GUÍA DE ESTUDIO

Ransomware en Colombia

Comprender un riesgo que puede detener operaciones, exponer información y producir extorsión, sin reducirlo a una sola calificación penal.

Fuentes revisadas: 2026-10-11 · Edición de lectura y trabajo.

Qué podrás hacer

01. Distinguir cifrado, exfiltración y extorsión.

02. Analizar dependencias con proveedores y continuidad.

03. Organizar respuesta técnica y jurídica con información verificable.

1. El fenómeno y sus variantes

CISA describe ransomware como malware que cifra archivos y explica la combinación con robo de datos y amenazas de publicación; puede existir extorsión de datos sin cifrado. Para el análisis propuesto, separar pérdida de disponibilidad, modificación y posible exposición evita tratar todos los incidentes como idénticos. La primera comunicación debe decir qué está confirmado, qué se investiga y qué servicio se afecta. No atribuir autoría basándose en una nota de rescate.

Consultar documento de soporte: www.cisa.gov

2. El caso IFX como lección de dependencia

MinTIC informó el 13 septiembre de 2023 que un ataque iniciado el 12 septiembre contra IFX afectó cerca de 762 compañías en Latinoamérica y servicios colombianos de justicia y salud. Es un reporte inicial de un evento regional, no un total de víctimas colombianas ni una tasa anual. La lección propuesta es revisar dependencias: un proveedor puede impactar trámites aunque el ataque no se dirija a cada entidad usuaria.

Consultar documento de soporte: mintic.gov.co

3. Preparación y respuesta técnica con responsables

La guía CISA propone prevención, respaldo, aislamiento y preservación coordinada. Para Colombia, los contactos y obligaciones deben adaptarse al contexto de la organización. El ejercicio asigna responsable de decisión, equipo técnico, asesoría jurídica y comunicación. La recuperación no se ensaya por primera vez durante una crisis: se propone un simulacro con copia de prueba y objetivos claros, evitando modificar sistemas reales sin autorización.

Consultar documento de soporte: www.cisa.gov

4. Análisis penal por actuaciones probadas

Ransomware no es por sí solo una calificación penal única. Se propone contrastar acceso, daño, obstaculización, software, datos y amenaza con los hechos y el catálogo legal; el artículo 244 se estudia cuando exista constricción para utilidad ilícita. El concurso y los sujetos responsables necesitan análisis concreto. Tampoco el pago permite presumir recuperación o eliminación de copias: la respuesta exige valoración técnica y jurídica documentada.

Consultar documento de soporte: cancilleria.gov.co

Consultar documento de soporte: www.policia.gov.co

5. Información, datos y aprendizaje después del incidente

La organización debería reconstruir una cronología de detección, decisiones y recuperación, con hechos comprobados y vacíos explícitos. El régimen de protección de datos obliga a considerar el tratamiento y sus condiciones, mientras la custodia penal atiende otro propósito. Proponemos separar informe técnico, comunicaciones y análisis jurídico, dejando una lista de mejoras verificables. Al publicar el caso, eliminar datos sensibles e indicadores que expongan innecesariamente a personas o sistemas.

Consultar documento de soporte: cancilleria.gov.co

Consultar documento de soporte: cancilleria.gov.co

Datos y alcance

value: 762

unit: compañías, aproximadamente

period: Reporte 13 septiembre de 2023 sobre ataque iniciado 12 septiembre de 2023

population: Latinoamérica; clientes afectados según comunicado inicial MinTIC

meaning: Impacto regional del incidente IFX

limitation: No totalColombia, no tasa anual, ni certeza final de exfiltración.

Cómo leer la evidencia

Cifrado y exfiltración extorsiva pueden combinarse; extorsión de datos puede existir sin cifrado.

Guía técnica pública estadounidense; no ley colombiana

Contexto colombiano; revisar alcance de la disposición o decisión.

Límite: La fuente respalda las afirmaciones indicadas, no todas las conclusiones de un caso individual. Las propuestas metodológicas de la guía son análisis editorial.

https://www.cisa.gov/stopransomware/ransomware-guide

Reporte inicial de ataque 12 sept 2023 a proveedor y cerca 762 compañías en Latinoamérica.

Reporte institucional de incidente

Tipo y ámbito de la fuente identificados; no se presenta como regla colombiana por el solo hecho de citarse.

Límite: La fuente respalda las afirmaciones indicadas, no todas las conclusiones de un caso individual. Las propuestas metodológicas de la guía son análisis editorial.

https://mintic.gov.co/portal/715/w3-article-278831.html

Se cotejaron artículos 244, 269F, 269I, 269J y nota de modificación del artículo 296 desde 28 de julio de 2026.

Ley colombiana; compilación normativa con notas de vigencia

Contexto colombiano; revisar alcance de la disposición o decisión.

Límite: La fuente respalda las afirmaciones indicadas, no todas las conclusiones de un caso individual. Las propuestas metodológicas de la guía son análisis editorial.

https://cancilleria.gov.co/normograma/compilacion/docs/ley_0599_2000.htm

Permite contrastar catálogo de artículos 269A a 269J y denominaciones legales.

Divulgación institucional de texto legal

Tipo y ámbito de la fuente identificados; no se presenta como regla colombiana por el solo hecho de citarse.

Límite: La fuente respalda las afirmaciones indicadas, no todas las conclusiones de un caso individual. Las propuestas metodológicas de la guía son análisis editorial.

https://www.policia.gov.co/index.php/normatividad-sobre-delitos-informaticos

Marco administrativo de tratamiento de datos, principios y derechos de titulares; no equivale al delito del 269F.

Ley estatutaria colombiana

Contexto colombiano; revisar alcance de la disposición o decisión.

Límite: La fuente respalda las afirmaciones indicadas, no todas las conclusiones de un caso individual. Las propuestas metodológicas de la guía son análisis editorial.

https://cancilleria.gov.co/normograma/compilacion/docs/ley_1581_2012.htm

Llévalo a la práctica

Caso ficticio

Un despacho pierde acceso a su gestor de documentos. El proveedor informa cifrado de servidores, pero aún no confirma extracción. Hay expedientes sensibles y audiencias próximas. El despacho activa continuidad y coordina preservación, evitando afirmar filtración o prometer reparación inmediata. La comunicación describe disponibilidad afectada y aspectos en investigación. El taller compara decisiones posibles y costos de retrasarlas sin recrear el ataque.

Tu recorrido de trabajo

01. Formula la pregunta concreta que el ejemplo permite resolver. Separa hechos dados de supuestos que añadiste.

02. Consulta dos fuentes de la guía. Para cada una registra autor o autoridad, fecha, ámbito y apartado que usarías.

03. Escribe una conclusión provisional con su sustento y una conclusión que todavía no puedas defender. Explica qué información falta.

04. Diseña una revisión humana proporcional al impacto y una regla para detener el uso si no puedes verificar la salida.

Resultado esperado

La meta no es repetir una respuesta predeterminada: es mostrar un razonamiento que otra persona pueda revisar, reconstruir y cuestionar.

Antes de darlo por terminado

01. El ejemplo permanece ficticio y no incorpora datos de un caso real.

02. Cada afirmación decisiva tiene un documento original y un alcance explícito.

03. La respuesta reconoce incertidumbre y no atribuye a una fuente algo que no demuestra.

Preguntas para leer con calma

¿Ransomware se califica siempre como un único delito?

La respuesta depende de los hechos: afectación del sistema o de los datos, exigencia de pago, acceso y posibles transferencias requieren análisis separado. La guía no publica técnicas de ataque ni presupone que pagar garantice recuperación.

¿Qué parte es investigación y qué parte es propuesta editorial?

Las secciones enlazan las fuentes de los hechos o reglas que describen. Los ejercicios, listas y protocolos se identifican como propuestas de trabajo; no se atribuyen a una autoridad ni se presentan como estándares obligatorios.

¿Cómo aportar una actualización o corregir esta guía?

Indica el apartado, el documento original y por qué modifica la afirmación. Una captura o un resumen de IA no reemplaza la fuente. La corrección pasa por revisión editorial y conserva una fecha de actualización.

Método y alcance

Síntesis educativa de fuentes primarias consultadas; análisis y ejercicios propuestos, sujetos a revisión jurídica y actualización.

Fuentes originales

01. CISA - #StopRansomware Guide

https://www.cisa.gov/stopransomware/ransomware-guide

Guía técnica pública estadounidense; no ley colombiana

02. MinTIC - ataque a proveedor IFX Networks y PMU Ciber

https://mintic.gov.co/portal/715/w3-article-278831.html

Reporte institucional de incidente

03. Código Penal - Ley 599 de 2000, compilación de Cancillería

https://cancilleria.gov.co/normograma/compilacion/docs/ley_0599_2000.htm

Ley colombiana; compilación normativa con notas de vigencia

04. Policía Nacional - normatividad de delitos informáticos

https://www.policia.gov.co/index.php/normatividad-sobre-delitos-informaticos

Divulgación institucional de texto legal

05. Ley Estatutaria 1581 de 2012 - protección de datos

https://cancilleria.gov.co/normograma/compilacion/docs/ley_1581_2012.htm

Ley estatutaria colombiana

06. Código de Procedimiento Penal - Ley 906 de 2004

https://cancilleria.gov.co/normograma/compilacion/docs/ley_0906_2004.htm

Ley colombiana; compilación normativa

Continúa en la web

https://alejoqqta.com/temas/ransomware-colombia.html

Consulta la versión web para actualizaciones posteriores a la fecha de revisión.