Análisis de un ciberataque y su impacto empresarial

Caso de Pemex (2019)

Integrantes del equipo:

López López Josue Emmanuel	182078
Mata Martinez Aaron Efraim	179419
Rodriguez Hernandez Edgar Omar	177888
Rodriguez Morin Estefano Alessandro	178584
Ros Padilla Ivan	177573
Salinas Carrillo Mauricio Josafat	177406

30 de enero de 2026

Glosario:

Introducción

El presente informe tiene como objetivo analizar de manera forense, técnica y estratégica el ciberataque sufrido por Petróleos Mexicanos (Pemex) en noviembre de 2019. Este incidente, perpetrado contra la empresa estatal más importante de México, no fue un evento aislado, sino un caso paradigmático de la tendencia criminal conocida como "Big Game Hunting", donde actores de amenazas avanzadas dirigen sus ataques hacia infraestructuras críticas con alta capacidad de pago.

El ataque fue ejecutado mediante el ransomware **DoppelPaymer**, atribuido al grupo criminal **INDRIK SPIDER**. El incidente comprometió más de 11,000 activos informáticos, paralizó sistemas administrativos y de facturación, y expuso severas deficiencias en la arquitectura de seguridad de la paraestatal, incluyendo una profunda "deuda técnica" y gestión deficiente de vulnerabilidades.

A través de este documento, el grupo de trabajo desglosará la cadena del ataque (*Cyber Kill Chain*), evaluará el impacto bajo el modelo de seguridad CIA (Confidencialidad, Integridad y Disponibilidad) y estimará los costos financieros y reputacionales derivados, con el fin de comprender la importancia crítica de la ciberseguridad en la sostenibilidad operativa de las organizaciones nacionales.

Fase 1. Investigación y Documentación: Línea de Tiempo del Ataque

A continuación, se presenta la reconstrucción cronológica de los hechos, basada en reportes técnicos de firmas de ciberseguridad (CrowdStrike, FireEye) y la auditoría forense de la Auditoría Superior de la Federación (ASF). Se destacan las vulnerabilidades iniciales que permitieron la intrusión.

Periodo / Fecha	Fase del Ataque (Kill Chain)	Hechos Clave y Descripción del Evento	Vulnerabilidades Iniciales y Vectores Explotados
Antecedentes (2015 - 2019)	**Vulnerabilidad Sistémica (Pre-Condiciones)**	Existe una obsolescencia tecnológica crítica en la infraestructura. Los servidores operan con sistemas fuera de soporte (End-of-Life) desde 2015.	**Sistemas Legacy:** Uso de Windows Server 2003 y Windows 7 sin actualizaciones de seguridad, creando un entorno permisivo para ataques.

Marzo - Abril 2019	**Aparición del Vector de Entrada (Reconnaissance)**	Microsoft publica parches para una falla crítica en SharePoint. **Pemex omite la instalación de estas actualizaciones**, dejando servidores expuestos a internet durante más de 6 meses.	**CVE-2019-0604:** Vulnerabilidad de Ejecución Remota de Código (RCE) en SharePoint. Falta de políticas de gestión de parches (*Patch Management*).
Septiembre - Octubre 2019	**Acceso Inicial (Initial Access)**	El grupo **INDRIK SPIDER** logra penetrar la red corporativa. Se presume la explotación de la vulnerabilidad web o campañas de *Spearphishing* dirigidas.	**Defensa Perimetral Débil:** Servidores expuestos a internet sin segmentación adecuada (DMZ) y posible falta de concientización de usuarios ante correos maliciosos.
Octubre - Inicios Nov 2019	**Persistencia y Movimiento Lateral**	Los atacantes permanecen en la red (*Dwell Time*) realizando reconocimiento. Usan herramientas como **Mimikatz** (robo de credenciales) y **Cobalt Strike** para escalar privilegios hasta obtener control de Administrador de Dominio.	**Falta de Visibilidad (EDR):** El 16.4% de equipos carecía de protección avanzada (ATP) y el 27.4% no tenía prevención de fuga de datos (DLP). Antivirus desactualizados no detectaron el comportamiento anómalo.
10 de Noviembre 2019 (Domingo)	**Ejecución e Impacto (Detonación)**	Se despliega el ransomware **DoppelPaymer** masivamente. El malware termina procesos de seguridad y bases de datos, y cifra la información con algoritmos AES-256 + RSA-2048 (extensión .locked).	**Falla en Segmentación:** La red plana permitió que el malware se distribuyera rápidamente desde los servidores centrales a las estaciones de trabajo.
11 de Noviembre 2019	**Descubrimiento y Respuesta**	Aparece la nota de rescate exigiendo **565 Bitcoins** (~4.9 MDD) con amenaza de publicar datos robados (Doble Extorsión). Pemex ordena desconectar la red para contener la propagación.	**Incapacidad de Respuesta Automatizada:** La falta de herramientas de orquestación obligó a una desconexión manual total ("botonazo"), afectando la disponibilidad.

Noviembre 2019 (Post-Ataque)	**Consecuencias Operativas**	Colapso de sistemas de facturación y logística. Se recurre a procesos manuales ("papel y lápiz") para el despacho de combustible, generando retrasos en la cadena de suministro.	**Dependencia IT/OT:** La caída de la red administrativa afectó la operación física, demostrando la falta de planes de continuidad de negocio (BCP) efectivos.

Fase 2. Análisis técnico, impacto económico y estratégico

Contexto general del ataque:

En noviembre del 2019, el panorama digital de México cambió drásticamente cuando PEMEX (Petróleos Mexicanos), el gigante estatal y columna vertebral de la economia nacional, se convirtió en el balcno de una ataque de ransomware sin precedentes. No fue un tropiezo accidente; fue una operación quirúrgica que aprovechó años de negligencia estructural.

Antes del impacto, la situación tecnológica de la paraestatal era un ecosistema de contrastes. Mientras se manejaban activos de miles de millones de dólares, la “casa digital” presentaba grietas profundas:

Componente	Estado Pre-Incidente	Impacto en el Ataque
Sistemas Operativos	Uso masivo de Windows 7 y Server 2003 (sin soporte).	Facilitó la ejecución de exploits antiguos.
Protección Endpoint	16.4% de los equipos carecían de antivirus avanzado (ATP).	Permitió que el malware pasará inadvertido (*Dwell Time*).
Segmentación de Red	Red plana (sin divisiones entre áreas).	El virus se propagó como fuego en pasto seco de IT a Logística.

El éxito de los atacantes no se debió a una gran tecnología avanzada si no a una combinación de tres factores que se alinearon de forma catastrófica:

1. La falla técnica : el “parche” olvidado
   La puerta de entrada fue, irónicamente, una vulnerabilidad ya muy conocida. Seis meses antes, Microsoft había lanzado el parche para el **CVE-2019-0604**

(SharePoint). Pemex, por falta de una política estricta de *Patch Management*, ignoró la actualización. Los atacantes no tuvieron que "romper" la cerradura; simplemente usaron una llave que Pemex dejó puesta en la puerta.

2. La Falla Humana: El Eslabón de Confianza
   Aunque el vector técnico fue SharePoint, se sospecha de campañas de Spearphishing dirigidas a empleados con altos privilegios. En un entorno donde la concientización sobre ciberseguridad era secundaria, un solo clic en un correo malicioso bastó para entregar las credenciales de administrador de dominio, permitiendo que el grupo INDRIK SPIDER se moviera como "dueño de la casa".

   La Falla Política: Austeridad vs. Resiliencia
   A nivel organizacional, la ciberseguridad no era vista como una prioridad estratégica, sino como un gasto administrativo.

   "La falta de un Plan de Continuidad de Negocio (BCP) actualizado y los recortes en el presupuesto de TI dejaron a los ingenieros sin herramientas de respuesta automatizada, obligándolos a recurrir al famoso 'botonazo' (desconexión física de servidores) para frenar el avance del ransomware."

Tabla tecnica del ataque:

Elemento	Descripción
Tipo de ataque	Ransomware bajo la modalidad de "Big Game Hunting" y Doble Extorsión.
Actor o grupo atacante	Grupo criminal **INDRIK SPIDER**.
Vector de entrada	Explotación de vulnerabilidad web en servidores expuestos o campañas de Spearphishing dirigidas.
Vulnerabilidad explotada	**CVE-2019-0604**: Ejecución Remota de Código (RCE) en Microsoft SharePoint.
Etapas del ataque (MITRE ATT&CK)	1. **Acceso Inicial:** Explotación de SharePoint. 2. **Persistencia y Movimiento Lateral:** Uso de Mimikatz y Cobalt Strike. 3. **Ejecución e Impacto:** Despliegue masivo del ransomware DoppelPaymer.

Sistemas comprometidos	Más de **11,000 activos informáticos**, incluyendo servidores centrales, sistemas administrativos, de facturación y estaciones de trabajo.
Duración del incidente	Desde la intrusión inicial (septiembre/octubre 2019) hasta la detonación masiva el 10 de noviembre de 2019.
Mecanismos de detección y respuesta	**Respuesta Manual:** Desconexión total de la red ("botonazo") para contener la propagación ante la falta de orquestación automatizada.

Evaluación del impacto

En el marco de análisis del ataque cibernético sufrido por PEMEX en noviembre de 2019 resulta esencial evaluar sus consecuencias bajo el estándar CIA (confidencialidad, integridad y Disponibilidad), el cual permite dimensionar de manera estructurada el impacto sobre los activos de información críticos de la organización. Esta metodología facilita identificar qué aspectos fueron más vulnerados, cómo se comprometió la operación y qué riesgos se derivan para la continuidad de sus labores regulares, ofreciendo una visión clara y sistemática del alcance del incidente.

Principio	Descripción del Impacto	Evidencia del caso
Confidencialidad	Exposición de información y documentos confidenciales de la empresa.	Amenaza pública por parte del grupo criminal de publicar los datos comprometidos en la Deep Web
Integridad	Base de datos principal vulnerada, alrededor de un 5% de la red de PEMEX fue comprometida, lo que equivale a alrededor de 10,000 equipos de cómputo, una gran cantidad de documentos sensibles expuestos o comprometidos.	El 12 de noviembre de 2019 PEMEX realiza un comunicado oficial admitiendo el ciberataque sufrido, mencionando el cifrado de archivos y el bloqueo de acceso a sus sistemas.
Disponibilidad	Pedidos por parte de empresarios inhabilitados, terminales de almacenamiento y distribución inmovilizadas e imposibilidad de acceso al sistema de información logístico.	Los sistemas logísticos de PEMEX y sus terminales de despacho y almacenamiento se vieron paralizadas tras el ciberataque.

Calculo de costos del ciberataque:

Tipo de Costo	Descripción	Estimación (MXN)
Pérdidas operativas	Días de inactividad, cancelación de operaciones o servicios.	Pérdida por ineficiencia logística: $574.82 - $766.42 millones de pesos. Ventas no realizadas: $229.92 - $383.2 millones de pesos Horas hombre perdidas: $95.8 - $153.28 millones de pesos
Daños reputacionales	Pérdida de clientes, caída en el valor de acciones, pérdida de confianza.	En campañas públicas y comunicación de crisis: $38.32 - $95.8 millones de pesos. Filtración de datos y pérdida de contratos: ~$478.99 millones de pesos (A día de hoy se le conoce como “la mancha”).
Costos técnicos	Recuperación de sistemas, consultorías externas, reemplazo de equipos	Formateo y/o reinstalación de equipo: ~$47.9 millones de pesos Forensia digital.$9.58 - $ 28.75 millones de pesos Licencias y parches de seguridad (con empresas como SAP e IBM): $929.26 millones de pesos
Costos legales / regulatorios	Multas, demandas o sanciones por incumplimiento (GDPR, ISO, etc.)	Peritajes y defensas jurídicas: $28.75 - $57.53 millones de pesos. Retrasos con proveedores: $95.80 - 191.60 millones de pesos. Auditorías de cumplimiento (Compliance): ~$38.32 millones de pesos.
Pago de rescate o extorsión	En caso de ransomware, monto pagado o solicitado	$93.23 millones de pesos.
Total Estimado	Suma total en pesos Mexicanos (MXN)	$2,567.46 - $3,170.98 millones de pesos mexicanos

Los datos de la tabla están basados en el valor del dólar en el año 2019 (19.16 MXN por dólar) publicado por el el Banco de México 2 días antes) por lo que haciendo la transformación a la actualidad (17.27 MXN por dólar) sería un aproximado de entre $2,314.15 millones y $2,858.11 millones de pesos, una “baja” en cuanto al cambio del dólar se refiere. Por otro lado, el costo del rescate es otra historia, ya que el costo exacto (encontrado por analistas de ciberseguridad en foros dentro de la “Web oscura”) indica que el precio del rescate era de 565 bitcoins, que a fecha del 10 de noviembre

del año 2019 significaban un valor de ~$165 mil pesos por bitcoin, pero a día de hoy 1 bitcoin está valuado en $1.43 millones de pesos, por lo que el precio total del rescate a día de hoy sería de ~$805.95 millones de pesos mexicanos.

Relación con marcos normativos:

ISO 27001 – Controles Relevantes y Prevención

La norma ISO 27001 define un SGSI (Sistema de Gestión de Seguridad de la Información) con controles aplicables a amenazas como ransomware.

Controles Específicos:

- **A.12.2.1 – Controles ante código malicioso**
  Relevancia: Implica medidas de protección contra software malicioso (antivirus, bloqueo de malware y escaneo), lo que puede impedir que ransomware como DoppelPaymer se instale y se ejecute.
  Prevención en Pemex: Si Pemex hubiera implementado y monitoreado este control de forma continua, el malware podría haber sido detectado antes de cifrar datos.

- **A.12.3.1 – Gestión de respaldos**
  Relevancia: Asegura que existan copias de respaldo frecuentes, lo que reduce la necesidad de pagar rescates.
  Mitigación: En caso de ataque, tener respaldos aislados hubiera permitido restaurar sistemas sin pagar ni depender de recuperación forense complicada.

- **A.9 – Control de acceso**
  Relevancia: Limita acceso a sistemas solo a personal autorizado y con el principio de menor privilegio.
  Prevención: El incidente pudo haberse iniciado con credenciales comprometidas; controles de acceso más estrictos (incluyendo MFA) hubieran dificultado el uso de credenciales robadas para propagación.

- **A.16 – Gestión de incidentes de seguridad**
  Relevancia: Define procesos para detectar, reportar, evaluar y responder ante incidentes.
  Mitigación: Una respuesta rápida y organizada habría contenido el impacto y reducido tiempo de exposición.

NIST Cybersecurity Framework (CSF) – Aplicación al Caso

El NIST CSF centra la gestión de riesgo de ciberseguridad en cinco funciones clave: Identify, Protect, Detect, Respond y Recover.

Funciones Relacionadas con un Ransomware como DoppelPaymer:

- **Identify (ID)**
  Control: Inventario de activos y evaluación de vulnerabilidades.
  Prevención: Si Pemex hubiera identificado sistemas críticos no actualizados, podrían aplicarse parches y reducir superficies de ataque.

- **Protect (PR)**
  Controles: Gestión de identidad, segmentación de red, políticas de acceso.
  Prevención: Segmentar redes (por ejemplo, separar IT administrativa de redes de producción) hubiera limitado la propagación del ransomware.

- **Detect (DE)**
  Controles: Monitoreo de anomalías y detección de malware.
  Prevención: Un sistema de detección de intrusiones (IDS) o SIEM podría haber alertado antes de que el ransomware se ejecutara en múltiples endpoints.

- **Respond (RS)**
  Controles: Plan de respuesta a incidentes y comunicación.
  Mitigación: Planes bien ensayados de respuesta habrían contenido la infección y asegurado actuación coordinada interna y con autoridades.

- **Recover (RC)**
  Controles: Planes de recuperación de sistemas.
  Mitigación: Estrategias de recuperación resilientes (por ejemplo, restauración desde respaldo seguro) reducen impactos operacionales y económicos.

GDPR – Consideraciones de Protección de Datos (Aunque México no aplica directamente)

Aunque el GDPR es una regulación europea de protección de datos personales, incluye principios que son útiles como buenas prácticas:

- **Principio de Seguridad (Art. 32)**
  Requiere: Implementar medidas técnicas y organizativas apropiadas para proteger datos personales.
  Relevancia preventiva: Si se tratara de datos personales de EU, GDPR exigiría controles como encriptación, control de acceso y evaluación de riesgo – que coinciden con ISO 27001 y NIST CSF.

- **Notificación de brechas (Art. 33-34)**
  Relevancia: Obliga a notificar a autoridades y titulares de datos en tiempos específicos tras una brecha; esto impulsa transparencia.

Mitigación: Habría mejorado la gestión de incidentes y comunicación post-ataque en Pemex si se siguieran estándares similares, aunque la ley mexicana difiere.

Conclusiones:

Tras el análisis forense y estratégico realizado, se concluye que el ciberataque a Pemex en 2019 no fue un evento fortuito, sino el resultado directo de una deuda técnica acumulada durante años. Este incidente evidenció que operar con sistemas obsoletos y omitir parches de seguridad críticos no representa únicamente un descuido administrativo, sino un riesgo de seguridad nacional capaz de paralizar la operatividad de una infraestructura esencial.

A partir de este caso, se identifican tres lecciones fundamentales:
La ciberseguridad no es un gasto, sino una garantía de continuidad operativa: Las pérdidas multimillonarias derivadas de la interrupción logística superaron ampliamente cualquier inversión preventiva que pudo haberse destinado a actualizaciones, licencias y medidas de protección.

La desconexión manual no constituye una estrategia sostenible: El llamado “botonazo” reflejó una preocupante ausencia de planes de respuesta automatizada. En un entorno moderno, la resiliencia debe formar parte integral de la arquitectura de red y no depender de acciones humanas improvisadas ante una crisis.

Gobernanza por encima de la tecnología: Más allá del malware DoppelPaymer, la vulnerabilidad principal residió en la falta de una cultura de gestión de riesgos respaldada por marcos internacionales como ISO y NIST, esenciales para una ciberseguridad estructurada y preventiva.

Referencias:

NIST (Gestión de riesgo de ransomware y CSF):
Fisher, B., Souppaya, M., Scarfone, K., & Barker, W. (2022). Ransomware Risk Management: A Cybersecurity Framework Profile (Spanish translation). NIST International Cybersecurity and Privacy Resources. https://doi.org/10.6028/NIST.IR.8374.spa

GDPR (Seguridad del procesamiento de datos personales):
Regulation (EU) 2016/679 of the European Parliament and of the Council. (2016). General Data Protection Regulation (GDPR), Art. 32: Security of processing. https://gdpr-info.eu/art-32-gdpr/

ISO/IEC 27001 (Norma de gestión de seguridad de la información):
ISO/IEC 27001. (2022). Information technology – Security techniques – Information security management systems – Requirements. International Organization for Standardization/International Electrotechnical Commission. (visto en Wikipedia).

INCIBE (Instituto Nacional de Ciberseguridad):
INCIBE-CERT. (2019, noviembre 12). La petrolera PEMEX sufrió un ciberataque de ransomware. Instituto Nacional de Ciberseguridad (INCIBE). https://www.incibe.es/incibe-cert/publicaciones/bitacora-de-seguridad/petrolera-pemex-sufrio-ciberataque-ransomware

ZEPO (Foro Web):
Enrique Holgado. (2023, 26 de julio), Información útil - Tipos de ciberataques - Ciberataque a Pemex: lecciones sobre la protección de datos en una era digital.
https://zepo.app/ciberataque-a-pemex-lecciones-sobre-la-proteccion-de-datos-en-una-era-digital/