40.969 casos en 2024 (un 19% más que en 2023).
- El hurto por medios informáticos fue la conducta más denunciada (31.095 casos, 20%), seguido de acceso abusivo a sistemas informáticos (11.406), violación de datos personales (10.155), suplantación de sitios web (4.716) y transferencia no consentida de activos (3.494).

[2] https://caivirtual.policia.gov.co/sites/default/files/observatorio/BALANCE%20ANUAL%20CECIP%202024.pdf

- Otras conductas incluyeron interceptación de datos, daño informático, uso de software malicioso y obstaculización ilegítima de sistemas.

Modalidades emergentes y tendencias

- Se identificaron nuevas modalidades como el robo de cuentas de WhatsApp, donde los atacantes emplean ingeniería social y técnicas de suplantación para acceder a cuentas y cometer fraudes.
- Destaca el uso creciente de inteligencia artificial para la comisión de delitos, especialmente mediante técnicas de deepfake (manipulación de imágenes y videos), deep voice (suplantación de voz), y automatización de ataques.
- El informe explica cómo funcionan estas técnicas y alerta sobre los desafíos que representan para la ciberseguridad y la credibilidad ciudadana.

Operaciones relevantes

- Se desarrollaron operaciones nacionales e internacionales exitosas en colaboración con INTERPOL, EUROPOL y otras agencias, desarticulando redes criminales vinculadas a fraude con criptoactivos, hackeo remoto, distribución de software malicioso y explotación sexual infantil.
- Ejemplos destacados incluyen las operaciones "CriptoEspaña – CanMoney", "Iserver", "Reserve", "Los CriptoCitas", "Hacker Remoto", "Fénix" y "Skype", que involucraron capturas, incautaciones de bienes y bloqueos de plataformas.

Resultados estratégicos

- Se fortaleció la articulación entre entidades del Estado y organismos internacionales para la gestión de incidentes, intercambio de información y generación de alertas de ciberseguridad.
- Se llevaron a cabo 144 charlas de prevención y concienciación en instituciones educativas, impactando a más de 13.000 personas, y se publicaron 12 boletines estratégicos y 10 análisis de vulnerabilidades.
- Hubo un crecimiento significativo en el alcance en redes sociales y en la gestión de alertas preventivas (424 emitidas en el año).
- El CAI Virtual y el Centro Cibernético Policial consolidaron su rol como ejes centrales en la prevención, atención y judicialización de los delitos informáticos en Colombia.

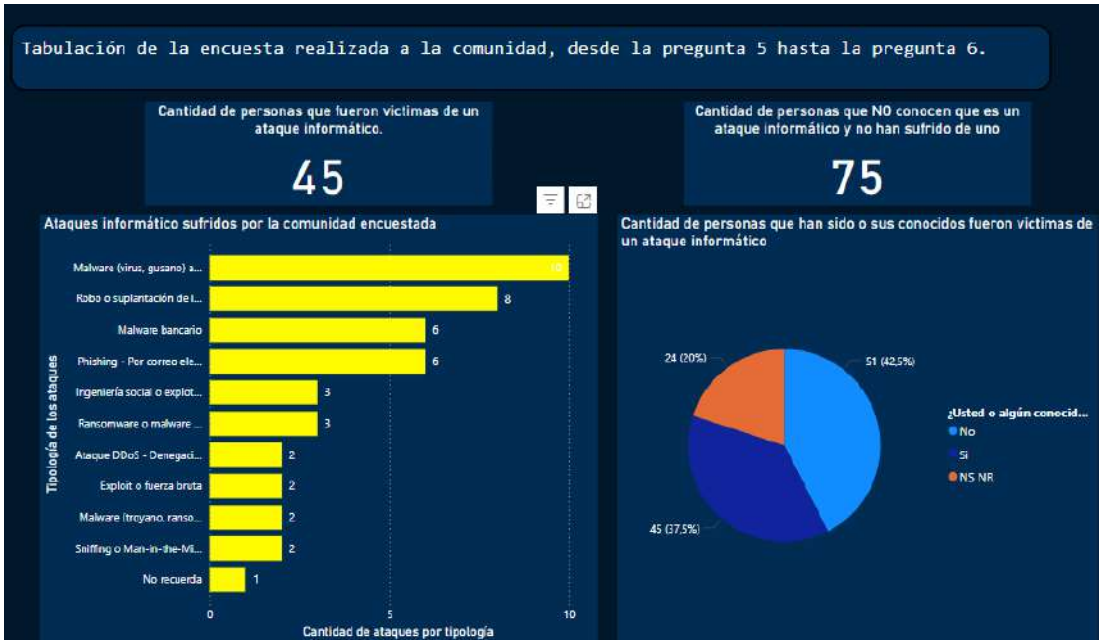
Estadísticas clave

- 77.866 denuncias por delitos informáticos en 2024 (en comparación con 63.249 en 2023).
- 11.866 incidentes atendidos y 424 alertas preventivas emitidas.
- 362 capturas relacionadas con delitos informáticos y abuso sexual infantil.
- 30.165 páginas bloqueadas en articulación con la Estrategia Integral de Ciberseguridad.

¿Como se Refleja en Nuestra Comunidad UNADISTA?

Una encuesta aplicada a 120 usuarios pertenecientes a la comunidad UNADISTA y partes interesadas, permite identificar que el phishing y el hurto por medio informáticos o semejantes ocupa el puesto número 4 con una tasa de 6 casos de 45. (ver la siguiente imagen).

Figura 7.
Estadística relacionada con encuesta aplicada a la comunidad UNADISTA respecto a conocimientos en ciberseguridad[3]



Fuente. http://datos.semillerocerosyunos.online/Analisis_Encuestas.html

[3] http://datos.semillerocerosyunos.online/Analisis_Encuestas.html

Experiencia directa de ataques manifestadas en el levantamiento de la información

- 45 personas de la muestra reportaron haber sido víctimas de algún tipo de ataque informático.
- Las tipologías más frecuentes fueron:

Malware (virus, gusano, etc.): 10 casos (la amenaza más común, en línea con la tendencia mundial, donde el malware sigue siendo el principal vector de ataque tanto en hogares como en organizaciones).

Robo o suplantación de identidad: 8 casos (destaca la relevancia de la protección de datos personales y credenciales, y la necesidad de educación en prevención del phishing y buenas prácticas en redes sociales).

Malware bancario y phishing: 6 casos, cada uno (el cibercrimen financiero y el fraude por correo electrónico son riesgos persistentes y cada vez más sofisticados).

Otros ataques: (ingeniería social, ransomware, DDoS, fuerza bruta, sniffing, etc.) muestran incidencia menor pero reflejan la diversidad de amenazas presentes en el entorno digital.

Percepción y cultura de ciberseguridad

75 personas no conocen qué es un ataque informático y reportan no haber sido víctimas de uno. Esto evidencia desinformación o baja percepción del riesgo en una parte importante de la muestra, lo que constituye un área crítica de mejora para las campañas de sensibilización y formación.

El gráfico circular indica que:

- 51 personas (42,5%) afirman que ni ellas ni sus conocidos han sido víctimas de ataques,
- 45 (37,5%) sí han experimentado incidentes directos o a través de conocidos,
- 24 (20%) no saben o no recuerdan, mostrando un nivel de desconocimiento relevante.
- Implicaciones y recomendaciones

La combinación de personas que no reconocen los ataques, que no han sido víctimas o que no recuerdan, es preocupante. En la ciberseguridad, la percepción del riesgo es tan importante como la capacidad técnica, y estos resultados sugieren que aún existe una "zona ciega" significativa en la comunidad. En este sentido , resultados como los anteriormente expuestos respaldan la necesidad de programas permanentes de capacitación y simulación, que expliquen los diferentes vectores de ataque y refuercen el reconocimiento de señales de alerta, tanto en lo personal como institucional.

Conclusiones

El fenómeno de los delitos informáticos en Colombia presenta un crecimiento sostenido y una diversificación constante en sus modalidades, impulsado por el avance tecnológico y la masificación del uso de servicios digitales. La evidencia estadística y documental muestra incrementos anuales significativos en denuncias e incidentes, así como una ampliación de los métodos utilizados por los ciberdelincuentes, que ahora incluyen técnicas avanzadas basadas en inteligencia artificial, deepfake, robo de identidad y fraudes financieros a través de criptoactivos. Este contexto plantea desafíos cada vez más complejos para las autoridades, las instituciones y los ciudadanos.

La respuesta institucional ha avanzado en materia de prevención, atención y judicialización, pero persisten brechas importantes en la cultura de ciberseguridad y la capacidad de adaptación ante amenazas emergentes.
Si bien la creación y fortalecimiento de organismos como el Centro Cibernético Policial, el CAI Virtual y los CSIRT han permitido articular acciones, incrementar las operaciones relevantes y mejorar la gestión de incidentes, la información revela que la falta de conocimiento, la baja percepción del riesgo y la subcultura de reporte siguen siendo obstáculos clave. El éxito de la gestión institucional dependerá de su capacidad para integrar la educación, la sensibilización y la cooperación multisectorial en todos los niveles.

El enfoque territorial, la articulación internacional y el uso de marcos normativos sólidos como la Ley 1273 de 2009 y estándares internacionales (ISO, NIST, OWASP) son esenciales para construir una resiliencia digital sostenible.
Las disparidades regionales en la incidencia y denuncia de delitos informáticos, así como la evolución de las amenazas a nivel global, evidencian la necesidad de estrategias diferenciadas, adaptativas y coordinadas, donde la academia, los entes estatales y el sector privado trabajen conjuntamente. Sólo a través de un esfuerzo integral y sostenido será posible reducir la vulnerabilidad, fortalecer la capacidad de respuesta y proteger de manera efectiva los derechos y la información de la ciudadanía en el entorno digital.

Bibliografía

abiertos, D. (2024). *Datos abiertos.* Obtenido de Reportes capturas policia nacional: https://www.datos.gov.co/Seguridad-y-Defensa/Reporte-Capturas-Polic-a-Nacional/3jdh-nmwu/about_data

Congreso. (2009). *Función publica.* Obtenido de Ley 1273 de 2009: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34492

Datos. (2024). *DELITOS INFORMÁTICOS.* Obtenido de datos.gov.co: https://www.datos.gov.co/Seguridad-y-Defensa/DELITOS-INFORM-TICOS/4v6r-wu98/about_data

EIGE. (2022). *European Institute for Gender Equality.* Obtenido de https://eige.europa.eu/sites/default/files/documents/combating_cyber_violence_against_women_and_girls.pdf

Contactenos

📧 **Correo electrónico:** csirt@unad.edu.co
🌐 **Página web:** https://csirt.unad.edu.co

🛡️ El CSIRT Académico UNAD está siempre disponible para apoyarte ante consultas o inquietudes relacionadas con la protección de la información en la universidad. No dudes en ponerte en contacto con nuestro equipo para recibir asesoría, reportar incidentes o recibir orientación en temas de seguridad digital. ¡Tu seguridad es nuestra prioridad!