Un Análisis de Incidentes de Ransomware y Ciberataques que Afectan a Empresas Privadas en 2025

I. Resumen Ejecutivo

El sector privado de la República Dominicana se encuentra en un entorno de amenazas cibernéticas cada vez más complejo y hostil en 2025. El ransomware se ha consolidado como una preocupación dominante y en constante evolución. Aunque las divulgaciones públicas detalladas de víctimas específicas en los medios locales son limitadas, un análisis de la inteligencia especializada en ciberseguridad confirma varios incidentes significativos que han afectado a entidades privadas a lo largo de 2025 y finales de 2024. Estos ataques, en su conjunto, ponen de manifiesto vulnerabilidades críticas derivadas de una rápida aceleración digital, persistentes brechas de talento en ciberseguridad y un enfoque predominantemente reactivo en las inversiones en seguridad. A pesar del compromiso proactivo del gobierno en iniciativas nacionales e internacionales para reforzar la resiliencia cibernética, persiste una brecha sustancial en la preparación general y las capacidades defensivas del sector privado.

La naturaleza de los ataques de ransomware ha trascendido la mera encriptación de datos para abarcar tácticas sofisticadas como la exfiltración de información para extorsión pública, ataques de denegación de servicio distribuido (DDoS) e incluso la posibilidad de envenenamiento de datos. La adopción generalizada del modelo "Ransomware-as-a-Service" (RaaS) está reduciendo significativamente la barrera técnica para los ciberdelincuentes, lo que contribuye directamente a un aumento en la frecuencia y el alcance de los ataques, siendo las Pequeñas y Medianas Empresas (PyMEs) objetivos particularmente vulnerables. Si bien la colaboración público-privada es cada vez más reconocida y buscada a nivel estratégico, su implementación práctica y la adopción generalizada de prácticas de ciberseguridad sólidas en los diversos sectores privados de la República Dominicana aún se encuentran en etapas incipientes.

La creciente oleada de ciberataques sofisticados plantea profundos riesgos financieros, operativos y reputacionales para las empresas privadas. Esta amenaza, si no se controla, tiene el potencial de obstaculizar el crecimiento económico, desalentar la inversión extranjera directa y erosionar la confianza internacional en el ecosistema digital de la República Dominicana. Una observación importante es la

marcada diferencia entre la información disponible en los informes públicos y los incidentes reales. Aunque los artículos de noticias locales discuten sectores generalmente afectados (como el gobierno, bancos y telecomunicaciones), rara vez proporcionan nombres específicos de empresas privadas que han sido víctimas en 2025.[1] Sin embargo, al examinar plataformas especializadas de seguimiento de ciberseguridad, se revelan múltiples entidades privadas afectadas. Esta disparidad sugiere que la prevalencia real y la escala de los ciberataques que impactan a las empresas privadas en la República Dominicana son probablemente subestimadas si se confía únicamente en los informes de noticias generales. Esta falta de transparencia puede generar una falsa sensación de seguridad entre las empresas y obstaculizar su motivación para invertir adecuadamente en ciberseguridad, además de señalar una posible deficiencia sistémica en los mecanismos de reporte de incidentes, que son cruciales para la defensa colectiva y una evaluación precisa del riesgo.

II. El Paisaje Evolutivo de Amenazas Cibernéticas en la República Dominicana (2025)

Tendencias Generales y Predicciones

La República Dominicana se encuentra inmersa en un entorno de amenazas digitales globales cada vez más intenso. El panorama general de la ciberseguridad para 2025 se proyecta como aún más complejo y desafiante, lo que subraya una tendencia continua al alza en la actividad cibercriminal.[2] Dentro de este contexto, el ransomware se perfila inequívocamente como el "gran protagonista" entre las amenazas de ciberseguridad en 2025. Los expertos anticipan su evolución con técnicas más sofisticadas, resistentes y menos descifrables, lo que aumenta la probabilidad de ataques exitosos.[3] A nivel global, el volumen de ciberataques ha experimentado un aumento significativo, con el informe de Check Point de 2025 indicando un incremento del 44% en los ciberataques generales en todo el mundo.[4] Estas tendencias globales sirven como un fuerte indicador de las crecientes presiones y amenazas que enfrenta la República Dominicana.

Estadísticas Generales y Volumen de Ataques

Los datos históricos proporcionan una línea de base crucial, ilustrando un volumen persistentemente alto de actividad cibernética. Entre junio de 2022 y julio de 2023, la República Dominicana sufrió una alarmante cifra de 7.6 ataques de malware por minuto, junto con 962 incidentes de ransomware y 2.2 millones de ataques de phishing.[2] Aunque estas cifras son anteriores a 2025, establecen un contexto de amenazas cibernéticas intensas y omnipresentes. Reforzando esta tendencia, Kaspersky informó haber bloqueado más de 5,000 intentos de ataques de ransomware específicamente dentro de la República Dominicana en el año anterior (implícitamente 2024), como parte de un total de 1.185 millones de intentos en toda América Latina.[3] Estos datos subrayan el volumen sostenido y elevado de ransomware dirigido al país, independientemente de la penetración exitosa o la divulgación pública.

Reconocimiento Gubernamental y Respuesta Estratégica

El gobierno dominicano ha demostrado un claro reconocimiento de la urgencia de la creciente amenaza cibernética. El Centro Nacional de Ciberseguridad (CNCS) está activamente involucrado en un enfoque multifacético para fortalecer el ecosistema cibernético nacional.[5] Un movimiento estratégico significativo en mayo de 2025 fue la firma de un acuerdo de cooperación entre la República Dominicana y los Emiratos Árabes Unidos en el evento GISEC Global 2025. Este acuerdo tiene como objetivo mejorar las capacidades nacionales de ciberseguridad, con un enfoque en la detección temprana de amenazas y la protección de sectores económicos estratégicos.[5] Esto significa un compromiso estratégico proactivo y de alto nivel para mejorar la resiliencia cibernética. El país también está fomentando activamente su papel como centro regional para el diálogo y el desarrollo de políticas de ciberseguridad, como lo destacó el evento "Digital Shield 2025".[7] Este liderazgo regional indica un compromiso con la seguridad colectiva.

A pesar de estos encomiables esfuerzos gubernamentales e iniciativas estratégicas, el sentimiento predominante entre los expertos en ciberseguridad a marzo de 2025 era que "aún queda mucho por hacer" para fortalecer adecuadamente la postura general de ciberseguridad del país.[1] Esto sugiere un reconocimiento de los desafíos significativos que aún quedan por delante para traducir la política en mejoras prácticas generalizadas. Existe una observación importante: la República Dominicana, a pesar de sus esfuerzos gubernamentales considerables y colaboraciones internacionales para abordar la ciberseguridad [5], enfrenta una madurez cibernética persistentemente baja, particularmente en el sector privado. Las proyecciones indican que para 2026, solo el 10% de las grandes empresas tendrán programas avanzados de ciberseguridad, en contraste con menos del 1% actual.[2] Esta situación revela una desconexión crítica: aunque la intención estratégica y la acción gubernamental son fuertes, la implementación práctica y la mejora generalizada en todo el ecosistema digital, especialmente dentro del diverso sector privado, están rezagadas. Esta situación resalta la necesidad de que los esfuerzos estratégicos se traduzcan en mejoras tangibles, accesibles y aplicables para las empresas privadas, posiblemente a través de incentivos específicos, marcos de cumplimiento simplificados o apoyo directo para el desarrollo de capacidades. La escasez de talento y la brecha de capacitación en ciberseguridad, señaladas en contextos más amplios de América Latina [8], probablemente constituyen barreras significativas para esta traducción dentro de la República Dominicana, limitando la capacidad del sector privado para adoptar e implementar prácticas de seguridad avanzadas.

III. Empresas Privadas Identificadas como Víctimas de Ransomware y Ciberataques en 2025

Desafíos en la Divulgación Pública

Es crucial señalar que los informes específicos y ampliamente publicitados que nombran a empresas privadas víctimas en la República Dominicana para 2025 son notablemente escasos en los medios de comunicación tradicionales.[1] Esta falta de divulgación pública puede ocultar la verdadera magnitud del problema. Sin embargo, las plataformas especializadas de seguimiento de ciberseguridad y los informes detallados proporcionan datos más granulares y procesables.

Víctimas Confirmadas del Sector Privado (2025)

Varias empresas privadas en la República Dominicana han sido identificadas como víctimas de ransomware o ciberataques en 2025.

- **INICIA Ltd:** Esta entidad fue descubierta como víctima el 8 de julio de 2025, con el ataque atribuido al grupo Direwolf.[10] INICIA está confirmada como una firma privada de gestión de activos [12], con una larga trayectoria en emprendimiento y creación de valor, y participación en diversos sectores, incluyendo productos y servicios avícolas.[12]
- **SJERP:** Descubierta como comprometida el 29 de abril de 2025, el ataque a SJERP fue llevado a cabo por el actor de amenazas Nova.[10] SJERP se describe explícitamente como un proveedor de un sistema integral de Planificación de Recursos Empresariales (ERP), que atiende principalmente a Pequeñas y Medianas Empresas (PyMEs) en la República Dominicana y América Latina.[14] Esto confirma su estatus privado y destaca la focalización en proveedores de servicios empresariales.
- **Cormidom (Corporación Minera Dominicana):** Esta empresa minera privada fue descubierta como víctima el 25 de marzo de 2025, con una fecha estimada de ataque del 18 de marzo de 2025, y el incidente fue atribuido al grupo Ransomhub.[10] Cormidom opera la mina Cerro de Maimón, centrándose en la extracción de concentrados de cobre y zinc.[17] El ataque resultó en una fuga sustancial de 381 GB de datos [15], lo que indica una exfiltración significativa de información.
- **Cana Group Corp:** Esta entidad fue descubierta como víctima el 20 de enero de 2025, con el ataque atribuido al grupo Sarcoma.[10] Cana Group Corp opera en

varios sectores, incluyendo agricultura, ganadería, agroindustria, pesca, madera y tabaco.[19] Sus marcas, como Cana, Guidom y Fresh Cana, sirven al público consumidor en general [10], lo que confirma su participación en el sector privado.

- **PCM (Proveedora de Consumibles de Papel y Empaques):** Esta empresa privada fue específicamente identificada como atacada en enero de 2025 por el grupo Ransom Hop.[20] La brecha fue de alto impacto, lo que llevó a la fuga de más de 3 GB de información sensible, incluyendo contratos críticos y datos de clientes de grandes corporaciones como Coca-Cola, Bimbo y Walmart.[20] Este incidente sirve como un ejemplo claro y temprano de una empresa privada victimizada por ransomware en 2025.

Casos Relevantes del Sector Público/Ambiguos (2025)

Algunas entidades públicas o de estatus ambiguo también fueron afectadas en 2025, lo que subraya la amplitud de los objetivos de los ciberdelincuentes.

- **Instituto Nacional de Recursos Hidráulicos (INDRHI):** Descubierto como víctima el 14 de julio de 2025.[10] Confirmado como una entidad de la administración pública y una institución gubernamental descentralizada.[21]
- **Fondo Patrimonial de las Empresas Reformadas (FONPER):** Descubierto como comprometido el 25 de junio de 2025, con el ataque atribuido a Incransom.[10] Esta entidad está confirmada como una institución del Estado dominicano.[10]
- **Edesur Dominicana:** Descubierta como afectada el 11 de marzo de 2025, con el ataque llevado a cabo por Hunters, notablemente involucrando la exfiltración de datos pero sin cifrado.[10] Esta entidad está inequívocamente confirmada como una empresa estatal de distribución de electricidad.[24] Aunque es pública, su inclusión destaca la focalización en infraestructuras críticas, un sector que con frecuencia involucra asociaciones y operadores del sector privado.[25]

Víctimas Confirmadas del Sector Privado (Finales de 2024 - para análisis de tendencias y contexto)

Para comprender mejor las tendencias, se incluyen incidentes de finales de 2024.

- **Ramon Corripio:** Descubierta como víctima el 30 de agosto de 2024, con una fecha estimada de ataque del 21 de agosto de 2024, y atribuida al grupo Ransomhub.[10] Ramon Corripio es una parte integral del Grupo Corripio privado, un conglomerado altamente diversificado con intereses significativos en varios sectores, incluyendo ferretería, materiales de construcción y artículos para el hogar.[26] El ataque resultó en una fuga de datos de 124 GB.[26]
- **Boombah Inc.:** Descubierta como comprometida el 9 de agosto de 2024, con una fecha estimada de ataque del 29 de junio de 2024, y atribuida a Incransom.[10] Boombah Inc. está confirmada como una empresa privada especializada en equipos y vestimenta deportiva.[29]
- **Unidad de Oftalmología y Catarata:** Descubierta como víctima el 19 de abril de 2024, con una fecha estimada de ataque del 10 de febrero de 2024, y atribuida al grupo Dispossessor.[10] Esta entidad opera como una empresa privada de atención médica.[31]

La lista de empresas privadas victimizadas en la República Dominicana en 2025 y

finales de 2024 revela una vulnerabilidad significativa en la cadena de suministro. El ataque de ransomware a PCM en enero de 2025 por Ransom Hop [20] es un ejemplo crítico. PCM, como "proveedora de consumibles de papel y empaques", es un eslabón dentro de un ecosistema empresarial más amplio. La consecuencia directa de esta brecha fue la fuga de datos sensibles de clientes importantes como Coca-Cola, Bimbo y Walmart. Esto no es solo un ataque directo a PCM, sino un caso de ataque a la cadena de suministro, donde los ciberdelincuentes explotan la postura de seguridad más débil de un proveedor externo para comprometer indirectamente o recopilar inteligencia sobre objetivos primarios más grandes y potencialmente más seguros. Esta observación se alinea con las predicciones de Kaspersky para 2025, que destacan los ataques a la cadena de suministro como una preocupación predominante en ciberseguridad.[32] Esto implica que las empresas privadas en la República Dominicana, especialmente aquellas que actúan como proveedores o prestadores de servicios a corporaciones más grandes o sectores críticos, representan puntos débiles significativos y a menudo pasados por alto en la cadena de ciberseguridad. Incluso si una gran empresa ha invertido fuertemente en defensas internas robustas, su dependencia de proveedores externos introduce riesgos indirectos sustanciales. Esto exige un cambio fundamental en la estrategia de ciberseguridad, de medidas de seguridad puramente internas a un enfoque más integral de gestión de riesgos de la cadena de suministro, incluyendo la debida diligencia rigurosa, el monitoreo continuo de la postura de seguridad de los proveedores y el establecimiento de obligaciones contractuales claras en materia de ciberseguridad con todos los socios externos.

Además, la diversidad de los sectores afectados en la República Dominicana es notable. Las víctimas identificadas del sector privado (INICIA - gestión de activos/avicultura; SJERP - software ERP; Cormidom - minería; Cana Group Corp - agricultura/bienes de consumo; PCM - papel/embalaje; Ramon Corripio - comercio minorista/distribución; Boombah Inc. - artículos deportivos; Unidad de Oftalmología y Catarata - atención médica) [10] demuestran una estrategia de focalización amplia y oportunista por parte de los ciberdelincuentes. Este patrón va más allá de los sectores tradicionalmente destacados como "infraestructura crítica" o "servicios financieros", abarcando una amplia gama de industrias. Mientras que los informes globales de Check Point [34] y Cyble [35] mencionan TI, agricultura, transporte, servicios profesionales y construcción como sectores frecuentemente atacados, los datos de la República Dominicana muestran que los actores de amenazas están lanzando una red aún más amplia, indicando que cualquier entidad con datos valiosos o sistemas operativos es un objetivo potencial, independientemente de su clasificación industrial

específica. Esto significa que ningún sector privado en la República Dominicana puede permitirse la complacencia con respecto a la ciberseguridad. Los ciberdelincuentes se mueven por la oportunidad y el beneficio económico, y explotarán las vulnerabilidades dondequiera que las encuentren. Esto exige la adopción de un nivel básico universal de higiene y concienciación en ciberseguridad en todas las empresas privadas, no solo en aquellas percibidas tradicionalmente como de alto riesgo. Además, la vulnerabilidad de las PyMEs, como se señala explícitamente en el contexto de la proliferación de Ransomware-as-a-Service [9], significa que las empresas más pequeñas con recursos limitados son particularmente susceptibles y requieren apoyo y orientación adaptados para mejorar sus defensas.

A continuación, se presenta una tabla que resume las empresas privadas en la República Dominicana que han sido víctimas de ransomware o ciberataques en 2025 y finales de 2024.

Tabla 1: Empresas Privadas en la República Dominicana Víctimas de Ransomware/Ciberataques (2025 y Finales de 2024)

Empresa	Fecha de Descubrimiento	Fecha Estimada de Ataque	Actor de Amenaza	Tipo de Ataque	Descripción Breve de la Empresa	Privada?
INICIA Ltd	2025-07-08	2025-07-08	Direwolf	Ransomware	Firma privada de gestión de activos y productos avícolas.	Sí [12]
SJERP	2025-04-29	No proporcionada	Nova	Ransomware	Proveedor de sistemas de Planificación de Recursos Empresariales (ERP) para PyMEs.	Sí [14]
Cormidom (Corporación Minera Dominicana)	2025-03-25	2025-03-18	Ransomhub	Ransomware	Empresa minera que opera la mina Cerro de Maimón (cobre y zinc).	Sí [17]
Cana Group Corp	2025-01-20	No proporcionada	Sarcoma	Ransomware	Opera en agricultura, ganadería, agroindustria, pesca, madera, tabaco.	Sí [19]
PCM (Proveedora de Consumibles de Papel y Empaques)	Enero 2025	No proporcionada	Ransom Hop	Ransomware	Proveedora de consumibles de papel y empaques.	Sí [20]
Ramon Corripio	2024-08-30	2024-08-21	Ransomhub	Ransomware	Parte del Grupo Corripio, mayorista de ferretería, construcción y hogar.	Sí [27]
Boombah Inc.	2024-08-09	2024-06-29	Incransom	Ransomware	Empresa de equipos y vestimenta deportiva.	Sí [29]
Unidad de Oftalmología y Catarata	2024-04-19	2024-02-10	Dispossessor	Ransomware	Empresa privada de atención médica oftalmológica.	Sí [31]

Nota: Se excluyen entidades públicas como INDRHI, FONPER y Edesur Dominicana, aunque fueron afectadas, para mantener el enfoque en el sector privado según la consulta original. Edesur Dominicana, aunque sufrió una exfiltración de datos, no

experimentó cifrado.[10]

IV. Análisis de Vectores de Ataque Clave y Tendencias de Ransomware

Tácticas Evolutivas del Ransomware (Global y Regional)

El ransomware en 2025 no es estático; se caracteriza por el despliegue de técnicas cada vez más sofisticadas, resistentes y menos descifrables, lo que mejora significativamente la probabilidad de ataques exitosos.[3] Una evolución crítica es el objetivo principal de los actores de ransomware, que ha pasado de simplemente cifrar datos a una extorsión multifacética. Esto a menudo implica la exposición pública de las víctimas, la exfiltración de datos sensibles y las amenazas de su divulgación pública si no se paga un rescate.[9] Esta táctica de "doble extorsión", e incluso la "triple extorsión" (que puede incluir ataques de denegación de servicio distribuido y presión directa sobre los clientes o proveedores de la víctima), aumenta drásticamente la presión sobre las organizaciones comprometidas.[9]

Las tendencias emergentes de ransomware para 2025, anticipadas por expertos como Kaspersky, incluyen:

- **Envenenamiento de Datos:** Una tendencia particularmente insidiosa donde los atacantes, más allá de simplemente bloquear el acceso, pueden alterar intencionalmente o inyectar datos incorrectos en los sistemas de una víctima. Esto hace que la información recuperada no sea confiable y puede socavar gravemente la integridad y la confianza de los datos, incluso si finalmente se restauran.[3]
- **Cifrado Resistente a la Cuántica:** Se anticipan avances en las técnicas de cifrado, que potencialmente aprovecharán métodos "resistentes a la cuántica", lo que hará que el descifrado de datos cifrados sea significativamente más desafiante tanto para los sistemas informáticos convencionales como para los avanzados, planteando un desafío criptográfico a largo plazo.[3]
- **Proliferación de Ransomware-as-a-Service (RaaS):** Este modelo de negocio sigue floreciendo, permitiendo incluso a ciberdelincuentes con experiencia técnica limitada adquirir kits de ransomware listos para usar, a veces por tan solo 40 dólares. Esto reduce significativamente la barrera de entrada para llevar a cabo ataques sofisticados, lo que lleva a una mayor frecuencia y un alcance más amplio de incidentes, particularmente dirigidos a Pequeñas y Medianas Empresas

(PyMEs) que pueden carecer de defensas robustas.[3] Nuevas variantes de RaaS como AiLock y Crux han sido observadas emergiendo en 2025.[35]

- **Uso Malicioso de la IA Generativa:** Los ciberdelincuentes están aprovechando cada vez más la Inteligencia Artificial (IA) generativa para automatizar y perfeccionar varias etapas de su ciclo de ataque. Esto incluye la depuración de código malicioso, la investigación eficiente de vulnerabilidades críticas, el refinamiento y la personalización de campañas de phishing para hacerlas más convincentes, y la generación de *deepfakes* para ingeniería social avanzada.[38] Esto mejora significativamente la escalabilidad y la eficacia de los ataques de ingeniería social.

Vectores de Ataque Prevalentes y Causas Raíz

Los métodos por los cuales los ciberataques logran su objetivo son variados, pero ciertos vectores y causas raíz son consistentemente predominantes.

- **Vulnerabilidades Explotadas:** Esta sigue siendo la causa raíz más común de los ataques de ransomware.[8] Un hallazgo preocupante es que muchas de las vulnerabilidades explotadas activamente son fallas antiguas y bien conocidas, lo que indica fallas persistentes en la gestión de parches y los procesos de remediación de vulnerabilidades de las organizaciones.[40]
- **Phishing:** A pesar de su larga historia, el phishing basado en correo electrónico sigue siendo el canal principal para iniciar ciberataques.[34] Los atacantes están empleando técnicas de phishing cada vez más sofisticadas, a menudo aumentadas por la IA, para engañar a los objetivos.[20]
- **Infostealers:** Estos tipos de ataques de malware experimentaron un aumento significativo del 58% en 2024. Los *infostealers* están diseñados para robar credenciales y otros datos sensibles de forma encubierta, lo que afecta tanto a individuos como a organizaciones al proporcionar a los atacantes acceso inicial o información valiosa para ataques posteriores.[34]
- **Vulnerabilidades en la Nube y Dispositivos de Borde:** La creciente adopción de entornos en la nube introduce nuevas superficies de ataque. Las configuraciones erróneas y la poca seguridad de las API dentro de las infraestructuras en la nube pueden dejar los sistemas expuestos, permitiendo a los atacantes moverse libremente entre sistemas interconectados. Al mismo tiempo, los dispositivos de borde (por ejemplo, dispositivos IoT, puntos de acceso remoto) están siendo explotados cada vez más como vectores de acceso inicial debido a sus posturas de seguridad a menudo laxas.[34]
- **Falta de Personal/Habilidades:** Un factor operativo crítico que contribuye a que las organizaciones sean víctimas es la importante escasez de personal de ciberseguridad calificado o la falta de habilidades adecuadas dentro de los equipos existentes (afectando al 63% de las organizaciones a nivel mundial).[8] Esta brecha de talento también se señala explícitamente como una razón clave para el crecimiento continuo de los incidentes de ransomware en América Latina.[9]

Actores de Amenazas Comunes (Relevantes para RD y LATAM)

Varios grupos de ciberdelincuentes han demostrado una actividad notable en la República Dominicana y la región latinoamericana.

- **Ransomhub:** Este grupo ha estado muy activo en 2025, siendo notablemente responsable del ataque a Cormidom en la República Dominicana.[10] También estuvo activo a finales de 2024, atacando a Ramon Corripio.[10] A nivel mundial, RansomHub emergió como un grupo de ransomware líder en enero de 2025 [41] y mantuvo una presencia significativa a lo largo de 2024.[34]
- **Direwolf:** Este grupo fue responsable del ataque de ransomware a INICIA en julio de 2025.[10]
- **Nova:** Atacó a SJERP en abril de 2025.[10]
- **Hunters:** Este grupo estuvo detrás del ataque a Edesur Dominicana en marzo de 2025.[10]
- **Sarcoma:** Atacó a Cana Group Corp en enero de 2025.[10]
- **Ransom Hop:** Este grupo fue específicamente identificado como atacante de PCM en enero de 2025.[20]
- **Incransom:** Este grupo atacó a FONPER en junio de 2025 [10] y a Boombah Inc. a finales de 2024.[10] También se señaló como el segundo grupo de ransomware más activo a nivel mundial en julio de 2025.[35]
- **Dispossessor:** Atacó a Unidad de Oftalmología y Catarata a finales de 2024.[10]
- **Qilin:** Este grupo se convirtió en el grupo de ransomware más activo a nivel mundial en julio de 2025, reclamando 73 víctimas.[35] Aunque no está directamente vinculado a una víctima de la República Dominicana en los fragmentos proporcionados, su dominio regional implica una amenaza significativa.
- **LockBit:** A pesar de los informes de que su líder fue desenmascarado, LockBit siguió siendo la variante de ransomware más activa a lo largo de 2024 [41] y fue una preocupación importante para las organizaciones en América Latina.[40] Su presencia continúa o grupos escindidos siguen siendo una amenaza.

Un análisis exhaustivo de la información disponible revela una fuerte correlación entre las tendencias globales y latinoamericanas de ciberseguridad y los incidentes específicos observados en la República Dominicana. Informes detallados de importantes firmas de ciberseguridad [3] destacan consistentemente fenómenos como la proliferación del modelo RaaS, la aparición de tácticas de envenenamiento de datos, el uso creciente de la IA en los ataques y la omnipresente brecha de talento. Es crucial que los incidentes específicos identificados en la República Dominicana [10] presenten actores de amenazas (por ejemplo, Ransomhub, Incransom) y

características de ataque (por ejemplo, exfiltración significativa de datos, ataques a PyMEs a través de sistemas ERP como SJERP) que reflejan directamente estas tendencias más amplias. Por ejemplo, el aumento global del RaaS [9] se correlaciona directamente con la creciente frecuencia de ataques y la capacidad de los actores de amenazas para dirigirse a entidades más pequeñas como SJERP.[14] El énfasis en la exfiltración de datos como componente clave de los ataques de ransomware modernos [9] se evidencia claramente en los incidentes de Edesur [10] y Cormidom.[15] Esto significa que el panorama digital de la República Dominicana está intrínsecamente ligado y directamente afectado por las amenazas cibernéticas globales. Las tendencias y tácticas sofisticadas observadas en todo el mundo y en la región latinoamericana en general se están manifestando activamente dentro del país. Las empresas privadas en la República Dominicana no pueden permitirse el lujo de desarrollar estrategias de seguridad aisladas; en cambio, deben adoptar defensas que no solo sean reactivas a incidentes locales pasados, sino también proactivas en la anticipación y defensa contra amenazas globales reconocidas y en evolución. El monitoreo continuo de la inteligencia de ciberseguridad internacional y la adopción de las mejores prácticas reconocidas a nivel mundial son primordiales para construir una ciberresiliencia efectiva.

Tabla 2: Tendencias y Amenazas Clave de Ciberseguridad para 2025 en la República Dominicana

Categoría de Tendencia/Amenaza	Descripción	Relevancia para el Sector Privado de la RD	IDs de Snippets de Apoyo
Evolución del Ransomware	Técnicas más sofisticadas, resistentes y menos descifrables; cambio de cifrado a extorsión pública (doble/triple extorsión).	Mayor probabilidad de ataques exitosos, presión intensificada sobre las víctimas, daño reputacional severo.	3
Envenenamiento de Datos	Ataques que alteran o inyectan datos incorrectos, comprometiendo la integridad y confiabilidad de la información.	Riesgo de pérdida de confianza en los datos, impacto en la toma de decisiones y operaciones, incluso si se recuperan los sistemas.	3
Proliferación de Ransomware-as-a-Service (RaaS)	Modelos de negocio que permiten a ciberdelincuentes con poca experiencia lanzar ataques sofisticados.	Aumento de la frecuencia y alcance de los ataques, PyMEs son objetivos más fáciles debido a menores barreras técnicas.	3
Uso Malicioso de IA Generativa	Ciberdelincuentes usan IA para depurar código, investigar vulnerabilidades, perfeccionar phishing y crear *deepfakes*.	Mayor sofisticación y personalización de ataques de ingeniería social, haciendo más difícil su detección por parte de los empleados.	38
Explotación de Vulnerabilidades (incluidas las antiguas)	Causa raíz principal de los ataques, a menudo debido a fallas en la gestión de parches y sistemas desactualizados.	Riesgo constante de compromiso incluso por vulnerabilidades conocidas, necesidad urgente de gestión de parches rigurosa.	8
Ataques a la Cadena de Suministro	Compromiso de proveedores externos para acceder a objetivos primarios más grandes o sensibles.	Las empresas, especialmente las PyMEs proveedoras, son eslabones débiles que pueden exponer a sus clientes y socios.	20
Brecha de Talento y Habilidades	Escasez de profesionales de ciberseguridad y falta de capacitación continua en las organizaciones.	Mayor vulnerabilidad a errores de configuración y menor capacidad de respuesta ante ataques, prolongando la exposición.	8
Ataques a la Nube y Dispositivos de Borde	Misconfiguraciones en la nube y seguridad laxa en dispositivos de borde crean nuevos vectores de ataque.	Expansión de la superficie de ataque con la adopción de tecnologías modernas; necesidad de seguridad robusta en todos los puntos de acceso.	34
Infostealers	Malware diseñado para robar credenciales y datos sensibles, a menudo como paso inicial para ataques mayores.	Riesgo de acceso no autorizado a sistemas y cuentas, facilitando ataques de ransomware o fraude.	34

V. Impacto y Consecuencias para el Sector Privado

Costos Multifacéticos de los Ataques

Las repercusiones de un solo ciberataque van mucho más allá del pago inmediato del rescate. Abarcan costos sustanciales de recuperación, una pérdida significativa de productividad debido al tiempo de inactividad operativa, posibles sanciones regulatorias (especialmente con la llegada de nuevas leyes de protección de datos) y un daño reputacional grave y a menudo duradero.[9] A nivel mundial, el costo promedio de recuperación de un ataque de ransomware se informó en 1.5 millones de dólares.[8] En 2024, el costo total promedio de un ciberataque alcanzó los 4.91 millones de dólares, lo que posiciona al ransomware como el tercer tipo de ciberataque más costoso.[42] Estas cifras, aunque globales, proporcionan una fuerte indicación de la carga financiera que enfrentan las empresas dominicanas.

Exfiltración de Datos y Extorsión Pública

Un alto porcentaje de los ciberataques modernos, particularmente los incidentes de ransomware, implican la exfiltración de datos sensibles (94% en 2024 a nivel mundial).[41] Estos datos robados se utilizan luego para amenazar con la exposición pública, lo que añade una capa crítica de riesgo reputacional y legal para las organizaciones víctimas.[9] Una estadística preocupante revela que incluso cuando se paga un rescate, no hay garantía de recuperación de datos o de seguridad contra la exposición pública; en 2024, solo el 47% de las víctimas que pagaron su rescate lograron recuperar sus datos sin corrupción.[42] Esto resalta la naturaleza poco confiable de pagar rescates.

Interrupción Operacional y Continuidad del Negocio

Los ciberataques pueden paralizar gravemente las operaciones comerciales principales, lo que lleva a un tiempo de inactividad significativo y a interrupciones del servicio. Esto se ejemplificó con el incidente de PCM, donde un ataque de ransomware afectó los datos y contratos de los clientes [20], y en general por las interrupciones generalizadas de los sistemas de TI.[32] El tiempo de recuperación de tales incidentes puede ser sustancial, lo que exacerba las pérdidas. En 2024, solo el 22% de las organizaciones atacadas lograron recuperarse en una semana, lo que indica un preocupante aumento en los períodos de recuperación.[42]

Impacto Humano y Tensión Organizacional

Más allá de los aspectos técnicos y financieros, los incidentes cibernéticos ejercen una inmensa presión psicológica y operativa sobre los equipos internos de TI y ciberseguridad, lo que afecta su moral, productividad y eficacia general.[8] La persistente "brecha de talento y capacitación" [9] y la general "falta de personal calificado" [8] exacerban aún más estos desafíos, dejando a las organizaciones críticamente vulnerables y excesivamente dependientes de personal sobrecargado.

Baja Preparación y Conciencia

Una parte significativa de las organizaciones en América Latina (32%) admite no poseer las herramientas necesarias para siquiera confirmar si han sido objeto de un ciberataque.[40] Esta falta de visibilidad es una barrera crítica para una defensa efectiva. Muchas organizaciones continúan reforzando su postura de ciberseguridad de forma reactiva,

después de experimentar un incidente, en lugar de invertir proactivamente en medidas preventivas.[9] Alarmantemente, el 56% de las organizaciones atacadas en 2024 no detectaron una brecha de ransomware durante un período prolongado, que osciló entre 3 y 12 meses, lo que indica un bajo nivel sistémico de conciencia y preparación ante esta amenaza generalizada.[42] Además, solo el 27% de las empresas

latinoamericanas tienen ciberseguro, una herramienta financiera crucial para mitigar el impacto económico y operativo de un ataque.[40] Esta baja tasa de adopción amplifica el golpe financiero cuando ocurre un incidente.

La postura reactiva y la lentitud en la detección de las empresas privadas en la República Dominicana conllevan riesgos compuestos. Los informes indican que muchas organizaciones refuerzan su ciberseguridad solo después de un incidente, no antes.[9] Esto se agrava por el hallazgo de que el 56% de las organizaciones atacadas en 2024 no detectaron una brecha de ransomware durante un período de 3 a 12 meses.[42] Esta detección lenta, junto con la falta de herramientas para confirmar un ataque [40], crea una situación peligrosa. Una "ventana de exposición" prolongada [9] significa que los atacantes tienen mucho más tiempo para exfiltrar datos, cifrar sistemas y causar daños extensos, lo que conduce directamente a "costos de mitigación más altos" [9] y un daño reputacional más severo. La ausencia de un ciberseguro adecuado [40] amplifica aún más la devastación financiera cuando, inevitablemente, ocurre un ataque bajo estas condiciones. Esta postura es económicamente insostenible y estratégicamente peligrosa para las empresas privadas dominicanas. Existe una necesidad urgente de un cambio fundamental de un enfoque de "esperar y ver" a uno de búsqueda proactiva de amenazas, monitoreo continuo de la seguridad y desarrollo de planes de respuesta a incidentes robustos y probados regularmente. Podrían ser necesarios incentivos regulatorios o iniciativas lideradas por la industria para fomentar este cambio y promover capacidades de detección más rápidas, lo que en última instancia reducirá el costo y el impacto general de los ciberataques.

VI. Recomendaciones para una Mayor Resiliencia en Ciberseguridad

Para fortalecer la ciberseguridad del sector privado en la República Dominicana, se sugieren las siguientes recomendaciones estratégicas:

Inversión Estratégica y Proactiva

Las empresas privadas de todos los tamaños en la República Dominicana deben reconocer la ciberseguridad como un imperativo empresarial crítico y adoptar estrategias proactivas para prevenir, detectar y responder a las amenazas, en lugar de simplemente reaccionar a los incidentes.[3] Es fundamental asignar un presupuesto suficiente y dedicado a la ciberseguridad, tratándolo como una inversión fundamental en la continuidad del negocio y la reputación, no solo como un gasto de TI.

Fortalecimiento de la Seguridad Fundacional

La base de una defensa sólida reside en la implementación rigurosa de medidas de seguridad esenciales.

- **Gestión de Parches:** Implementar la aplicación rigurosa y oportuna de actualizaciones de seguridad para todos los sistemas operativos, software y firmware. Las vulnerabilidades explotadas siguen siendo la causa raíz número uno de los ataques, y muchas son antiguas, lo que destaca las fallas persistentes en esta área.[8]
- **Autenticación Multifactor (MFA):** Exigir la implementación de MFA resistente al phishing (por ejemplo, *tokens* basados en aplicaciones o hardware, no SMS) para la mayor cantidad de servicios y cuentas de usuario que sea técnicamente factible.[43]
- **Políticas de Contraseñas Robustas:** Aplicar políticas de contraseñas sólidas, incluidos los requisitos de complejidad y la rotación regular, junto con la concienciación continua del usuario sobre la higiene de las contraseñas.[20]
- **Copia de Seguridad y Recuperación de Datos:** Establecer y mantener procedimientos robustos, aislados y probados regularmente de copia de seguridad y recuperación de datos. Las copias de seguridad deben ser inmutables y almacenarse sin conexión o en entornos segregados para evitar su compromiso durante un ataque.[40]

- **Segmentación de Red:** Implementar la segmentación de red para dividir lógicamente la red en zonas más pequeñas y aisladas. Esto limita el movimiento lateral de los atacantes dentro de la red, conteniendo las brechas y reduciendo su impacto.[25]

Mejora de las Capacidades de Detección y Respuesta

Es vital que las organizaciones puedan identificar y responder rápidamente a las amenazas.

- Adoptar herramientas avanzadas para la protección antimalware centralizada, fuentes de inteligencia de amenazas y monitoreo continuo de la seguridad para mejorar significativamente la visibilidad de las amenazas y reducir los tiempos de detección.[25]
- Desarrollar, documentar y probar regularmente planes integrales de respuesta a incidentes. Estos planes deben describir claramente los roles, responsabilidades y procedimientos para contener, erradicar, recuperar y aprender de los incidentes cibernéticos.[41]

El Elemento Humano y la Capacitación

El factor humano es un punto de entrada frecuente para los ciberdelincuentes.

- **Capacitación de Empleados:** Realizar capacitaciones continuas, atractivas y relevantes sobre concienciación en ciberseguridad para todos los empleados. Se debe hacer especial hincapié en reconocer los intentos sofisticados de phishing, las tácticas de ingeniería social y los peligros de hacer clic en enlaces sospechosos o abrir archivos adjuntos no solicitados.[20] El factor humano es a menudo el punto de entrada más fácil y explotado para los ciberdelincuentes.[20]
- **Desarrollo de Talento:** Abordar activamente la brecha de talento y habilidades en ciberseguridad invirtiendo en el desarrollo profesional continuo y la capacitación de los equipos internos de TI y seguridad. Fomentar una cultura de concienciación y responsabilidad en ciberseguridad desde la alta dirección de la organización.[8]

Gestión de Riesgos de la Cadena de Suministro y Terceros

La dependencia de proveedores externos introduce riesgos significativos que deben gestionarse proactivamente.

- Implementar procesos rigurosos de debida diligencia para todos los proveedores, suministradores y prestadores de servicios externos. Reconocer que estas entidades pueden servir como puntos de entrada significativos para los atacantes en el ecosistema de una organización.[32]
- Establecer requisitos claros de ciberseguridad, obligaciones contractuales y procesos de auditoría regulares para todos los socios de la cadena de suministro para garantizar que cumplen con los estándares mínimos de seguridad.

Colaboración e Intercambio de Información

La seguridad colectiva se beneficia enormemente del intercambio de conocimientos y la cooperación.

- Fomentar activamente la colaboración y el intercambio de información entre entidades gubernamentales, empresas privadas y ciudadanos individuales para crear una postura nacional de ciberseguridad más resiliente.[1]

- Participar en iniciativas nacionales y regionales de intercambio de información sobre ciberseguridad y aprovechar los recursos proporcionados por entidades como el Centro Nacional de Ciberseguridad (CNCS).[5]

Considerar el Ciberseguro

Evaluar y considerar la inversión en ciberseguro como una herramienta crucial para mitigar el impacto financiero y operativo significativo de un ciberataque exitoso.[40]

Un tema recurrente en múltiples fuentes señala el papel fundamental de las vulnerabilidades humanas en el éxito de los ciberataques. Se afirma explícitamente que "lo más fácil y por donde menos recursos se gasta es vulnerar a las personas".[20] Esto se ve reforzado por hallazgos que indican que "el 63% se ve afectado por la falta de personal o de conocimientos" [8], una "baja conciencia de phishing" [9], y que las "capacitaciones en ciberseguridad siguen siendo una necesidad pendiente".[40] Además, la predicción de Gartner para 2027, donde "la mitad de los líderes de ciberseguridad adoptarán prácticas centradas en el ser humano" [2], subraya el creciente reconocimiento de este elemento crucial. Este énfasis consistente indica que depender únicamente de los controles técnicos es insuficiente; el elemento humano representa una superficie de ataque significativa y a menudo subestimada. Para que las empresas privadas en la República Dominicana construyan una resiliencia de ciberseguridad verdaderamente efectiva, deben adoptar una estrategia de seguridad integral que integre sin problemas defensas tecnológicas robustas con un énfasis fuerte y continuo en los factores humanos. Esto se traduce en una capacitación obligatoria, atractiva y actualizada regularmente en ciberseguridad para todos los empleados, fomentando una cultura de seguridad omnipresente que comienza desde el nivel ejecutivo. Simultáneamente, debe haber una inversión sostenida en el desarrollo profesional y la retención de personal de ciberseguridad calificado. Sin abordar adecuadamente el elemento humano, incluso las soluciones técnicas más avanzadas seguirán siendo susceptibles a la explotación, lo que hará que los esfuerzos generales de seguridad sean incompletos y vulnerables.

VII. Conclusión

El sector privado de la República Dominicana se enfrenta a un panorama de amenazas cibernéticas cada vez más desafiante y sofisticado en 2025. El ransomware, en constante evolución con tácticas avanzadas como el envenenamiento de datos, el cifrado resistente a la cuántica y la proliferación de modelos de Ransomware-as-a-Service, representa un riesgo significativo y omnipresente. Si bien los esfuerzos gubernamentales para reforzar la ciberseguridad nacional son encomiables y crecientes, persiste una brecha crítica en la preparación proactiva y los mecanismos de defensa robustos de muchas entidades privadas. Los incidentes identificados que afectan a diversas empresas privadas en varios sectores subrayan que ninguna industria es inmune, y las vulnerabilidades de la cadena de suministro presentan una preocupación particular, creando peligrosos efectos en cadena en toda la economía.

Los costos financieros, operativos y reputacionales de los ciberataques son sustanciales y duraderos, a menudo extendiéndose más allá de los gastos de recuperación inmediatos. Para mitigar eficazmente estos riesgos crecientes y garantizar un crecimiento económico sostenido y la confianza de los inversores, las empresas privadas en la República Dominicana deben pasar urgentemente de respuestas reactivas a estrategias de ciberseguridad integrales y proactivas. Esto implica no solo una inversión estratégica en tecnología de vanguardia y un parcheo diligente de las vulnerabilidades, sino, crucialmente, empoderar el elemento humano a través de la educación continua, fomentar una cultura de seguridad sólida y abordar la brecha crítica de talento. Los esfuerzos de colaboración entre los sectores público y privado, aumentados por sólidas asociaciones internacionales, son esenciales para construir colectivamente un ecosistema digital verdaderamente resiliente y confiable en la República Dominicana. La era de la complacencia con respecto a las amenazas cibernéticas ha terminado inequívocamente. La naturaleza escalada y evolutiva de estas amenazas exige una atención inmediata, sostenida y estratégica, transformando la ciberseguridad de una mera preocupación técnica en un imperativo empresarial fundamental para cada empresa privada que opera en la República Dominicana.

Citas

1. Ciberataques: Una amenaza creciente | Acento, accessed August 12, 2025, https://acento.com.do/opinion/ciberataques-una-amenaza-creciente-9471944.html
2. República Dominicana: Empresas y otros sectores necesitan ..., accessed August 12, 2025, https://www.business-humanrights.org/es/latest-news/rd-empresas-y-otros-sectores-necesitan-fortalecer-su-ciberseguridad-ante-incremento-de-ciberataques/
3. 2025: un año bajo la sombra del ransomware - Forbes República ..., accessed August 12, 2025, https://forbes.do/tecnologia/2025-01-15/2025-un-ano-bajo-la-sombra-del-ransomware
4. Reporte de Ciberseguridad 2025: Aumentan los Ciberataques un 44% | Check Point, accessed August 12, 2025, https://www.youtube.com/watch?v=Zf3lc5fL-g4
5. Noticias - Centro Nacional de Ciberseguridad (CNCS), accessed August 12, 2025, https://cncs.gob.do/noticias/
6. La República Dominicana y Emiratos Árabes Unidos firman acuerdo de cooperación para fortalecer la ciberseguridad, accessed August 12, 2025, https://presidencia.gob.do/noticias/la-republica-dominicana-y-emiratos-arabes-unidos-firman-acuerdo-de-cooperacion-para
7. Digital Shield 2025 afianzó caminos para potenciar la ciberseguridad regional desde la gran capacidad que posee República Dominicana - Delfino.cr, accessed August 12, 2025, https://delfino.cr/2025/05/digital-shield-2025-afianzo-caminos-para-potenciar-la-ciberseguridad-regional-desde-la-gran-capacidad-que-posee-republica-dominicana
8. El estado del ransomware 2025 - Sophos, accessed August 12, 2025, https://www.sophos.com/es-es/content/state-of-ransomware
9. Ransomware en Latinoamérica 2025, accessed August 12, 2025, https://www.redicom.cl/ransomware-en-latinoamerica-2025/
10. Ransomware.live 16 victims for Dominican Republic, accessed August 12, 2025, https://www.ransomware.live/map/DO
11. INICIA - Ransomware.live Victim, accessed August 12, 2025, https://www.ransomware.live/id/SU5JQ0lBQGRpcmV3b2xm
12. INICIA - Asset Management, accessed August 12, 2025, https://inicia.com/
13. Felipe Vicini impulsa a INICIA como una firma de talentos y creadora de valor perdurable, accessed August 12, 2025, https://robertocavada.com/nacionales/2024/07/16/felipe-vicini-impulsa-a-inicia-como-una-firma-de-talentos-y-creadora-de-valor-perdurable/
14. SJERP - SJ ERP, accessed August 12, 2025, https://www.sj.com.do/tag/sjerp/
15. CORMIDOM Data Breach in 2025 - Breachsense, accessed August 12, 2025, https://www.breachsense.com/breaches/cormidom-data-breach/
16. www.cormidom.com.do - Ransomware.live Victim, accessed August 12, 2025, https://www.ransomware.live/id/d3d3LmNvcm1pZG9tLmNvbS5kb0ByYW5zb21odWI=
17. CORMIDOM - Corporación Minera Dominicana | | SITIO CREADO POR CONTROL DIGITAL AGENCY, accessed August 12, 2025, https://cormidom.com.do/
18. Cormidom - Revista Factor de Éxito, accessed August 12, 2025, https://www.revistafactordeexito.com/p/252/cormidom
19. Información de Empresa CANA GROUP CORP. - REP. DOMINICANA - Credit Reporting Agency, accessed August 12, 2025, https://delrisco.com.pe/e0000988059213852-es/cana-group-corp
20. The worst CYBERATTACKS of 2025 Are you really prepared? - YouTube, accessed August 12, 2025, https://www.youtube.com/watch?v=LF8GYSQ9JTI
21. El INDRHI, institución número 60 de la Administración Pública que presenta su Carta Compromiso al Ciudadano, accessed August 12, 2025, https://map.gob.do/2019/09/05/el-indrhi-institucion-numero-60-de-la-administracion-publica-que-presenta-su-carta-compromiso-al-ciudadano/
22. Sistema de Información del Agua República Dominicana Parte #1 acerca de: - Cepei, accessed August 12, 2025, https://cepei.org/wp-content/uploads/2020/06/Gobernaza-SIA_Israel_Acosta.pdf
23. Edesur Dominicana Data Breach in 2025 - Breachsense, accessed August 12, 2025, https://www.breachsense.com/breaches/edesur-dominicana-data-breach/
24. es.wikipedia.org, accessed August 12, 2025, https://es.wikipedia.org/wiki/Edesur_(Rep%C3%BAblica_Dominicana)
25. Ciberseguridad 2025: Protección de Infraestructuras Críticas | - Entel Digital, accessed August 12, 2025, https://enteldigital.cl/reporte-ciberseguridad
26. Ramón Corripio Data Breach in 2024 - Breachsense, accessed August 12, 2025, https://www.breachsense.com/breaches/ram%C3%B3n-corripio-data-breach/
27. Grupo Corripio - Wikipedia, la enciclopedia libre, accessed August 12, 2025, https://es.wikipedia.org/wiki/Grupo_Corripio
28. Grupo Corripio, accessed August 12, 2025, http://www.elmirador.edu.co:8081/wikipedia_es_all_maxi_2023-05/A/Grupo_Corripio
29. 131190741 - Información de Empresa BOOMBAH DOMINICANA S.R.L. - Credit Reporting Agency, accessed August 12, 2025, https://delrisco.com.pe/E0000956558193537-es/boombah-dominicana-srl
30. Official Site - Custom Uniforms, Footwear and Athletic Equipment - Huge Color Selection - Boombah, accessed August 12, 2025, https://www.boombah.com/index2.html
31. Unidad De Oftalmología y Catarata SRL | Bupa medical insurance for Latin America and the Caribbean, accessed August 12, 2025, https://contenidos.bupasalud.com/en/unidad-de-oftalmologia-catarata-srl

32. Ciberamenazas declaradas para empresas en 2025 - Listín Diario, accessed August 12, 2025, https://listindiario.com/la-vida/20250115/ciberamenazas-declaradas-empresas-2025_841473.html
33. Ciberamenazas declaradas para empresas en 2025 - Periódico elDinero, accessed August 12, 2025, https://eldinero.com.do/309629/ciberamenazas-declaradas-para-empresas-en-2025/
34. Resumen del Informe de Ciberseguridad 2025 de Check Point - Data Warden, accessed August 12, 2025, https://www.datawarden.com/blog/resumen-del-informe-de-ciberseguridad-2025-de-check-point
35. Qilin Leads Ransomware Groups Attacks for July 2025 - Cyble, accessed August 12, 2025, https://cyble.com/blog/ransomware-groups-july-2025-attacks/
36. Nosotros - Cana Sports Group, accessed August 12, 2025, https://www.canasportsgroup.com/nosotros/
37. Cyber security report 2025 | Check Point Software, accessed August 12, 2025, https://www.checkpoint.com/security-report/
38. Tendencias en ciberseguridad 2025 - ESET, accessed August 12, 2025, https://www.eset.com/py/acerca-de-eset/sala-de-prensa/comunicados-de-prensa/articulos-de-prensa/tendencias-en-ciberseguridad-2025/
39. The State of Ransomware 2025 - Sophos, accessed August 12, 2025, https://www.sophos.com/en-us/content/state-of-ransomware
40. ESET Security Report 2025 | El estado de la ciberseguridad en empresas de Latinoamérica, accessed August 12, 2025, https://www.welivesecurity.com/es/informes/eset-security-report-2025-ciberseguridad-empresas-latinoamerica/
41. Ransomware 2025: Lessons from the Past Year and What Lies Ahead - GovTech, accessed August 12, 2025, https://www.govtech.com/blogs/lohrmann-on-cybersecurity/ransomware-2025-lessons-from-the-past-year-and-what-lies-ahead
42. Ransomware Tracker 2025 | Latest Ransomware Attacks | Spin.AI, accessed August 12, 2025, https://spin.ai/resources/ransomware-tracker/
43. #StopRansomware: RansomHub Ransomware | CISA, accessed August 12, 2025, https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-242a