UNIREMINGTON®
CORPORACIÓN UNIVERSITARIA REMINGTON
RES. 2661 MEN JUNIO 21 DE 1996

TRABAJO DE GRADO
Opción Seminario-Diplomado.

Análisis de ciberseguridad de la EPM

Corporación Universitaria Remington.

Nombre de la facultad: INGENIERÍA

Nombre del programa académico: INGENIERIA EN SISTEMAS

Nombre del Autor: Juan Sebastián ramirez ossa

Nombre del Tutor del trabajo de grado Jorge Leonardo Ramirez Restrepo.

Seminario

2026

Tabla de Contenidos

Resume

El presente informe técnico aplica los fundamentos del seminario de ciberseguridad organizacional al análisis de la empresa pública de Medellín EPM, empresa industrial y comercial del estado colombiano, operadora de infraestructura critica en los sectores energéticos de gas natural y agua potable y telecomunicaciones para más de cuatro millones de usuarios en Colombia y en varios países de latino América. EPM constituye un caso de estudio de alto valor académico, dado que en diciembre de 2022 fue víctima de un ataque de ransomware ejecutado por un grupo criminal llamado BlackCat/ALPHV, el cual comprometió sus sistemas administrativos y digitales interrumpió servicios de atención al cliente y genero la exfiltración de más de 500GB de información confidencial

El análisis se estructuro en tres componentes identificación y clasificación de activos de información evaluación de riesgos mediante una matriz activo, vulnerabilidad impacto y propuesta de controles de seguridad alineados con la ISO/IEC 27001 (ISO, 2013), el NIST y el estándar IEC 62443 para entornos industriales al análisis de la EPM y su condición de infraestructura critica la convierte en un objetivo de alto valor para ransomware y de ciberataque lo cual el ataque que sufrió afecto gravemente sus operaciones administrativos y suspendió su portal web y aplicación móvil y se identificaron ocho activos de información estratégica clasificada en niveles críticos. También se identificaron entre los ocho activos seis de ellos de niveles críticos y altos

Entre ellos los sistemas de SCADA/ICS, el ERP corporativo SAP y los centros de datos propios. Se construyo una matriz de riesgos de ocho amenazas priorizadas, siendo el ransomware sobre seguridad alineados con ISO/IEC 27001, NIST e IEC 62443 destacando la segmentación de redes OT/IT, la evidencia que la EPM ha fortalecido su postura de seguridad tras su incidente,

pero persiste brechas críticas en la convergencia OT/IT y en la cultura organizacional de ciberseguridad.

Según la ISO (2013), la gestión de riesgos permite proteger los activos críticos de una organización.

La convergencia OT/IT incrementa la superficie de ataque en infraestructuras críticas (IEC, 2013).

El framework NIST (2018) establece funciones esenciales para la gestión de incidentes de ciberseguridad.

La Ley 1581 de 2012 regula la protección de datos personales en Colombia (Congreso de Colombia, 2012).

Los ataques de ransomware representan una amenaza creciente para las infraestructuras críticas (IBM Security, 2024).

Palabras clave: ISO 27001, BlackCat/ALPVH, SCADA/ICS IEC 62443 ciberseguridad OT/IT, gestión de riesgos, infraestructura critica, EPM

Marco conceptual y contextual

1. Marco conceptual

La ciberseguridad organizacional es un conjunto de políticas, procesos y tecnologías que implementa para proteger la confidencialidad, integridad y disponibilidad de sus activos frente amenazas internas y externas. Un activo de información es cualquier recurso con valor estratégico cuya pérdida, alteración o divulgación no autorizada generaría un impacto operativo, legal o reputacional. Una amenaza es cualquier evento potencial capaz de explotar una vulnerabilidad y causar daño, el riesgo se cuantifica mediante la formula riesgo igual a probabilidad en una escala de 1 a 5, lo que permite priorizar los esfuerzos de protección Un control de seguridad es cualquier medida técnica, administrativa u organizativa orientada a reducir dichos riesgos lo que la Confidencialidad, integrada y disponible de los activos de la infraestructura critica como la EPM esta diciplina adquiere una dimensión adicional de la OT que incluye los sistemas de control industrial ICS y las redes SCADA responsables de gestión de procesos físicos como la generación de energía la distribución de gas y el tratamiento del agua potable.

La OT/IT es decir la integración progresiva de los sistemas de control

industrial con las redes corporativas de tecnología de información han multiplicado los ataques a las empresas de infraestructura mientras que los entornos IT pueden actualizar diseñados para funcionar durante décadas lo que dificulta que se creen vulnerabilidades estructurales de difícil resolución

El estándar de la ISO 27001 de 2013 establece los requisitos para la implementación de un sistema de gestión de seguridad de información

proporcionando un marco de referencia para la gestión de riesgos y dando controles de seguridad complementario, el framework NIST CSF del instituto nacional de estándares de y tecnología de estados unidos ofrece gua practica industriales, el estándar IEC 62443 define requisitos específicos de seguridad para sistemas de control y automatización industrial.

En la ley 1581 de 2012 regula el tratamiento de datos personales y establece los principios de legalidad, finalidad y seguridad en el manejo de información de ciudadanos por incumplimiento responsable de su vigilancia y puede imponer sanciones económicas por el incumplimiento regulatorios la comisión de energía y gas estableciendo requisitos específicos para los operadores del sector energético

Desarrollo e implementación del aprendizaje

1.2. Marco contextual: La EPM

La EPM es una empresa industrial y comercial del estado, fundada en 1955 y con sedes en Medellín Antioquia. Es propiedad del municipio de Medellín y constituye uno de los grupos empresariales de servicios públicos más grandes e importantes de latino América. La EPM opera en los sectores de energía de gas y de agua potable, saneamiento y telecomunicaciones a través de su afiliar UNE con presencia en Colombia Guatemala el salvador Panamá chile y Brasil.

La empresa presta servicios a más de 4 millones de personas en Colombia y su capacidad de generación eléctrica supera 3.500 MW su compleja infraestructura tecnológica, opera plantas hidroeléctricas, termoeléctricas y energías renovables

como también redes de distribución de gas natural que cubre múltiples departamentos, sistema de acueductos y alcantarillado para el área metropolitana del valle de aburra y una red de telecomunicaciones con más de un millón de clientes a través de UNE.

En diciembre de 2022, EPM fue víctima de un ciberataque de ransomware ejecutado por el grupo criminal BlackCat/ALPHV. El ataque comprometió los sistemas administrativos y digitales de la empresa fueron forzados a la suspensión temporal del portal web de control operacional y la aplicación web y varios servicios no se vieron afectados por el ataque y expuso, vulnerabilidades de la OT/IT y puso en evidencia la necesidad de fortalecer la seguridad de la organización el grupo afirma haber infiltrado más de 500GB lo que llevaría a la EPM activo protocolos de emergencia esto obligo a la empresa a gestionar pagos y servicios de manera virtual durante la contingencia.

Este antecedente real convierte hace que la EPM se vuelva un caso de estudio de alto valor académico y profesional pues nos permite ver los controles de seguridad existente con las vulnerabilidades la empresa que fueron explotadas y propone hacer cambios y mejorar basada en la evidencia anterior.

2. Desarrollo del aprendizaje e implementación

2.1. identificación de activos

Con base en las normas ISO/IEC 27001 considerando la naturaleza de la OT/IT de la EPM se identificaron seis activos de información estratégicos clasificada según se criticidad los sistemas SCADA/ICS fueron catalogados como críticos dado a

su compromiso afectaría el suministro de servicios esenciales en la gestión financiera y de recursos humanos. Los centros de datos de clientes contienen datos personales protegidos por la ley 1581 de 2012. El portal web y la aplicación móvil fueron afectados durante el ataque de 2022. La tabla 1 presenta el inventario de los activos identificados y la información potencial que la perdida de datos y la alteración de estos y la indisponibilidad y la protección de la información de los clientes.

Tabla 1

Activos de información de EPM

ACTIVO DE INFORMACION	DESCRIPCION
SISTEMAS DE INFORMACION TECNICA.	Datos de redes de acueductos alcantarillas y distribución de energía (SDL, STR, STN) y redes de gas.
ERP corporativa	Plataforma de gestión financiera y de recursos humanos y contables
Redes de fibra óptica y telecomunicaciones	Infraestructura de conectividad de UNE de servicios corporativos
Base de datos de usuarios y de facturación	Datos personales y contractuales de más de 4 millones de personas
Data centers	Infraestructuras físicas que alojan los sistemas de la organización
Directorio activo	Sistema de comunicación interna y gestión de identidades
Información financiera	Reportes, presupuestos y proyectos financieros

Nota. Los activos fueron identificados con base a la estructura operativa de la EPM y clasificados según su criticidad conforme a ISO/IEC 27001 (ISO, 2013)

Lo centros de datos son activos de mayor criticidad desde la perspectiva de seguridad nacional, dada que su compromiso podría afectar el suministro de energía de agua y de gas afectando a

millones de colombianos en muchos municipios. El ERP corporativo centra la información financiera y de gestión de recursos humanos de toda la organización mientras la base de datos contiene información de los usuarios registrados, protegidos por la ley 1581 de 2012.

2.2. Análisis de amenazas

La evaluación de riesgos se realizó mediante el método cuantitativo asignando valores de probabilidad de amenazas del 1 a 5 donde se representa el nivel mínimo con 1 y el máximo con 5 y el control propuesto. el análisis tomo como referencia al antecedente real del ataque de ransomware de diciembre de 2022

Tabla 2

Matriz de amenazas, vulnerabilidades y controles propuestos para la EPM

Amenazas y vulnerabilidad	Probabilidad	Control propuesto
Ransomware dirigido a la infraestructura (caso BlackCat)	5	Backup offline segmentación OT/IT EDR avanzado
Acceso no autorizado al sistema	4	Aislamiento de red OT. MFA monitorear por 24 horas
Fuga masiva de datos de clientes (habeas data)	3	Cifrado AES-256, DPL
Phishing	5	Capacitación simulaciones filtros activos
Acceso indebido de terceros a la red interna	3	Segmentación de red con VPN con MFA

Nota. La probabilidad se cuantifica en la escala de 1 a 5, donde 1 es el mínimo de amenaza y 5 el máximo de amenaza. Los controles propuestos están alineados con ISO /IEC 27001, NIST CSF e IEC62443

La evaluación de riesgos relacionados por cada activo con su amenaza principal, la vulnerabilidad explotable y el riesgo resultante con forme a ISO/IEC 27001 ISO, 2013 y el NIST. El ransomware sobre la infraestructura critica alcanzo puntuación máxima 25/25 dado a la red sin segmentación permitió la propagación lateral de malware tal como ocurrió en el incidente de BlackCat/ALPHV. El acceso no autorizado a SCADA se asocia a la convergencia OT/IT sin controles diferenciados. La fuga de datos de los clientes se vincula al almacenamiento sin cifrado, vulnerando, el phishing tiene probabilidad máxima por ausencia de capacitación El análisis revela que EPM enfrenta riesgos en nivel crítico y cuatro niveles altos configurando el panorama de amenazas que se enfrenta son de alta complejidad la puntuación de ransomware sobre la infraestructura no es teórica, es información real del incidente de 2022 lo que da posibilidad de recurrencia a nivel máximo mirando el vector de ataque ya fue explotado sus vulnerabilidades de la empresa y su infraestructura.

2.3. Lecciones aprendidas del incidente real

Propuesta de controles y política de seguridad, los controles propuestos responden directamente a las vulnerabilidades identificadas y que se alineen con ISO/IEC 27001, el NIST CSF e IEC 62443. La segmentación de redes OT/IT

mediante zonas de aislamiento para los sistemas SCADA/ICS es el control más urgente pues habría limitado la propagación del ransomware en 2022. La autentificación multifactor MFA en sistemas críticos reduce el acceso no autorizado los backups cifrados offline con verificación trimestral asegura una recuperación sin pagar rescate.

La construcción de cultura organizacional en ciberseguridad convierte a cada empleado en una línea de defensa activa lo aprendido del incidente real del 2022. El ataque que sufrió el EPM EN diciembre constituyo una fuente invaluable de información para la gestión de la seguridad. A continuación, un análisis de los factores que contribuyo al éxito del ataque y las mejoras que derivan de cada uno

Tabla 3

Analisis de lecciones aprendidas del ataque de ransomware Blakcat/ALPHV en la EPM (2022)

Factor incidente	Impacto identificado	Mejoras propuestas
Propagación lateral por red corporativa	El ransomware se extendió a múltiples sistemas por mucho tiempo	Microsegmentación y arquitectura Zero trust
Tiempo de detección de ataques tardíos	El ataque opero de forma encubierta antes de cifrar	SIEM con detección de comportamiento anómalo
Acceso de terceros sin monitoreo adecuado	Vector de entrada inicial no controlado	Asegurar los permisos y revisar si están autorizados

Nota. Cada factor extraído del análisis forense del ataque real del 2022. Las propuestas dadas se alinean con los marcos ISO/IEC 27001, NIST CSF Y LA arquitectura Zero Trust.

El incidente ilustra la tendencia global que tienden las empresas de infraestructura se han convertido en el objetivo favorito del ransoware de doble extorsión precisamente porque la presión de servicios esenciales aumenta la probabilidad de pago del rescate la propuesta adecuada no es el pago, sino la construcción de capacidades de resiliencia que permita recuperar las operaciones sin ceder ante criminales.

Conclusiones

- La EPM representa un caso de estudio en campo de ciberseguridad organizacional pues combina la complejidad de los entornos de infraestructura critica con el antecedente de un ataque de ransoware real y de alto impacto. El análisis realizado demuestra conceptos teóricos del seminario una gestión de activos una evaluación de riesgos y diseño de controles tienen aplicaciones directa y urgente en organizaciones con esta naturaleza.
- La matriz de riesgos de amenazas en un nivel crítico y cuatro de nivel alto con el ransoware sobre su infraestructura critica. La validación empírica de este riesgo mediante el incidente real de 2022 pide con urgencia de implementar los controles propuestos especialmente el OT/IT, los backups offline y la autenticación multifactor.
- La elaboración de este informe me permitió aplicar contenidos del seminario de ciberseguridad organizacional con un caso real en Colombia fortaleciendo

el análisis de riesgos diseño de controles y aplicaciones de marcos normativos internacionales

REFERENCIAS

(ISO., International Organization for Standardization. (2013). ISO/IEC 27001:2013 — Information security management systems — Requirements. ISO.)

(IEC., International Electrotechnical Commission. (2013). IEC 62443 — Security for industrial automation and control systems. IEC.)

(National Institute of Standards and Technology.) (2018). Framework for Improving Critical Infrastructure Cybersecurity (Version 1.1). NIST.)

(2012, Congreso de Colombia. (2012). Ley 1581 de 2012) (Disposiciones generales para la protección de datos personales.)

International Organization for Standardization. (2013). ISO/IEC 27001:2013 Information security management systems — Requirements. ISO.

International Electrotechnical Commission. (2013). IEC 62443 Security for industrial automation and control systems. IEC.

National Institute of Standards and Technology. (2018). Framework for improving critical infrastructure cybersecurity (Version 1.1). NIST.

Congreso de Colombia. (2012). Ley 1581 de 2012: Protección de datos personales.

IBM Security. (2024). Cost of a data breach report 2024. IBM.

Cisco. (2023). Cybersecurity for critical infrastructure. Cisco.

Microsoft Security. (2024). Ransomware defense best practices. Microsoft.

Empresas Públicas de Medellín. (2023). Comunicados oficiales sobre incidentes tecnológicos.

EPM.