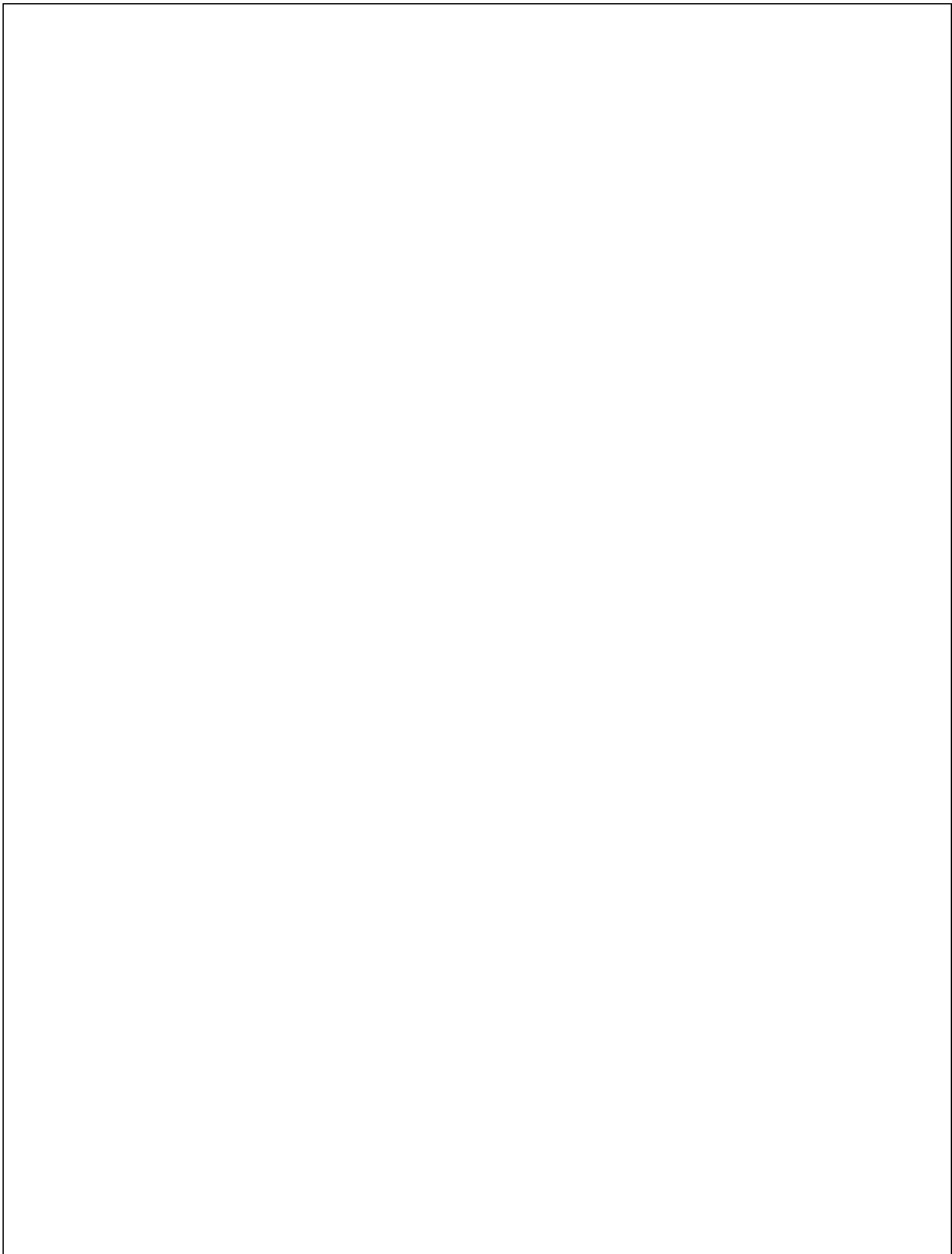


Actividad 01

Análisis en grupo de un ciberataque real y su impacto empresarial.

Colonial Pipeline

- América Fabiola Guerra Ramírez - 179888
- Bruno Axel Puente Luna - 177876
- Laura Ivon Montelongo Martinez - 177291
- Gustavo Michael Larios Guerra - 178318
- Carol Elizabeth Cortes Beltran - 177203
- Benites Rangel Cesar Yahir - 179091
- Cristian Alejandro Rodriguez Moreno - 181641



Contenido

Introducción	5
1.1 Investigación y Documentación.....	6
Contexto general del ataque	8
Tabla Técnica del ataque	10
Evaluación del Impacto.....	11
Costo total del ciberataque	12
1. Coste de Ruptura (CTB).....	12
2. Coste de Construcción (B).....	12
5. Relación con marcos normativos.....	18
ISO 27001 – Controles relevantes aplicables al incidente:	18
Control ISO 27001	18
Relación con el incidente	18
Prevención / Mitigación posible	18
A.9.2.3 – Gestión de credenciales de acceso.....	18
La cuenta VPN sin MFA y con contraseña filtrada permitió el acceso inicial.....	18
Habría exigido MFA y rotación de contraseñas, bloqueando el acceso con credenciales robadas.....	18
A.13.1.1 – Controles de red	18
Falta de segmentación entre TI y OT.....	18
Una segmentación adecuada habría contenido el ataque en la red administrativa.....	18
A.12.3.1 – Copias de seguridad.....	18
Los respaldos fueron eliminados o no eran eficientes para recuperación rápida.....	18
Respaldos <i>offline</i> y pruebas regulares habrían permitido restaurar sin depender del rescate.....	18
A.16.1.5 – Respuesta a incidentes	18
La respuesta fue reactiva y no evitó la exfiltración de datos.....	18
Un plan de respuesta probado habría acelerado la contención y reducido el tiempo de inactividad.....	18
NIST Cybersecurity Framework (CSF) – Controles relevantes:	18
Función NIST CSF.....	18
Controles aplicables	18
Prevención / Mitigación posible	18
Protect.....	18
PR.AC-1 (Gestión de identidades) y PR.AC-7 (Protección de accesos remotos)	18
MFA y revisión de cuentas habrían evitado el acceso no autorizado.....	18
Detect.....	18
DE.CM-1 (Monitoreo de red)	18

Un SIEM con detección de exfiltración habría alertado antes del cifrado.	18
Respond	18
RS.RP-1 (Plan de respuesta)	18
Un plan ejecutado con simulacros habría reducido la paralización operativa.	18
Recover	18
RC.RP-1 (Plan de recuperación)	18
Respaldos validados y herramientas de recuperación eficientes habrían acelerado el retorno.	18
6. Lecciones aprendidas y recomendaciones	20
6.1 Fallas críticas detectadas	20
Fallas técnicas	20
Fallas humanas y organizacionales	20
6.2 Buenas prácticas que habrían reducido el daño	21
6.3 Lecciones estratégicas clave	21
6.4 Recomendaciones para el contexto mexicano y latinoamericano	21
MX Infraestructura crítica en México (energía, transporte, gobierno)	21
Para empresas privadas latinoamericanas	22
6.5 Conclusión del punto	22
Referencias	23

Introducción

En un entorno empresarial caracterizado por la alta dependencia de sistemas digitales y la interconexión entre tecnologías de la información (TI) y tecnologías operativas (OT), la ciberseguridad se ha convertido en un factor crítico para la continuidad del negocio, la estabilidad financiera y la protección de activos estratégicos. Para las organizaciones que operan infraestructura crítica, una disruptión cibernetica no solo representa un incidente tecnológico, sino un evento con potencial de impacto económico, reputacional y operativo a gran escala.

Durante los últimos años, los ataques de tipo ransomware han evolucionado hacia esquemas altamente sofisticados, impulsados por grupos criminales organizados que operan bajo modelos empresariales estructurados, como el Ransomware as a Service (RaaS). Estos ataques combinan técnicas de acceso no autorizado, exfiltración de información y cifrado de sistemas, con el objetivo de maximizar la presión financiera y operativa sobre las organizaciones afectadas. Como resultado, incluso empresas con capacidades técnicas avanzadas pueden verse obligadas a interrumpir operaciones críticas ante la falta de controles preventivos y de resiliencia adecuados.

El presente análisis tiene como objetivo evaluar de manera técnica, económica y estratégica un ciberataque real ocurrido en una infraestructura crítica, con el fin de identificar las causas raíz, el desarrollo del incidente, su impacto sobre los principios fundamentales de la seguridad de la información y las consecuencias operativas y financieras asociadas. El caso seleccionado corresponde al ataque de ransomware sufrido por Colonial Pipeline Company en 2021, considerado un referente a nivel internacional por su impacto directo en el suministro energético y por las implicaciones que generó en materia de gestión de riesgos cibernéticos.

A partir de fuentes técnicas verificables, reportes oficiales y análisis especializados, este documento examina los actores involucrados, los vectores de ataque empleados y las debilidades estructurales que facilitaron el incidente. Asimismo, se evalúan los efectos del ataque sobre la confidencialidad, integridad y disponibilidad (CIA) de los sistemas afectados, se estiman los costos directos e indirectos derivados del evento y se contrasta la postura de seguridad de la organización con marcos internacionales de referencia, como NIST Cybersecurity Framework, ISO/IEC 27001 y regulaciones aplicables en materia de protección de la información. Finalmente, se formulan recomendaciones estratégicas orientadas al fortalecimiento de la gobernanza de ciberseguridad y a la mitigación de riesgos futuros en organizaciones que operan activos críticos.

1.1 Investigación y Documentación.

Fase	Fecha / Periodo	Hito o Evento Clave	Descripción del Suceso
I. Infiltración	Antes del 7 de mayo	Acceso inicial	Los atacantes vulneran la red (probablemente vía VPN/RDP robado o Phishing).
	7 de mayo (Madrugada)	Exfiltración masiva	Se roban aproximadamente 100 GB de información en un lapso cercano a dos horas antes de ejecutar el cifrado de los sistemas.
II. El Ataque	7 de mayo (Mañana)	Activación de DarkSide	El grupo DarkSide ejecuta el ransomware, cifrando los sistemas de Tecnologías de la Información (TI) internos y externos de Colonial Pipeline.
	7 de mayo (Día)	Parada preventiva	Aunque el ataque afectó sistemas TI, la insuficiente segmentación entre entornos TI y OT obliga a Colonial Pipeline a detener preventivamente la operación del oleoducto para evitar una posible propagación. Colonial avisa inmediatamente al Gobierno, el Departamento de Energía y al FBI que están siendo atacados. Colonial Contrata a FireEye para mitigar los efectos del ransomware. (Empresa de ciberseguridad privada).
	7 de mayo	Efectos del Hackeo	Colonial Pipeline detuvo la operación de aproximadamente 5500 Millas (8850 Km) de oleoducto, el cual proveía a la costa este en aproximadamente 45% del petróleo total en la zona. Colonial Pipeline debe de dar una explicación a sus clientes sobre el hackeo y como esto evitara que se suministre gasolina y combustible de avión, lo cual crea especulaciones sobre el precio de estos.
	7-8 de mayo (Noche)	Pago del rescate	La empresa paga 75 BTC (~\$5M USD) a las pocas horas del ataque.
III. Crisis	8-10 de mayo	Escasez, pánico y respuesta gubernamental	La interrupción del oleoducto provoca desabasto progresivo en la Costa Este. Se registran compras de pánico en gasolineras, afectaciones al sector aéreo y reuniones de emergencia en la Casa Blanca. El impacto en el precio del combustible es inicialmente limitado, con incrementos marginales durante los primeros días.
	8 de mayo	Confirmación	Colonial Pipeline confirma al estado que el ransomware no puede ser desencriptado sin ayuda de los hackers, además de confirmar los 100Gb de información robada antes del ataque. Colonial indicó que reactivaría el servicio en segmentos del ducto “de forma escalonada” y consultando con el Departamento de Energía. Dijo que el objetivo de su plan era “restaurar sustancialmente el servicio operacional para el final de la semana”.
	9 de mayo	Sin éxito en la restauración, especulaciones	Colonial Pipeline hace el intento de restaurar sus sistemas sin suerte, las gasolineras empiezan a quedarse secas, puesto que el ultimo abasto de gasolina fue alrededor de dos días antes.

			<p>Se estimó que nada menos que el 7 % de las gasolineras solo en Virginia se quedarían sin combustible al día siguiente.</p> <p>Se cree que los atacantes fueron rusos, Joe Biden sostiene una llamada con Vladimir Putin para preguntar si Rusia estaba involucrada; no se cuenta con información para apuntar a que el gobierno ruso estuviera involucrado, pero se cree que los atacantes residen y operan en rusia, por lo cual se le pide a Vladimir Putin que tome la responsabilidad de atender la situación.</p>
	10 de mayo	Investigación forense y atribución	<p>Se confirma por parte del FBI que los atacantes, en efecto, son el grupo conocido como “DarkSide”, proveedores de ransomware in-home, el FBI publica un comunicado para advertir a otras empresas petroleras del potencial peligro.</p> <p>Por su parte, DarkSide declara públicamente ser un grupo “apolítico” cuyo objetivo es exclusivamente financiero. Paralelamente, Colonial Pipeline establece como meta la restauración sustancial del servicio para finales de esa misma semana.</p>
	11 de mayo	Estados de Emergencia	<p>Carolina del Norte, Virginia, Georgia y Florida declaran emergencia.</p> <p>La escasez empeora. Se autoriza a los conductores de camiones cisterna a trabajar más horas para transportar combustible por carretera</p> <p>El oleoducto número 4 comienza a operar de forma manual y limitada</p>
IV. Retorno	12 de mayo	Reanudación parcial	Colonial anuncia el reinicio de operaciones tras recibir la llave de descifrado.
	13 de mayo	Entrega de combustible	Se restablece el suministro en la mayoría de los mercados.
	14 de mayo	Caída de DarkSide	<p>Los hackers anuncian el cierre de su grupo tras perder acceso a su infraestructura.</p> <p>Darkside vendió su plataforma a otro grupo de hackers</p>
	19 de mayo	Confirmación oficial	Colonial Pipeline confirma públicamente ante el gobierno el pago del rescate.
	7 de junio	Recuperación	El Departamento de Justicia recupera 63,7 bitcoins (Aproximadamente 2,3 Millones de dólares de los atacantes).
	8 de junio	Audiencia del Congreso.	La administración Biden emitió una orden ejecutiva para las agencias del gobierno de Estados Unidos. Que tomen una serie de medidas proactivas para reforzar la ciberseguridad.

Contexto general del ataque

En el año 2021, la empresa Colonial Pipeline Company, operadora de infraestructura crítica en Estados Unidos, fue víctima de un ciberataque de tipo ransomware, atribuido a la familia de malware conocida como DarkSide.

Colonial Pipeline administra el mayor sistema de oleoductos de productos petrolíferos refinados del país, responsable de aproximadamente el 45 % del suministro de combustible de la Costa Este, lo que convirtió al incidente en un evento de alto impacto a nivel nacional. El ataque fue detectado el 7 de mayo de 2021, fecha en la que la empresa emitió un comunicado oficial informando sobre la afectación a sus sistemas informáticos.



Ruta del oleoducto Colonial Pipeline a lo largo de la costa este de Estados Unidos.

El compromiso inicial ocurrió en la red de tecnología de la información (TI) de la organización. Tras confirmarse la presencia del malware, los operadores decidieron desconectar de manera preventiva determinados sistemas de tecnología operativa (OT) con el objetivo de evitar una posible propagación del ataque hacia los entornos industriales.

Esta medida provocó la suspensión total de las operaciones del oleoducto entre el 7 y el 12 de mayo. De acuerdo con la Cybersecurity and Infrastructure Security Agency (CISA), no se identificaron evidencias de que los atacantes hayan obtenido acceso directo a los sistemas OT; sin embargo, la interrupción fue considerada necesaria ante el riesgo potencial para la infraestructura crítica. Reportes especializados indicaron, además, que los atacantes lograron filtrar aproximadamente 100 GB de información durante las primeras etapas del incidente.

En relación con el rescate, el 12 de mayo de 2021, medios de comunicación como CNN informaron que los atacantes habían exigido un pago cercano a los 5 millones de dólares estadounidenses. De acuerdo con fuentes citadas por dicho medio, existía la posibilidad de que la empresa, con apoyo de las autoridades, hubiese logrado recuperar parte de los datos sustraídos que aún no habían sido transferidos fuera de servidores intermedios ubicados en Estados Unidos, lo que habría reducido la necesidad de negociar con los atacantes. No obstante, al día siguiente, Bloomberg publicó información indicando que Colonial Pipeline habría efectuado el pago del rescate en criptomonedas el mismo 7 de mayo, pocas horas después de detectado el ataque, y que funcionarios del gobierno estadounidense tenían conocimiento de dicha transacción.

Posteriormente, la firma especializada en análisis de transacciones en blockchain Elliptic reportó que identificó la billetera de Bitcoin utilizada por el grupo DarkSide, la cual habría recibido un pago aproximado de 75 BTC por parte de

Colonial Pipeline el 8 de mayo de 2021, una porción significativa del cual fue transferida a otras direcciones al día siguiente. Finalmente, el 19 de mayo, un representante de Colonial Pipeline confirmó públicamente que la empresa había realizado el pago del rescate. Tanto la compañía como representantes del Consejo de Seguridad Nacional de Estados Unidos se abstuvieron de proporcionar comentarios detallados sobre el proceso de negociación.

A pesar de haber recibido una herramienta de descifrado por parte de los atacantes, la restauración de los sistemas se vio retrasada, ya que dicha herramienta resultó ser extremadamente lenta e ineficiente, lo que obligó a la empresa a continuar el proceso de recuperación principalmente mediante el uso de respaldos propios. Esta situación contribuyó a prolongar la interrupción del servicio y evidenció limitaciones en las capacidades de recuperación ante incidentes.

Desde la perspectiva de las condiciones de ciberseguridad previas, la organización presentaba un nivel de madurez insuficiente para enfrentar amenazas cibernéticas avanzadas. Reportes técnicos de CISA y análisis especializados de Kaspersky señalan la carencia de controles de seguridad preventivos adecuados, particularmente en los mecanismos de acceso remoto. Entre las principales deficiencias se identificó la ausencia de autenticación multifactor (MFA) en al menos una cuenta comprometida, así como una segmentación inadecuada entre los entornos de TI y OT, lo que incrementó el riesgo de impacto operativo.

Adicionalmente, las políticas de monitoreo continuo, detección de intrusiones y respuesta a incidentes no se encontraban plenamente integradas, y la estrategia de respaldo y recuperación no garantizó una restauración oportuna de los sistemas críticos. La empresa tampoco contaba con un esquema maduro de gestión de identidades y accesos (IAM) ni con una adopción integral de marcos de referencia reconocidos, como el NIST Cybersecurity Framework o los estándares ISA/IEC 62443, esenciales para operadores de infraestructura crítica.

En conjunto, los factores que facilitaron el ataque corresponden principalmente a fallas técnicas y de política de seguridad, incluyendo el uso de credenciales válidas sin mecanismos de autenticación reforzada, controles insuficientes sobre accesos remotos y una gobernanza de ciberseguridad limitada. Estas condiciones reflejan un enfoque predominantemente reactivo, que redujo la capacidad de prevención y resiliencia de la organización frente a un ataque dirigido contra infraestructura crítica de importancia estratégica nacional.

Tabla Técnica del ataque

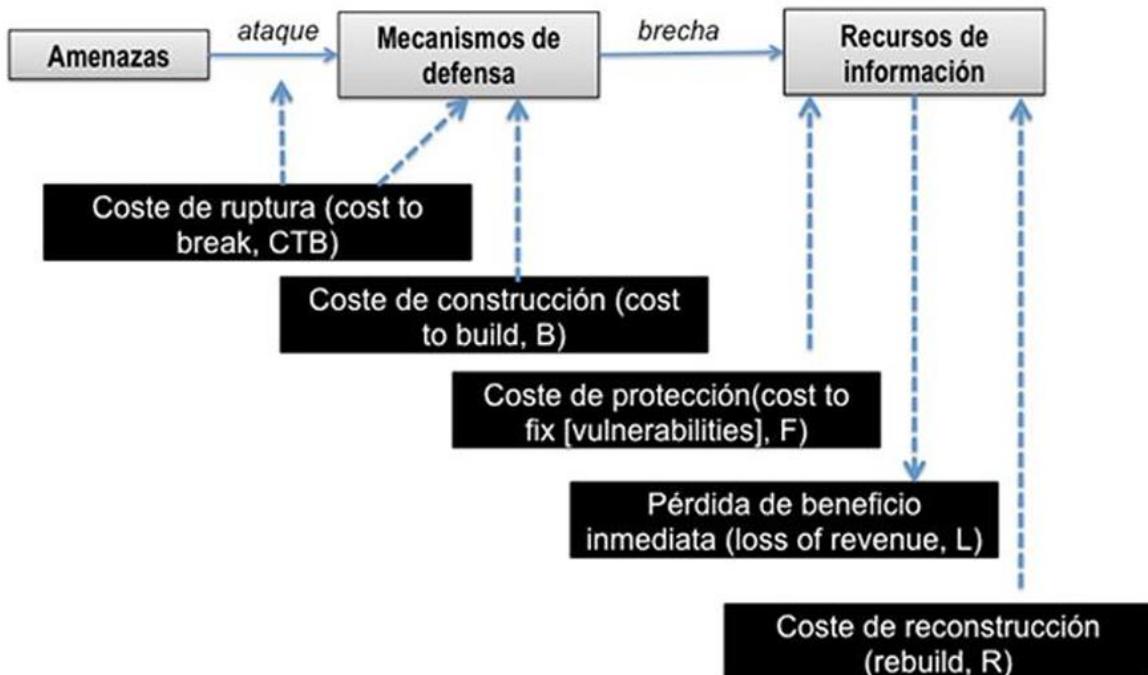
Elemento	Descripción Técnica Ampliada
Tipo de ataque	Ransomware de doble extorsión el cual consistió en el robo masivo de datos confidenciales y el cifrado de los sistemas importantes.
Actor o grupo atacante	El grupo criminal DarkSide que trabaja mediante el sistema de Ransomware as a Service (RaaS) y se cree que es de origen ruso.
Vector de entrada	Acceso remoto mediante una cuenta de VPN antigua(legacy) que estaba activa pero no estaba siendo utilizada facilitando el acceso a los intrusos a la red.
Vulnerabilidad explotada	Se tuvo la falla de políticas de identidad ya que la cuenta carecía de autenticación multifactor (MFA) y utilizaba una contraseña filtrada previamente en la dark web.
Etapas del ataque (MITRE ATT&CK)	El primer acceso fue el 29 de abril seguido de la exfiltración de casi 100 GB de datos y el impacto final con el cifrado de archivos el 7 de mayo.
Sistemas o servicios comprometidos	La red administrativa de IT, servidores de archivos y sistemas de acceso remoto y los sistemas de control OT se apagaron por precaución.
Duración del incidente	Tuvo impacto durante 14 días de crisis desde la infiltración inicial del 29 de abril hasta el reinicio de las operaciones principales el 12 de mayo.
Mecanismos de detección y respuesta	Investigación forense de Mandiant colaboración con CISA FBI, usaron restauración mediante backups y el pago de un rescate de aproximadamente 4.4 y 5 millones.

Evaluación del Impacto.

Principio.	Descripción Del Impacto.	Evidencia del Caso.
Confidencialidad.	<p>Exfiltración masiva de datos y extorsión de su publicación.</p> <p>Los Atacantes robaron aproximadamente 100GB de datos en una ventana de solo 2 horas antes de cifrar los sistemas.</p> <p>Esto habilitó la “doble extorsión (cifrado y amenaza de publicación) lo cual presionó a la empresa a pagar rápidamente.</p>	<p>“En el caso de Colonial Pipeline, los atacantes extrajeron unos 100GB de datos de la red corporativa”. (Pankov N., 12 de mayo 2021).</p>
Integridad.	<p>Eliminación de respaldos.</p> <p>Los respaldos fueron eliminados o fueron poco eficientes para una rápida recuperación.</p>	<p>“Tras el Robo de datos, los atacantes infectaron la red informática de Colonial Pipeline con ransomware que afectó a muchos sistemas informáticos, incluidos los de facturación y contabilidad”. (Kerner M., 26 de abril de 2022).</p> <p>“La herramienta de descifrado era tan lenta que la compañía continuó utilizando sus propios respaldos para restaurar el sistema”. (Turton W., Et Al, 13 de mayo, 2021).</p>
Disponibilidad.	<p>Se obligó a detener operaciones y congelar sistemas IT.</p> <p>La herramienta de desencriptación tomó mucho tiempo de procesamiento, no podía restablecer el sistema lo suficientemente rápido.</p> <p>Provocó escasez de combustible en diferentes estaciones y afectó varios aeropuertos.</p>	<p>“Esto provocó retrasos en el suministro de combustible a lo largo de la Costa Oeste, lo que provocó un aumento del 4% en los futuros de gasolina”. (N. Pankov, 12 de mayo 2021).</p>

4. Costo total del ciberataque

Aplicando el marco económico de Adrian Mizzi, se hizo el cálculo de cuál fue el gasto total del ciberataque.



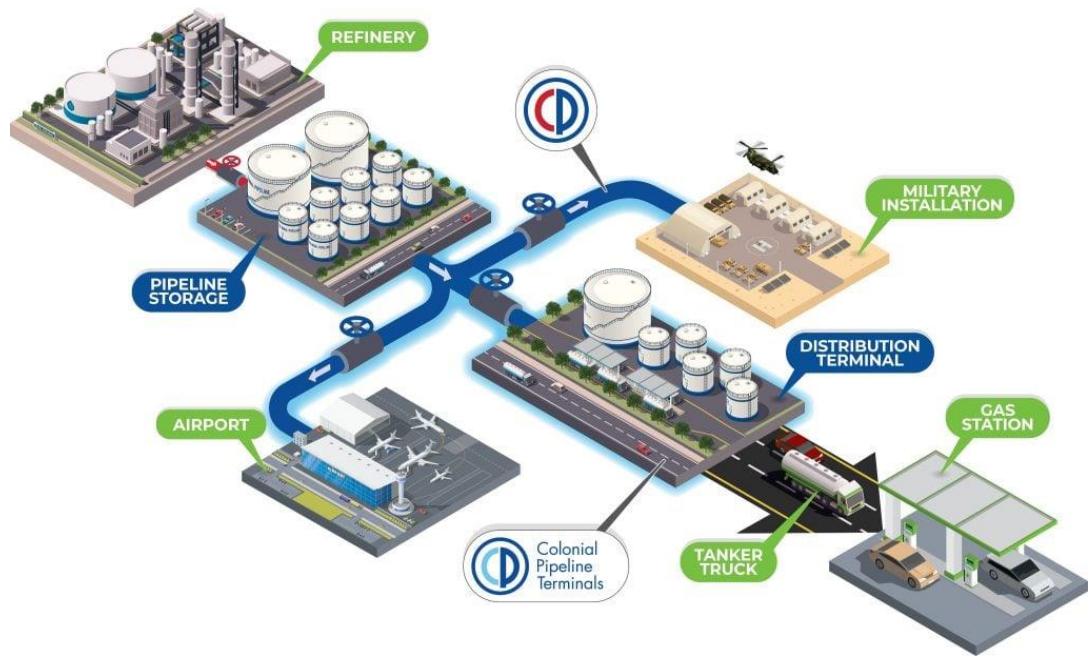
1. Coste de Ruptura (CTB)

El coste de ruptura es el costo total que enfrenta el atacante para romper la seguridad, incluyendo dinero, tiempo, esfuerzo técnico y los riesgos, para nuestro contexto, los atacantes Darkside usaron ransomware ya desarrollado, por lo que se determina que el CTB es de rango medio-bajo, haciendo estimaciones, se proponen estos precios con ayuda de referencias como [Kaspersky](#), [SQ Maganize](#), y [Purplesec](#)

Componente	Estimación (MXN)
Acceso inicial (phishing/credenciales)	\$50000 a \$100000
RaaS / herramientas criminales	\$100000 a \$200000
Herramientas avanzadas / exploits	\$300000 a \$800000
Tiempo y operación (reconocimiento + lateral)	\$200000 a \$600000
Total CTB	\$650000 a \$1700000

2. Coste de Construcción (B)

Para los costes de construcción, se deben de tomar en cuenta Firewalls, IDS, políticas, cifrado, personal y procesos para mantener segura la infraestructura y los sistemas OT. En la página oficial de Colonial Pipeline, relatan algunos de sus servicios y productos.





Pipeline Services

Colonial provides energy logistics and solutions to our shippers and customers. We also offer system storage (tank leasing services), New York Intra Harbor Transfer service, exchange, title transfer, and other support services. Regardless of the service, our goal remains the same—helping our shippers safely and efficiently transport refined petroleum products to their destination.



Pipeline Products

We safely transport various grades of gasoline, diesel, home heating oil and jet fuel, as well as fuels designated for the U.S. military through our pipeline system. These products are primarily received from refineries located on the Gulf Coast and are transported to customers and markets throughout the Southeast and East Coast. Importantly, the various products we transport are tested both as they enter and exit our system to ensure they are delivered on-specification.



Terminals

Colonial entered the terminal business in 2020 through the acquisition of several refined product terminals. Branded as Colonial Pipeline Terminals, the terminal business is a natural extension of our overall business, providing the opportunity to serve our customers in new ways while building and strengthening relationships in the industry.

We provide terminal services in the Southeast and Mid-Atlantic markets. Two of our terminals – located in Austell, Ga. and Chattanooga – are exclusively connected to the Colonial Pipeline system; another terminal, located in Fredericksburg, Va., is connected to the SE Products Pipeline, and our Charlotte terminal is connected to both Colonial Pipeline and the SE Products Pipeline. Each of these locations provides throughput, storage, and distribution solutions for gasoline, diesel, and renewable fuels.

En resumen, Colonial Pipeline ofrece servicios de refinado de combustible en diferentes grados, almacenamiento de combustible, logística de energía, transporte de producto, terminales de combustible, consistiendo en 8850 Km de oleoducto repartidos en 3 líneas, con capacidad de proveer 3 millones de barriles de combustible entre Texas y New York. Con todo esto en mente, podemos suponer que la infraestructura de Colonial Pipeline necesita una inversión muy alta en Seguridad, puesto que casi la mitad del sur dependen de sus servicios.

Toda la infraestructura requiere sistemas OT (desaladoras, hornos, torres de destilación, unidades de conversión y de tratamiento, junto con tanques de almacenamiento y antorchas de seguridad), por ende, estos sistemas necesitan un Firewall.

- IDS/IPS para los sistemas OT.
- Seguridad dedicada TI.
- SOC y monitoreo.
- Personal especializado y consultorías.
- Políticas, procesos y hardening.

Para una infraestructura segura, se requiere inversión en infraestructura física de red que soporte segmentación, control de acceso y visibilidad, especialmente en entornos donde TI y OT conviven. El [catálogo de Panduit](#) ofrece productos clave para esto, y sus precios nos permiten estimar el coste de Construcción de forma objetiva.

Categoría	Cantidad estimada	Total estimado (MXN)
Cables y conectores	6 sets	\$120000 a \$186000
Gabinetes + racks	4 c/u	\$160000 a \$320000
Gestión de cables	-	\$60000 a \$100000
Seguridad física puertos	-	\$24000 a \$48000
UPS y energía	4 c/u	\$120000 a \$240000
Total infraestructura física		\$484000 a \$894000

3. Coste de Protección (F)

El Coste de Protección (F) representa los gastos anuales continuos necesarios para mantener y operar eficazmente los mecanismos de defensa que protegen la infraestructura de TI y OT. Esto incluye licencias de software de seguridad (firewalls, IDS/IPS, SIEM, autenticación multifactor), contratos de soporte y mantenimiento, el salario de personal especializado en ciberseguridad, servicios de monitoreo 24/7 (SOC), auditorías periódicas de cumplimiento (ISO/NIST/ISA/IEC 62443) y capacitación continua del personal técnico.

Con base en rangos de mercado para organizaciones de gran escala, se estima que el coste total anual de protección (F) se sitúa entre \$9,200,000 y \$16,600,000 pesos mexicanos por año, con un valor representativo de aproximadamente \$12,500,000 MXN anuales. Este rango considera tanto licencias y servicios gestionados como personal interno y actividades de mejoramiento continuo.

Categoría	Rango anual (MXN)
Licencias	\$2600000 a \$5200000
Soporte	\$500000 a \$1200000
Personal	\$3000000 a \$4500000
SOC / Monitoreo	\$2000000 a \$3500000
Auditorías	\$800000 a \$1500000
Capacitación	\$300000 a \$700000
Total F	\$9200000 a \$16600000 por año

4. Perdida de beneficio inmediata (L)

Las Perdida de beneficio inmediata (L) representa el impacto económico directo sufrido por Colonial Pipeline como resultado de la interrupción operativa causada por el ataque de ransomware. Esto incluye los ingresos no generados

durante los aproximadamente cinco días de paralización de operaciones, el impacto de mercado derivado de la escasez temporal de combustible, así como costos regulatorios y legales posteriores al incidente.

Con base en estimaciones de ingresos diarios de la operación normal del oleoducto, convertidos a pesos mexicanos, y apoyados en análisis económicos de interrupciones de servicios críticos, se estima que el costo total de pérdidas se sitúa en un rango aproximado de 1,062.5 millones a 2,006.25 millones de pesos mexicanos, con un valor representativo de 1,500 millones MXN para fines de análisis cuantitativo.

Componente	Estimación (MXN)
L1 – Ingresos operativos perdidos	875 M a 1312.5 M
L2 – Impacto de mercado/reputación	87.5 M a 393.75 M
L3 – Costos regulatorios y legales	100 M a 300 M
Total L	1062.5 M a 2006.25 M

5. Coste de reconstrucción (R)

El Coste de Reconstrucción (R) representa los gastos incurridos después del incidente para restaurar operatividad, reforzar controles y documentar acciones de recuperación. Este costo incluye la restauración de sistemas TI y OT, servicios de análisis forense y consultoría especializada, implementación de mejoras de seguridad y configuración, además de actividades administrativas y cumplimiento posterior al incidente.

Basado en rangos de proyectos de recuperación y respuesta a incidentes de ransomware de gran escala, se estima que R se sitúa entre \$150 millones y \$480 millones de pesos mexicanos, con un valor representativo de \$300 millones MXN. Este rango contempla tanto trabajo técnico especializado como actualizaciones estructurales necesarias tras el ataque.

Componente	Estimación (MXN)
R1 – Restauración técnica	\$87.5M – \$262.5M
R2 – Forense/Consultoría	\$17.5M – \$87.5M
R3 – Hardening/Mejoras	\$35M – \$105M
R4 – Administración y documentación	\$10M – \$25M
Total R	\$150M – \$480M MXN

6. Conclusión del costo total del ciberataque

El análisis económico del ataque de ransomware a Colonial Pipeline, utilizando el marco de Adrian Mizzi, evidencia que el impacto financiero total del incidente, estimado entre 2,525 y 3,800 millones de pesos mexicanos, superó ampliamente el presupuesto anual típico de ciberseguridad del sector energético, el cual suele ubicarse alrededor de los 400 a 500 millones de pesos anuales. Esto implica que el costo del ataque fue entre cinco y ocho veces mayor que una inversión anual razonable en controles preventivos, monitoreo y resiliencia. El caso demuestra que la ciberseguridad no debe considerarse un gasto operativo opcional, sino una inversión estratégica esencial para la continuidad del negocio, especialmente en organizaciones que operan infraestructura crítica, donde una interrupción tecnológica puede traducirse en crisis económicas, sociales y de seguridad nacional.

Tipo de costo	Descripción	Estimación (MXN)
Pérdidas operativas	Días de inactividad, cancelación de operaciones o servicios.	\$875000000 a \$1312500000
Daños reputacionales	Impacto de mercado, pérdida de confianza, especulación de clientes/mercados.	\$87500000 a \$393750000
Costos técnicos	Recuperación de sistemas, consultorías, reemplazo de procesos y mejoras.	\$150000000 a \$480000000

Costos legales / regulatorios	Auditorías, cumplimiento, posibles sanciones, documentación legal.	\$100000000 a \$300000000
Pago de rescate o extorsión	Monto pagado por Colonial Pipeline en criptomonedas.	\$1312500000 (equivalente a 75 BTC ~ \$5M USD)
TOTAL ESTIMADO	Suma total aproximada de los impactos económicos.	\$252500,000 a \$3800000000

5. Relación con marcos normativos

ISO 27001 - Controles relevantes aplicables al incidente:

Control ISO 27001	Relación con el incidente	Prevención / Mitigación posible
A.9.2.3 - Gestión de credenciales de acceso	La cuenta VPN sin MFA y con contraseña filtrada permitió el acceso inicial.	Habría exigido MFA y rotación de contraseñas, bloqueando el acceso con credenciales robadas.
A.13.1.1 - Controles de red	Falta de segmentación entre TI y OT.	Una segmentación adecuada habría contenido el ataque en la red administrativa.
A.12.3.1 - Copias de seguridad	Los respaldos fueron eliminados o no eran eficientes para recuperación rápida.	Respaldos <i>offline</i> y pruebas regulares habrían permitido restaurar sin depender del rescate.
A.16.1.5 - Respuesta a incidentes	La respuesta fue reactiva y no evitó la exfiltración de datos.	Un plan de respuesta probado habría acelerado la contención y reducido el tiempo de inactividad.

NIST Cybersecurity Framework (CSF) - Controles relevantes:

Función NIST CSF	Controles aplicables	Prevención / Mitigación posible
Protect	PR.AC-1 (Gestión de identidades) y PR.AC-7 (Protección de accesos remotos)	MFA y revisión de cuentas habrían evitado el acceso no autorizado.
Detect	DE.CM-1 (Monitoreo de red)	Un SIEM con detección de exfiltración habría alertado antes del cifrado.
Respond	RS.RP-1 (Plan de respuesta)	Un plan ejecutado con simulacros habría reducido la paralización operativa.
Recover	RC.RP-1 (Plan de recuperación)	Respaldos validados y herramientas de recuperación eficientes habrían acelerado el retorno.

GDPR (aplicación contextual):

Aunque Colonial Pipeline no está sujeta al GDPR, los principios de **notificación de violaciones de datos y protección de datos personales** son relevantes. La exfiltración de 100 GB pudo incluir datos personales de empleados o clientes. Bajo

GDPR, esto habría exigido notificación a autoridades en 72 horas, lo que podría haber acelerado la respuesta y la transparencia pública.

Conclusión

La aplicación estructurada de marcos como **ISO 27001** y **NIST CSF** habría fortalecido la postura de seguridad de Colonial Pipeline, especialmente en gestión de accesos, segmentación, monitoreo y recuperación. La adopción de estos marcos no es solo un requisito normativo, sino una estrategia de resiliencia operativa ante amenazas como el ransomware.

6. Lecciones aprendidas y recomendaciones

El incidente de Colonial Pipeline evidenció que incluso operadores de infraestructura crítica pueden verse comprometidos cuando la ciberseguridad no es tratada como un componente estratégico del negocio. El ataque no fue producto de una sola vulnerabilidad, sino de una **cadena de fallas técnicas, operativas y de gobernanza**.

6.1 Fallas críticas detectadas

Fallas técnicas

1. Ausencia de autenticación multifactor (MFA) en accesos remotos

El acceso inicial se produjo mediante una cuenta VPN antigua que solo utilizaba usuario y contraseña. Esta credencial estaba filtrada en la dark web. Esto permitió que los atacantes ingresaran como un usuario legítimo.

2. Gestión deficiente de identidades y accesos (IAM)

- Cuenta obsoleta aún activa
- Falta de revisión periódica de accesos
- Ausencia de principio de mínimo privilegio

3. Segmentación insuficiente entre TI y OT

Aunque el malware no llegó a sistemas industriales, el riesgo de propagación obligó a detener la operación del oleoducto.

4. Monitoreo y detección tardíos

Los atacantes exfiltraron 100 GB de información antes de activar el cifrado sin ser detectados oportunamente.

5. Estrategia de respaldo y recuperación poco efectiva

- La herramienta de descifrado fue lenta
- Dependencia parcial del pago del rescate
- Restauración prolongada

6. Controles de acceso remoto débiles

VPN sin MFA, sin políticas estrictas de dispositivos confiables o verificación adicional.

Fallas humanas y organizacionales

1. Gobernanza de ciberseguridad débil

La ciberseguridad no estaba plenamente integrada en la gestión de riesgos corporativos.

2. Enfoque reactivo, no preventivo

No se priorizaron controles básicos a pesar de operar infraestructura crítica.

3. Falta de cultura de seguridad

Las cuentas antiguas no deberían existir si hubiera procesos estrictos de revisión.

4. Planes de continuidad no probados a nivel realista

La interrupción operativa mostró que los planes no estaban optimizados para un escenario de ransomware.

6.2 Buenas prácticas que habrían reducido el daño

Si se hubieran aplicado correctamente, estas medidas habrían evitado o minimizado el impacto:

Área	Buena práctica	Impacto que habría mitigado
Accesos remotos	MFA obligatorio	Habría bloqueado el acceso inicial
Identidades	Auditoría periódica de cuentas	La VPN obsoleta habría sido eliminada
Red	Segmentación TI/OT estricta	Menor necesidad de detener operaciones
Monitoreo	SIEM + detección de exfiltración	Alerta antes del cifrado
Respaldo	Backups offline y pruebas periódicas	Recuperación sin pagar rescate
Respuesta a incidentes	Simulacros de ransomware	Reducción del tiempo de inactividad
Gobernanza	Alineación con NIST CSF e ISA/IEC 62443	Mejor preparación estructural

6.3 Lecciones estratégicas clave

1. El ransomware es un riesgo operativo, no solo informático

Puede detener infraestructura física crítica.

2. Las credenciales robadas son el vector más peligroso hoy en día

No fue un exploit sofisticado, fue mala gestión de accesos.

3. Pagar rescate no garantiza recuperación rápida

El descifrador fue ineficiente.

4. TI y OT están conectados a nivel de riesgo

Aunque no se infectó OT, la empresa tuvo que detenerlo.

5. La ciberseguridad es un asunto de seguridad nacional

El incidente generó impacto económico y político.

6.4 Recomendaciones para el contexto mexicano y latinoamericano

MX Infraestructura crítica en México (energía, transporte, gobierno)

1. Implementar MFA obligatorio en todos los accesos remotos

2. Eliminar cuentas heredadas y accesos no utilizados

- 3. Adoptar el marco NIST CSF como base mínima**
- 4. Separar redes TI y OT físicamente cuando sea posible**
- 5. Establecer monitoreo continuo con detección de exfiltración**
- 6. Mantener respaldos offline (air-gapped)**
- 7. Realizar simulacros anuales de ciberataques**
- 8. Crear equipos CSIRT internos o sectoriales**
- 9. Invertir en capacitación del personal**
- 10. Integrar la ciberseguridad en la alta dirección (gobernanza)**

Para empresas privadas latinoamericanas

- No depender solo de antivirus tradicional
- Revisar accesos VPN cada mes
- Usar Zero Trust para accesos externos
- Contratar auditorías de ciberseguridad anuales
- Tener seguro de riesgo cibernético

6.5 Conclusión del punto

El ataque a Colonial Pipeline demuestra que:

La ausencia de controles básicos puede generar crisis nacionales.

No fue un ataque técnicamente imposible de prevenir, sino el resultado de fallas acumuladas de gestión, monitoreo y gobernanza.

Las organizaciones latinoamericanas que operan servicios esenciales pueden aprender de este caso implementando controles preventivos antes de enfrentar un evento de alto impacto.

Referencias

Agencias y Organismos Públicos

1. CISA. (2021a, mayo 11). *Alert AA21-131A: DarkSide ransomware best practices*. Cybersecurity and Infrastructure Security Agency. <https://www.cisa.gov/news-events/cybersecurity-advisories/aa21-131a>
2. CISA. (2021b). *DarkSide ransomware: Best practices for preventing business disruption from ransomware attacks.* Cybersecurity and Infrastructure Security Agency. <https://www.cisa.gov/resources-tools/resources/darkside-ransomware-best-practices-preventing-business-disruption-ransomware>
3. ENISA. (2023). *Threat landscape report 2023.* European Union Agency for Cybersecurity. <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023>
4. FBI. (2021, mayo 10). *DarkSide ransomware: Indicators of compromise.* Federal Bureau of Investigation. <https://www.ic3.gov/Media/News/2021/210511.pdf>
5. NIST. (2017). *Digital identity guidelines* (Publicación SP 800-63B). National Institute of Standards and Technology. <https://doi.org/10.6028/NIST.SP.800-63b>
6. NIST. (2018). *Contingency planning guide for federal information systems* (Publicación SP 800-34 Rev. 1). National Institute of Standards and Technology. <https://doi.org/10.6028/NIST.SP.800-34r1>
7. NIST. (2020a). *Glossary: Malware.* National Institute of Standards and Technology. <https://csrc.nist.gov/glossary/term/malware>
8. NIST. (2020b). *Zero trust architecture* (Publicación SP 800-207). National Institute of Standards and Technology. <https://doi.org/10.6028/NIST.SP.800-207>
9. U.S. Department of Energy. (2021). *Colonial Pipeline cyber incident summary.* <https://www.energy.gov/sites/default/files/2021-06/Colonial%20Pipeline%20Cyber%20Incident%20Summary.pdf>
10. **Organismos de Estándares y Marcos**
 11. ISO/IEC. (2022). *Information security, cybersecurity and privacy protection — Information security management systems — Requirements* (ISO/IEC 27001:2022). International Organization for Standardization.
 12. ISA/IEC 62443. (2018). *Security for industrial automation and control systems* (Serie de Estándares IEC 62443). International Society of Automation / International Electrotechnical Commission.
 13. MITRE. (s.f.). *Exfiltration (TA0010).* MITRE ATT&CK Framework. Recuperado el [fecha de acceso], de <https://attack.mitre.org/tactics/TA0010/>
14. **Sector Privado e Investigación**
 15. Gartner. (2022). *Magic quadrant for security information and event management.*
 16. Kaspersky. (2022). *Ransomware explained: What it is and how it works.* <https://www.kaspersky.com/resource-center/threats/ransomware-attacks-and-types>
 17. MITRE Engenuity. (2023). *MITRE Engenuity ATT&CK evaluations for endpoint detection and response.* <https://attackevals.mitre-engenuity.org/>
 18. Verizon. (2023). *2023 Data breach investigations report.* <https://www.verizon.com/business/resources/reports/dbir/>
 19. Kaspersky ICS CERT. (2021, 21 de mayo). *DarkChronicles: the consequences of the Colonial Pipeline attack.* Kaspersky. <https://ics-cert.kaspersky.com/publications/reports/2021/05/21/darkchronicles-the-consequences-of-the-colonial-pipeline-attack/>
 20. The New York Times. (2021, 8 de mayo). *Cyberattack forces a shutdown of a top U.S. pipeline.* NYTimes.com. <https://www.nytimes.com/2021/05/08/us/politics/cyberattack-colonial-pipeline.html>
 21. The New York Times. (2021, 11 de mayo). *Ciberataque al oleoducto Colonial Pipeline: esto sabemos* [Edición en español]. NYTimes.com. <https://www.nytimes.com/es/2021/05/11/espanol/colonial-pipeline-ransomware.html>
 22. The New York Times. (2021, 14 de mayo). *DarkSide, blamed for gas pipeline attack, says it is shutting down.* NYTimes.com. <https://www.nytimes.com/2021/05/14/business/darkside-pipeline-hack.html>

23. The New York Times. (2021, 15 de mayo). *Hacked pipeline is now delivering 'millions of gallons' an hour, owner says.* [NYTimes.com](https://www.nytimes.com/2021/05/15/business/colonial-pipeline-hack-southeast.html). <https://www.nytimes.com/2021/05/15/business/colonial-pipeline-hack-southeast.html>
24. The New York Times. (2021, 2 de junio). *El caso DarkSide: Rusia se está convirtiendo en el paraíso del cibersecuestro* [Edición en español]. [NYTimes.com](https://www.nytimes.com/es/2021/06/02/espanol/darkside-rusia-ciber-ataque.html). <https://www.nytimes.com/es/2021/06/02/espanol/darkside-rusia-ciber-ataque.html>
25. Cybersecurity and Infrastructure Security Agency (CISA). (2022, 1 de abril). *The attack on Colonial Pipeline: What we've learned & what we've done over the past two years.* <https://www.cisa.gov/news-events/news/attack-colonial-pipeline-what-weve-learned-what-weve-done-over-past-two-years>
26. Sophos. (2021, 11 de mayo). *A defender's view inside a DarkSide ransomware attack.* <https://www.sophos.com/en-us/blog/a-defenders-view-inside-a-darkside-ransomware-attack>
27. Federal Bureau of Investigation. (2021, 10 de mayo). *FBI statement on compromise of Colonial Pipeline networks.* <https://www.fbi.gov/news/pressrel/press-releases/fbi-statement-on-compromise-of-colonial-pipeline-networks>
28. Sanger, D. E., & Krauss, C. (2021, 14 de mayo). *Cyberattack forces a shutdown of a vital U.S. pipeline.* The New York Times. <https://www.nytimes.com/2021/05/08/us/politics/cyberattack-colonial-pipeline.html>
29. Amaya, J. (2022, 7 de septiembre). Mercado de acceso inicial: ¿Cómo entran los atacantes a sus víctimas? Kaspersky Daily. <https://latam.kaspersky.com/blog/initial-access-market-2022/24941/>
30. St John, D. (2023, 25 de mayo). Cyberattacks and ransomware statistics – UK & worldwide. SQ Magazine. <https://sqmagazine.co.uk/ransomware-statistics/>
31. PurpleSec. (2023, 12 de junio). Average cost of ransomware attacks in 2023. PurpleSec. <https://purplesec.us/learn/average-cost-of-ransomware-attacks/>
32. Panduit. (2025). Infraestructura de redes corporativas [Catálogo de productos, CPCB295-SA-ROLATAM-01-2025]. <https://www.panduit.com/content/dam/panduit/es/website/support/documents/infraestructura-de-redes-corp-catalogo-cpcb295-sa-rolatam-01-2025.pdf>
33. Arzate Noticias. (2026, 29 de enero). Solo 49% de las organizaciones invierten en ciberseguridad tras filtración de datos. <https://arzatenoticias.com/index.php/2026/01/29/solo-49-de-las-organizaciones-invieren-en-ciberseguridad-tras-filtracion-de-datos/>
34. EY Australia. (2022, 1 de junio). How cyber security can keep pace with the energy transition. EY. https://www.ey.com/en_au/insights/cybersecurity/how-cyber-security-can-keep-pace-with-the-energy-transition
35. Pankov N. (2021, 12 de mayo) . "How Colonial Pipeline managed its ransomware attack". <https://www.kaspersky.com/blog/pipeline-ransomware-mitigation/39907/>
36. Kerner M. (2022, 26 de abril). "Colonial Pipeline hack explained: Everything you need to know". <https://www.techtarget.com/whatis/feature/Colonial-Pipeline-hack-explained-Everything-you-need-to-know>
37. Turton W. Et al. (2021, 13 de mayo) "Colonial Pipeline paid hackers nearly \$5 Million in Ransom". <https://archive.is/20210514165246/https://www.bloomberg.com/news/articles/2021-05-13/colonial-pipeline-paid-hackers-nearly-5-million-in-ransom>