NOMBRE DEL TRABAJO

**Luis ayasta_ Suficiencia_ modificado fin al v_40.pdf**

AUTOR

**Luis Fernando Ayasta Portocarrero**

RECUENTO DE PALABRAS

**11619 Words**

RECUENTO DE CARACTERES

**72014 Characters**

RECUENTO DE PÁGINAS

**63 Pages**

TAMAÑO DEL ARCHIVO

**1.5MB**

FECHA DE ENTREGA

**Feb 27, 2024 7:25 PM GMT-5**

FECHA DEL INFORME

**Feb 27, 2024 7:26 PM GMT-5**

## 22% de similitud general

El total combinado de todas las coincidencias, incluidas las fuentes superpuestas, para cada base de datos.

- 22% Base de datos de Internet
- 2% Base de datos de publicaciones
- Base de datos de Crossref
- Base de datos de contenido publicado de Crossref
- 0% Base de datos de trabajos entregados

## Excluir del Reporte de Similitud

- Material bibliográfico

UNTELS | UNIVERSIDAD NACIONAL TECNOLÓGICA DE LIMA SUR

# FORMULARIO DE AUTORIZACIÓN PARA LA PUBLICACIÓN DE TRABAJOS DE INVESTIGACIÓN EN EL REPOSITORIO INSTITUCIONAL DE LA UNTELS

**(Art. 45° de la ley N° 30220 – Ley)**

Autorización de la propiedad intelectual del autor para la publicación de tesis en el Repositorio Institucional de la Universidad Nacional Tecnológica de Lima Sur (https://repositorio.untels.edu.pe), de conformidad con el Decreto Legislativo N° 822, sobre la Ley de los Derechos de Autor, Ley N° 30035 del Repositorio Nacional Digital de Ciencia, Tecnología e Innovación de Acceso Abierto, Art. 10° del Rgto. Nacional de Trabajos de Investigación para optar grados académicos y títulos profesionales en las universidades – RENATI Res. N° 084-2022-SUNEDU/CD, publicado en El Peruano el 16 de agosto de 2022; y la RCO N° 061-2023-UNTELS del 01 marzo 2023.

## TIPO DE TRABAJO DE INVESTIGACIÓN

1). TESIS ( ) 2). TRABAJO DE SUFICIENCIA PROFESIONAL (X)

## DATOS PERSONALES

| | |
|---|---|
| Apellidos y Nombres: | Ayasta Portocarrero Luis Fernando |
| D.N.I.: | 71902485 |
| Otro Documento: | |
| Nacionalidad: | Peruana |
| Teléfono: | 915351486 |
| e-mail: | 2015100190@untels.edu.pe |

## DATOS ACADÉMICOS

**Pregrado**

| | |
|---|---|
| Facultad: | Facultad de Ingeniería y Gestión |
| Programa Académico: | Trabajo de Suficiencia Profesional |
| Título Profesional otorgado: | Ingeniero Electrónico y Telecomunicaciones |

**Postgrado**

| | |
|---|---|
| Universidad de Procedencia: | |
| País: | |
| Grado Académico otorgado: | |

**Datos de trabajo de investigación**

| | |
|---|---|
| Título: | Implementación de un Sistema de Encriptación con Tecnología Bitlocker para reforzar la seguridad y la prevención de pérdida de datos (DLP) en una empresa de ventas. |
| Fecha de Sustentación: | 17 de diciembre de 2023 |
| Calificación: | Aprobado por unanimidad |
| Año de Publicación: | 2024 |

UNTELS | UNIVERSIDAD NACIONAL TECNOLÓGICA DE LIMA SUR

## AUTORIZACIÓN DE PUBLICACIÓN EN VERSIÓN ELECTRÓNICA

A través de la presente, autorizo la publicación del texto completo de la tesis, en el Repositorio Institucional de la UNTELS especificando los siguientes términos:

Marcar con una X su elección.

1) Usted otorga una licencia especial para publicación de obras en el REPOSITORIO INSTITUCIONAL DE LA UNIVERSIDAD NACIONAL TECNOLÓGICA DE LIMA SUR.

Si autorizo _____ No autorizo _X_

2) Usted autoriza para que la obra sea puesta a disposición del público conservando los derechos de autor y para ello se elige el siguiente tipo de acceso.

| Derechos de autor | | |
|---|---|---|
| TIPO DE ACCESO | ATRIBUCIONES DE ACCESO | ELECCIÓN |
| ACCESO ABIERTO 12.1(*) | **info:eu-repo/semantics/openAccess** (Para documentos en acceso abierto) | ( ) |

3) Si usted dispone de una **PATENTE** puede elegir el tipo de **ACCESO RESTRINGIDO** como derecho de autor y en el marco de confiabilidad dispuesto por los numerales 5.2 y 6.7 de la directiva Nº 004-2016-CONCYTEC DEGC que regula el Repositorio Nacional Digital de CONCYTEC (Se colgará únicamente datos del autor y el resumen del trabajo de investigación).

| Derechos de autor | | |
|---|---|---|
| TIPO DE ACCESO | ATRIBUCIONES DE ACCESO | ELECCIÓN |
| ACCESO RESTRINGIDO | **info:eu-repo/semantics/restrictedAccess** (Para documentos restringidos) | (X) |
| | **info:eu-repo/semantics/embargoedAccess** (Para documentos con períodos de embargo. Se debe especificar las fechas de embargo) | ( ) |
| | **info:eu-repo/semantics/closedAccess** (para documentos confidenciales) | ( ) |

(*) http://renati.sunedu.gob.pe

UNTELS | UNIVERSIDAD NACIONAL TECNOLÓGICA DE LIMA SUR

**Rellene la siguiente información si su trabajo de investigación es de acceso restringido:**

**Atribuciones de acceso restringido:**

info:eu-repo/semantics/openAccess

Motivos de la elección del acceso restringido:

El motivo de la restricción es porque hay datos de la empresa que son confidenciales y no pueden ser públicos

Ayanta Portocarrero Luis Fernando

APELLIDOS Y NOMBRES

71902485

DNI

Firma y huella:

Lima, 17 de enero del 2024

# UNIVERSIDAD NACIONAL TECNOLÓGICA DE LIMA SUR

**FACULTAD DE INGENIERÍA Y GESTIÓN**
ESCUELA PROFESIONAL DE INGENIERÍA ELECTRÓNICA Y TELECOMUNICACIONES

# “IMPLEMENTACIÓN DE UN SISTEMA DE ENCRIPTACIÓN CON TECNOLOGÍA BITLOCKER PARA REFORZAR LA SEGURIDAD Y LA PREVENCIÓN DE PÉRDIDA DE DATOS (DLP) EN UNA EMPRESA DE VENTAS”

**TRABAJO DE SUFICIENCIA PROFESIONAL**
Para optar el Título Profesional de

**INGENIERO ELECTRÓNICO Y TELECOMUNICACIONES**

**PRESENTADO POR EL BACHILLER**

AYASTA PORTOCARRERO, LUIS FERNANDO
ORCID: 0009-0005-2376-7196

**ASESOR**
YAURI RODRÍGUEZ, RICARDO
ORCID: 0000-0001-9884-9317

**Villa El Salvador**
**2023**

UNIVERSIDAD NACIONAL
TECNOLÓGICA DE LIMA SUR

"Año de la unidad, la paz y el desarrollo"

**VI Programa de Titulación por la Modalidad de Trabajo de SuficienciaProfesional**
**Decanato de la Facultad de Ingeniería y Gestión**

# ACTA DE SUSTENTACIÓN DE TRABAJO DE SUFICIENCIA PROFESIONAL PARA OBTENER EL TÍTULO PROFESIONAL DE INGENIERO ELECTRÓNICO Y TELECOMUNICACIONES

En Villa El Salvador, siendo las 17:02 horas del día 17 de diciembre de 2023, se reunieron en las instalaciones de la Universidad Nacional Tecnológica de Lima Sur, los miembros del Jurado Evaluador del Trabajo de Suficiencia Profesional integrado por:

| | | | |
|---|---|---|---|
| Presidente | : | MG. JOSÉ AMBROSIO MACHUCA MINES | CIP Nº 158894 |
| Secretario | : | MG. DANIEL LÉVANO RODRIGUEZ | CIP Nº 155059 |
| Vocal | : | DR. JULIO ENRIQUE QUISPE TUESTA | CIP Nº 150139 |

Designados con Resolución de Decanato de la Facultad de Ingeniería y Gestión N° 984-2023-UNTELS-R-D de fecha 13 de diciembre del 2023.

Se da inició al acto público de sustentación y evaluación del Trabajo de Suficiencia Profesional, para obtener el Título Profesional de Ingeniero Electrónico y Telecomunicaciones, bajo la modalidad de Titulación por Trabajo de Suficiencia Profesional (Resolución de Consejo Universitario Nº 065-2023-UNTELS-CU de fecha 08 de agosto del 2023), en la cual se APRUEBA el "Reglamento, Directiva, Cronograma y Presupuesto del VI Programa de Titulación por la Modalidad de Trabajo de Suficiencia Profesional de la Universidad Nacional Tecnológica de Lima Sur" ; siendo que el Art. 4º del precitado Reglamento establece que: **"La Modalidad de Titulación prevista consiste en la presentación, aprobación y sustentación de un Trabajo deSuficiencia Profesional que dé cuenta de la experiencia profesional y además permita demostrar el logro de las competencias adquiridas en el desarrollo de los estudios de pregrado que califican para el ejercicio de la profesión correspondiente. Quienes participen en esta modalidad no podrán tramitar simultáneamente otrasmodalidades de titulación. Además, los participantes inscritos en esta modalidad, deberán acreditar un mínimo de dos (02) años de experiencia laboral, de acuerdo a lo establecido en la Resolución Nº 174-2019- SUNEDU/CD y al anexo 1 sobre Glosario de Términos en el punto veinte (20)..."**, en el cual;

El Bachiller **LUIS FERNANDO AYASTA PORTOCARRERO**
Sustentó su Trabajo de Suficiencia Profesional: **IMPLEMENTACIÓN DE UN SISTEMA DE ENCRIPTACIÓN CON TECNOLOGÍA BITLOCKER PARA REFORZAR LA SEGURIDAD Y LA PREVENCIÓN DE PÉRDIDA DE DATOS (DLP) EN UNA EMPRESA DE VENTAS**

Concluida la Sustentación del Trabajo de Suficiencia Profesional, se procedió a la calificación correspondiente según el siguiente detalle:

Condición Aprobado por unanimidad Equivalencia Bueno de acuerdo al Art. 65º del Reglamento General para el Otorgamiento de Grado Académico y Título Profesional de la UNTELS vigente.

Siendo las 17:25 horas del día 17 de diciembre de 2023 se dio por concluido el acto de sustentación del Trabajo de Suficiencia Profesional, firmando la presente acta los miembros del Jurado.

PRESIDENTE
MG. JOSÉ AMBROSIO MACHUCA MINES
CIP N° 158894

SECRETARIO
MG. DANIEL LÉVANO RODRIGUEZ
CIP N° 155059

VOCAL
DR. JULIO ENRIQUE QUISPE TUESTA
CIP N° 150139

Nota: Art. 14°.- La sustentación del Trabajo de Suficiencia Profesional se realizará en un acto público. De faltar algún miembro del Jurado, la sustentación procederá con los dos integrantes presentes. En caso de ausencia delpresidente del jurado, asumirá la presidencia el docente de mayor categoría y antigüedad. En caso de ausencia de dos o más miembros del jurado, la sustentación será reprogramada durante los 05 días siguientes.

## DEDICATORIA

Dedicado a mi amado padre Luis Ayasta Rodriguez Q.E.P.D., mi querida madre Olga Portocarrero Lucho, además, se lo dedico a todas las personas que compartí gratos momentos en mi vida estudiantil, laboral, universitaria y profesional.

**AGRADECIMIENTO**

Un agradecimiento a Dios y a mi familia por brindarme en todo momento su apoyo incondicional.

**ÍNDICE**

*DEDICATORIA* ..... *ii*
*AGRADECIMIENTO* ..... *iii*
*ÍNDICE DE FIGURAS* ..... *vi*
*ÍNDICE DE TABLAS* ..... *viii*
*RESUMEN* ..... *ix*
*INTRODUCCIÓN* ..... *x*
*CAPÍTULO I: ASPECTOS GENERALES* ..... *1*
1.1 Contexto ..... 1
1.2 Delimitación del Proyecto ..... 2
*1.2.1 Espacial* ..... 2
*1.2.2 Temporal* ..... 2
*1.2.3 Teórica* ..... 2
1.3 Objetivos ..... 2
*1.3.1 Objetivo General* ..... 2
*1.3.2 Objetivos Específicos* ..... 2
*CAPÍTULO II: MARCO TEÓRICO* ..... *3*
2.1 Antecedentes ..... 3
*2.1.1 Antecedentes Nacionales* ..... 3
*2.1.2 Antecedentes Internacionales* ..... 4
2.2 Bases Teóricas ..... 6
*2.2.1 Encriptación* ..... 6
*2.2.2 Bitlocker* ..... 13
2.2.3 Tecnología de Trend Micro ..... 14
2.3 Definición de términos básicos ..... 15
*CAPÍTULO III: DESARROLLO DEL TRABAJO PRPOFESIONAL* ..... *18*
3.1 Determinación y Análisis del Problema ..... 18
3.2 Modelo de Solución Propuesto ..... 20
3.2.1 Análisis de Requisitos ..... 21
3.2.2 Determinación de características de accesibilidad ..... 21
3.2.3 Definición de arquitectura ..... 22
3.2.4 Implementación del Servidor ..... 24
3.2.5 Políticas de acceso y autorización ..... 29
3.2.6 Funcionamiento de la solución de encriptación ..... 33
3.3 Resultados ..... 42

*CONCLUSIONES* ..... *46*
*RECOMENDACIONES* ..... *47*
*REFERENCIAS BIBLIOGRÁFICAS* ..... *48*
*ANEXO* ..... *52*

## ÍNDICE DE FIGURAS

***Figura 1*** ..... 7
*Cifrado simétrico*..... 7
***Figura 2*** ..... 8
*Cifrado asimétrico*..... 8
***Figura 3*** ..... 11
*Encriptación de correo electrónico* ..... 11
***Figura 4.*** ..... 19
*Tipos de Ciberataques más usados en Perú en época de pandemia.* ..... 19
***Figura 5.*** ..... 20
*Delitos con mayor incidencia en zonas urbanas de Perú durante el primer semestre de 2023.* ..... 20
***Figura 6*** ..... 23
*Arquitectura de la solución de encriptación.* ..... 23
***Figura 7*** ..... 24
*Creación del servidor PW3004Q* ..... 24
***Figura 8*** ..... 25
*Características hardware del servidor* ..... 25
***Figura 9*** ..... 25
*Configuración de red en el servidor a través de ipconfig*..... 25
***Figura 10*** ..... 27
*Módulos de seguridad de Trend Micro.* ..... 27
***Figura 11*** ..... 28
*Escaneo al servidor PW3004Q utilizando la solución de Tenable.*..... 28
***Figura 12*** ..... 29
*Configuración de IP de un usuario conectado a la VPN*..... 29
***Figura 13*** ..... 30
*Configuración del equipo conectado a la VPN* ..... 30
***Figura 14*** ..... 31
*Creación de regla el Firewall Checkpoint que permite conexión hacia el destino 10.31.1.7* ..... 31
***Figura 15*** ..... 32
*Comando Telnet – Validación puerto* ..... 32
***Figura 16*** ..... 32
*Acceso exitoso mediate Telnet*..... 32

***Figura 17*** ..... 33
*Evidencia de tráfico exitoso hacia el servidor 10.31.1.7* ..... 33
***Figura 18*** ..... 34
*Permisos en la base de datos SQL "MobileArmorLog" del servidor "PW3004Q"* . 34
***Figura 19*** ..... 35
*Permisos en la base de datos SQL "MobileArmorDB" del servidor "PW3004Q"* .. 35
***Figura 20*** ..... 36
*Regla creada en el Firewall desde el servidor hacia el AD* ..... 36
***Figura 21*** ..... 36
*Agente PolicyServer* ..... 36
***Figura 22*** ..... 37
*Servicio del PolicyServer activado* ..... 37
***Figura 23*** ..... 38
*Inicio de sesión del PolicyServer* ..... 38
***Figura 24*** ..... 38
*Configuración de políticas "Full Disk Encryption"* ..... 38
***Figura 25*** ..... 39
*Mensaje de encriptación con Bitlocker en sincronización con el agente PolicyServer* ..... 39
***Figura 26*** ..... 40
*Encriptación exitosa al equipo* ..... 40
***Figura 27*** ..... 41
*Validación de la encriptación bitlocker activada en el equipo del usuario.* ..... 41
***Figura 28*** ..... 42
*Error de conexión por escritorio remoto.* ..... 42
***Figura 29*** ..... 43
*Conexiones activas en el puerto 3389* ..... 43
***Figura 30*** ..... 44
*Evidencia de instalación del PolicyServer MMC* ..... 44
***Figura 31*** ..... 45
*Equipos con encriptación de disco activos y no activos* ..... 45

## ÍNDICE DE TABLAS

***Tabla 1*** ..... *6*
*Ventajas y desventajas del cifrado simétrico* ..... *6*
***Tabla 2*** ..... *8*
*Ventajas y desventajas del cifrado asimétrico* ..... *8*
***Tabla 3*** ..... *10*
*Ventajas y desventajas de la encriptación de correo electrónico* ..... *10*
***Tabla 4*** ..... *11*
*Ventajas y desventajas de la encriptación de almacenamiento en nube* ..... *11*
***Tabla 5*** ..... *22*
*Requisitos de Policy Server* ..... *22*

## RESUMEN

Este proyecto se desarrolló en una empresa de ventas líder en Perú y aborda desafíos significativos de seguridad de datos y prevención de pérdida de información. El problema central radica en la vulnerabilidad de la empresa a brechas de seguridad y fugas de datos debido a la falta de enfoque en el cifrado de disco y DLP en los equipos finales (*endpoints*).

Para abordar este problema, se está implementando la solución *Endpoint Encryption* y DLP de la tecnología *Trend Micro*. La metodología incluye una evaluación exhaustiva de la infraestructura existente, la configuración de políticas de seguridad y pruebas exhaustivas.

Los resultados esperados abarcan una mejora sustancial en la seguridad de datos, la reducción de riesgos, una mayor conciencia de seguridad y una mayor eficiencia operativa. Finalmente, el proyecto tiene como objetivo proteger la integridad y confidencialidad de los datos de la empresa, garantizando el cumplimiento con las regulaciones de privacidad de datos.

# INTRODUCCIÓN

La presente era digital se encuentra en constante cambio, la seguridad de la información se ha convertido en uno de los pilares fundamentales de la supervivencia y éxito de organizaciones, tanto públicas como privadas. La creciente sofisticación de las amenazas cibernéticas y el aumento de inseguridad ciudadana han dejado en claro que la protección de datos es un desafío continuo que requiere una atención constante y soluciones innovadoras. En este contexto, la implementación de la encriptación de equipos finales (endpoints) se ha convertido en un componente esencial para fortalecer la seguridad de la información y garantizar la protección de datos confidenciales.

El presente estudio se analizó de manera exhaustiva la implementación de una solución de encriptación con tecnología de Trend Micro como una medida efectiva para reforzar la seguridad y la prevención de pérdida de datos (Data Loss Prevention - DLP) en el entorno empresarial. La solución de encriptación de equipos finales, también conocida como Endpoint Encryption, no sólo se ha consolidado como una herramienta confiable para resguardar la confidencialidad de datos sensibles, sino que también desempeña un papel clave en la mitigación de las amenazas internas y externas que comprometen la integridad de la información.

La elección de Trend Micro como punto focal de este estudio está fundamenta en su reconocido uso en el ámbito de la ciberseguridad y su constante innovación tecnológico; además posee un enfoque proactivo en la detección y prevención de amenazas cibernéticas. La solución de encriptación de esta reconocida marca a nivel mundial es un ejemplo sobresaliente de su capacidad para abordar las necesidades de seguridad de las empresas. Esta tecnología proporciona una capa adicional de protección al cifrar los datos en dispositivos finales, lo que garantiza que incluso si un dispositivo está comprometido, los datos permanecen inaccesibles para los atacantes. Es por ese motivo que esta investigación aborda, de manera crítica, el panorama actual de la ciberseguridad empresarial. Finalmente, se desarrolla de manera integral la planificación y concepción de la solución, así como su análisis y evaluación en la práctica.

# CAPÍTULO I: ASPECTOS GENERALES

## 1.1 Contexto

Las empresas en el sector minorista, un ámbito caracterizado por su enfoque en la venta de productos al consumidor final, desempeñan un papel fundamental en la economía y la sociedad, además, una empresa de este rubro se distingue por su sólida misión de brindar una experiencia de compra excepcional a sus clientes, al ofrecer productos de alta calidad y un servicio al cliente insuperable. Su visión abarca convertirse en una organización reconocida a nivel nacional e internacional, caracterizada por su innovación, calidad y compromiso con la responsabilidad social.

Además de su misión y visión, la empresa desarrolla una amplia variedad de servicios y productos que engloban desde moda y belleza hasta tecnología y productos para el hogar, satisfaciendo así una amplia gama de necesidades y deseos de sus clientes. Asimismo, su compromiso no solo se limita a su clientela, sino también a la sociedad en general. Sus valores fundamentales, que incluyen la integridad, la excelencia, la pasión por el cliente, la responsabilidad social y el trabajo en equipo, son los pilares que guían todas sus acciones y decisiones. Por esta razón la seguridad cibernética en el sector del minorista es de suma importancia en la actual era digital.

Las grandes empresas no solo gestionan una gran cantidad de información personal y realizan transacciones en línea, sino que también son responsables de salvaguardar datos críticos de los clientes y operaciones comerciales. La importancia de la ciberseguridad radica en la protección de esta información vital y la garantía de operaciones sin interrupciones. Es por ello que, el área de ciberseguridad, tiene la responsabilidad de analizar y gestionar incidencias de seguridad, contribuyendo así a salvaguardar la integridad de los sistemas y datos críticos de la organización.

## 1.2 Delimitación del Proyecto

### *1.2.1 Espacial*

El presente proyecto de implementación un sistema de encriptación con tecnología *bitlocker* para reforzar la seguridad y la prevención de pérdida de datos se desarrolló en una empresa líder en el sector *retail*, ubicado en el distrito de San Isidro, Lima.

### *1.2.2 Temporal*

La implementación del sistema de encriptación con tecnología *bitlocker* para reforzar la seguridad y la prevención de pérdida de datos, con el objetivo de fortalecer la seguridad y DLP, se inició en junio y culminó en setiembre del 2023.

### *1.2.3 Teórica*

La delimitación teórica de esta investigación se enfocó en explorar y analizar la implementación de un sistema de encriptación con tecnología *BitLocker* con el propósito de reforzar la seguridad y la prevención de pérdida de datos en una empresa de ventas.

## 1.3 Objetivos

### *1.3.1 Objetivo General*

OG. Implementar un sistema de encriptación con tecnología *bitlocker* para reforzar la seguridad y la prevención de pérdida de datos (DLP) en una empresa de ventas.

### *1.3.2 Objetivos Específicos*

OE1. Definir la arquitectura de seguridad para la solución de encriptación con tecnología de BitLocker para reforzar la seguridad y la DLP.

OE2. Establecer políticas de acceso y autorización para la solución de encriptación con tecnología de *BitLocker.*

OE3. Evaluar funcionamiento de la solución de encriptación con tecnología *BitLocker.*

# CAPÍTULO II: MARCO TEÓRICO

## 2.1 Antecedentes

### *2.1.1 Antecedentes Nacionales*

Mori (2019) desarrolló el trabajo de investigación denominado: "*Optimización del algoritmo estándar de encriptación avanzada (AES) para la protección de la información*". El problema que se abordó en esta tesis es que la complejidad computacional del algoritmo AES puede ser un obstáculo para su implementación en dispositivos con recursos limitados, como dispositivos móviles o dispositivos de Internet de las cosas (IoT); así mismo, hace referencia que el algoritmo AES puede ser susceptible a ataques de fuerza bruta, especialmente en dispositivos con recursos limitados. Por lo tanto, el autor propone optimizar el algoritmo AES para dispositivos con recursos limitados, utilizando técnicas de optimización de software como la reducción de instrucciones, la eliminación de código redundante y la optimización de la memoria. En cuanto a la metodología empleó la técnica de-optimización de software, el cual es un proceso esencial en el desarrollo de aplicaciones que implica la identificación y corrección de cuellos de botella, la mejora de algoritmos y estructuras de datos, la optimización directa del código, el ajuste de recursos y la utilización de herramientas especializadas. Concluyó mencionando, la importancia de la encriptación y el uso obligado para todo tipo de organizaciones, ya que gestionan datos sensibles, los cuales que pueden ser víctimas de ciberataques como el *ransomware, phishing o cryptojacking.*

Asurza (2022), trabajó la investigación de nombre: "*Diseño de una arquitectura de seguridad informática para incrementar la seguridad de información en la empresa Bafing S.A.C. en 2021".* El problema que se desarrolló se presentó en la empresa Bafing que enfrentó riesgos de seguridad de información, como el acceso no autorizado, la modificación de datos, la pérdida de datos y la interrupción de los servicios. Por lo tanto, el autor propone el diseño de una arquitectura de seguridad informática basada en integridad, confidencialidad y disponibilidad. La técnica aplicada es la seguridad informática, utilizada para proteger los sistemas informáticos de los ataques. Algunos ejemplos de técnicas de seguridad informática son el cifrado, la autenticación y la autorización. Este trabajo permitió comprender

la importancia de la confidencialidad de los datos en la seguridad de la información, la cual es un pilar fundamental de la seguridad de la información. En este contexto, la encriptación de disco es una medida eficaz para proteger la confidencialidad de los datos.

### *2.1.2 Antecedentes Internacionales*

Saenz (2019), quien realizó la investigación: "*Técnicas de transparencia y encriptación de información"*. La problemática que se trabajó es si la complejidad de las técnicas de encriptación tradicionales puede dificultar su implementación y uso. También mencionó el problema del cifrado de datos si puede afectar el rendimiento de los sistemas informáticos. En esta investigación se trabajó con las técnicas de transparencia y encriptación de información. Estas técnicas permiten cifrar los datos de manera transparente para el usuario, sin afectar el rendimiento de los sistemas informáticos ni dificultar el análisis de datos. También se emplearon las técnicas de encriptación tradicionales, como el cifrado simétrico y el cifrado asimétrico, métodos de encriptación como el cifrado de bloques y el cifrado de flujo. Concluye esta investigación afirmando la importancia de las técnicas de transparencia y encriptación de información, además cómo se puede usar para mejorar la seguridad de los datos sin afectar la usabilidad de los sistemas informáticos.

Padilla (2018), desarrolló la investigación: "*Implementación de un esquema de seguridad de aseguramiento lógico en estaciones utilizando un software de protección final para una entidad financiera".* El problema que se trabajó es que la entidad financiera enfrenta riesgos de seguridad de información, como el acceso no autorizado, la modificación de datos, la pérdida de datos y la interrupción de los servicios**.** Para abordar este problema el autor propone el diseño e implementación de un esquema de seguridad de aseguramiento lógico en estaciones basado en el uso de un software de protección final. El software de protección final elegido es Symantec Endpoint Protection (SEP). En cuanto al método se utilizó la evaluación de la seguridad informática. Este método sirve para evaluar la seguridad de los sistemas informáticos. Finalmente, este trabajo permitió comprender la importancia de la seguridad de las estaciones de trabajo en las entidades. Las estaciones de

trabajo son un activo crítico para las entidades, ya que almacenan y procesan información confidencial.

Richard Nyarko (2018), desarrolló la investigación: "*Security of Big Data: Focus on Data Leakage Prevention (DLP)", Luleå University of Technology, Suecia*. El problema que se trabajó es la vulnerabilidad de los datos confidenciales en entornos de *Big Data*, donde se argumentó que la creciente cantidad y complejidad de los datos, la proliferación de dispositivos móviles y el uso de la nube crean nuevos riesgos de seguridad para los datos. En esta investigación se propone implementar una estrategia de seguridad de datos integral; además, utilizar técnicas de DLP para detectar y prevenir la fuga de datos y capacitar a los trabajadores sobre la seguridad de los datos. En cuanto a la técnica que se utilizó el autor analiza las diferentes técnicas de DLP disponibles, que se pueden clasificar en dos categorías principales: detección y prevención. Finalmente, este trabajo permite entender que los datos confidenciales son cada vez más vulnerables a la fuga o al robo; por lo tanto, es necesario implementar una estrategia de seguridad de datos integral para protegerlos.

Isabel Herrera (2022), desarrolló la investigación: *"Survey of Techniques on Data Leakage Protection and Methods to address the Insider threat"*. El problema que se abordó es la creciente amenaza de fugas de datos causadas por amenazas internas. Los autores argumentaron que las amenazas internas son una de las principales causas de fugas de datos, y que es necesario implementar medidas para mitigarlas. Por lo tanto, se propuso implementar técnicas de prevención de fugas de datos, también implementar políticas y procedimientos de seguridad y capacitar a los empleados sobre la seguridad de la información. La metodología empleada fue de análisis de riesgos para identificar las principales amenazas internas. Este trabajo permitió comprender que las amenazas internas son una de las principales causas de fugas de datos. Para mitigar estas amenazas, las organizaciones deben implementar técnicas de prevención de fugas de datos, capacitar a los empleados sobre la seguridad de la información e implementar políticas y procedimientos de seguridad.

## 2.2 Bases Teóricas

### *2.2.1 Encriptación*

La encriptación es el proceso mediante el cual cierta información o texto sin formato es cifrado de forma que el resultado sea ilegible a menos que se conozcan los datos necesarios para su interpretación (Justiniano, 2015). La encriptación se utiliza como una medida de seguridad para proteger la información confidencial durante su almacenamiento o transmisión, dificultando su acceso por parte de terceros. Entre las técnicas de encriptación tenemos:

#### *a) Encriptación Simétrica*

La encriptación simétrica es una técnica de cifrado que utiliza una única clave tanto para cifrar como para descifrar datos; es decir, la misma clave se emplea tanto en el extremo del remitente (para cifrar el mensaje) como en el extremo del receptor (para descifrar el mensaje), como lo señaló Justiniano (2015), que "todo documento encriptado con una clave, deberá desencriptarse, en el proceso inverso, con la misma clave."

El cifrado simétrico tiene una limitación importante, el cual es que ambas partes (remitente y receptor) deben conocer la clave secreta. Esto puede ser un problema si las partes están comunicando de forma inalámbrica o a través de Internet, ya que la clave puede ser interceptada por un atacante. Para proteger la clave secreta, se utilizan diferentes técnicas, como la autenticación, la autorización y la gestión de claves. En la tabla 1 se visualiza las ventajas y desventajas que conlleva la encriptación simétrica, donde el beneficio principal es la eficiencia por ser rápida y eficiente.

***Tabla 1***

Ventajas y desventajas del cifrado simétrico

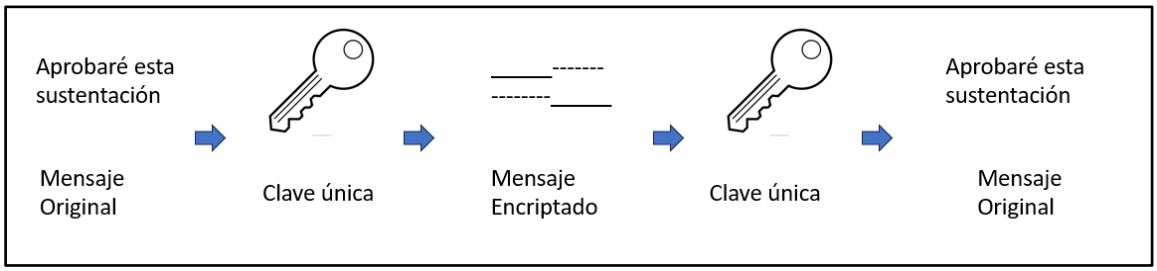
| Ventajas | Desventajas |
|---|---|
| - Eficiencia: La encriptación simétrica es más eficiente en términos de almacenamiento que la encriptación asimétrica, ya que solo requiere almacenar una clave. Esto se debe a que la encriptación asimétrica requiere almacenar dos claves, una pública y una privada (Radwan, 2016). | - Problema de distribución de claves: La clave secreta debe distribuirse a todos los participantes en el protocolo de cifrado. Esto puede ser un desafío, especialmente para grandes grupos de personas (Radwan, 2016). |

| | |
|---|---|
| - Simplicidad: La encriptación simétrica es más fácil de usar que la encriptación asimétrica, ya que solo requiere que las partes que se comunican compartan una clave secreta. Esto se debe a que la encriptación asimétrica requiere que las partes que se comunican intercambien dos claves, una pública y una privada. (Radwan, 2016). | - Escalabilidad: como se explica en el trabajo de investigación de Rudnytskyi, V., Korchenko, O., Lada, N., Ziubina, R., Wieclaw, L., & Hamera, L. (2022) el cifrado simétrico no es adecuado para escenarios en los que una gran cantidad de usuarios necesitan comunicarse de forma segura, ya que cada par de usuarios requeriría una clave única. |

En la figura 1 se visualiza la estructura básica el cifrado simétrico, en donde se muestra cómo el mensaje original (aprobaré esta sustentación) se cifra con la llave única para crear un mensaje encriptado. El mensaje encriptado luego se descifra con la misma llave única para restaurar el mensaje original.

***Figura 1***

Cifrado simétrico




Fuente: Propia

### *b) Encriptación Asimétrica*

En la criptografía asimétrica, se crean dos llaves de cifrado al mismo tiempo, la llave pública se comparte públicamente y llave privada se usa para descifrar el mensaje cifrado con la llave pública (Fernandez, 2021). Estos algoritmos, en términos conceptuales, satisfacen tres necesidades fundamentales (privacidad, verificación de la autenticidad y la imposibilidad de negación), pero su velocidad de ejecución en el proceso de asegurar la información es notablemente reducida, en la tabla 2 se visualiza las ventajas y desventajas que conlleva la encriptación asimétrica, en donde el beneficio principal es su autenticación y la desventaja primordial radica en su rendimiento.

***Tabla 2***

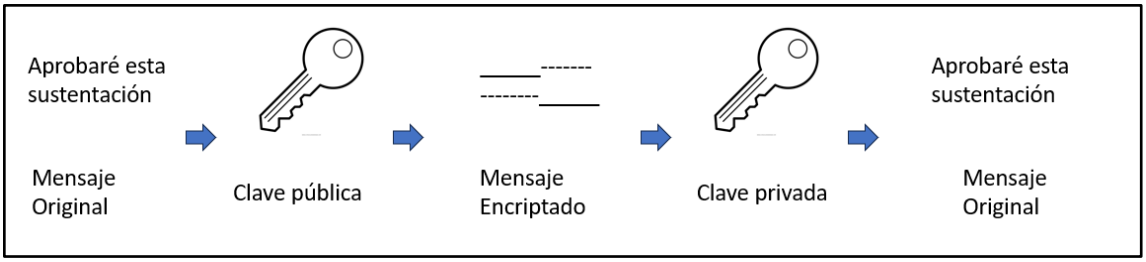
Ventajas y desventajas del cifrado asimétrico

| Ventajas | Desventajas |
|---|---|
| Autenticación: el cifrado asimétrico proporciona mecanismos de autenticación integrados mediante el uso de firmas digitales. Permite al destinatario verificar la integridad y autenticidad de los datos cifrados Rudnytskyi, Korchenco (2022). | Rendimiento más lento: los algoritmos de cifrado asimétrico son computacionalmente intensivos y más lentos en comparación con los algoritmos de cifrado simétrico. No son adecuados para cifrar grandes cantidades de datos en tiempo real Rudnytskyi, Korchenco (2022). |
| Escalabilidad: el cifrado asimétrico es adecuado para escenarios en los que una gran cantidad de usuarios necesitan comunicarse de forma segura. Cada usuario puede tener su propio par de claves único Rudnytskyi, Korchenco (2022). | Complejidad: como se explica en el trabajo de investigación de Rudnytskyi, Korchenco (2022) el cifrado asimétrico es más complejo de implementar y gestionar en comparación con el cifrado simétrico. |

La encriptación asimétrica es un método de encriptación muy seguro y se utiliza en una amplia gama de aplicaciones, como la seguridad de la información, la firma digital y la autenticación, en la figura 2 se muestra la estructura básica el consiste el cifrado asimétrico, en donde se muestra como el mensaje original (aprobaré esta sustentación) se cifra con la llave pública del emisor para crear un mensaje encriptado. El mensaje encriptado luego se descifra con la llave privada del emisor para restaurar el mensaje original.

***Figura 2***

Cifrado asimétrico




Fuente: Propia

### *c) Encriptación de Datos en Reposo*

Según IBM (2021) la encriptación de datos en reposo se refiere a la práctica decifrar los datos que se encuentran almacenados en bases de datos y que no se transmiten a través de redes. Al implementar la encriptación de datos en reposo, se garantiza la protección de los datos almacenados en reposo, lo que incluye incluso

las copias de seguridad que se almacenan de forma offline y esto se logra utilizando una clave secreta que solo conocen los usuarios autorizados. Los ataques contra los datos en reposo incluyen intentos de obtener acceso físico al hardware en el que se almacenan los datos y, a continuación, poner en peligro los datos contenidos. En este tipo de ataque, la unidad del disco duro de un servidor puede utilizarse de forma incorrecta durante el mantenimiento permitiendo a un atacante eliminar la unidad de disco duro. Más adelante el atacante tendría que poner el disco duro en un equipo bajo su control para intentar obtener acceso a los datos.

***d) Encriptación de Datos en Tránsito***

Según Avast (2020), los datos en tránsito son lo opuesto a los datos en reposo, esto quiere decir que los datos en tránsito están activos y se pueden transferir a través de cables y transmisión inalámbrica a otras ubicaciones dentro o entre sistemas informáticos. Estos datos pueden viajar a través de una red y pueden leerse, actualizarse o procesarse. Los ejemplos incluyen datos en movimiento desde el almacenamiento local a la nube o un correo electrónico que se envía; cuando los datos llegan a la bandeja de entrada del destinatario, se convierten en datos en reposo. Según *Vaheedbasha, S., Natajaran, K.* (2022) los beneficios de la encriptación de datos en tránsito son los siguientes:

- Seguridad: el cifrado de datos en tránsito garantiza que la información esté protegida contra el acceso no autorizado o la interceptación durante la transmisión.
- Privacidad: el cifrado proporciona una capa adicional de privacidad, evitando que personas no autorizadas vean o manipulen datos confidenciales.
- Cumplimiento: cifrar datos en tránsito ayuda a las organizaciones a cumplir con las regulaciones de protección de datos y los estándares de la industria que requieren la transmisión segura de información confidencial.

***e) Encriptación de Correo Electrónico***

Según Li, H., Huang, Q., Shen, J. (2019) definieron el cifrado de correo electrónico como un mecanismo que permite la transmisión segura de correos electrónicos mediante el cifrado del contenido de los correos electrónicos y las palabras clave asociadas. En este sistema, el remitente encripta los correos

electrónicos y las palabras clave utilizando la clave pública del destinatario y los envía a un servidor de correo electrónico en la nube. A continuación, el destinatario puede recuperar los correos electrónicos cifrados proporcionando una trampilla asociada a una palabra clave específica. El servidor busca correos electrónicos cifrados coincidentes y los devuelve al destinatario, que puede descifrar y leer el contenido, en la tabla 3 se visualiza las ventajas y desventajas que conlleva la encriptación de datos en tránsito.

***Tabla 3***

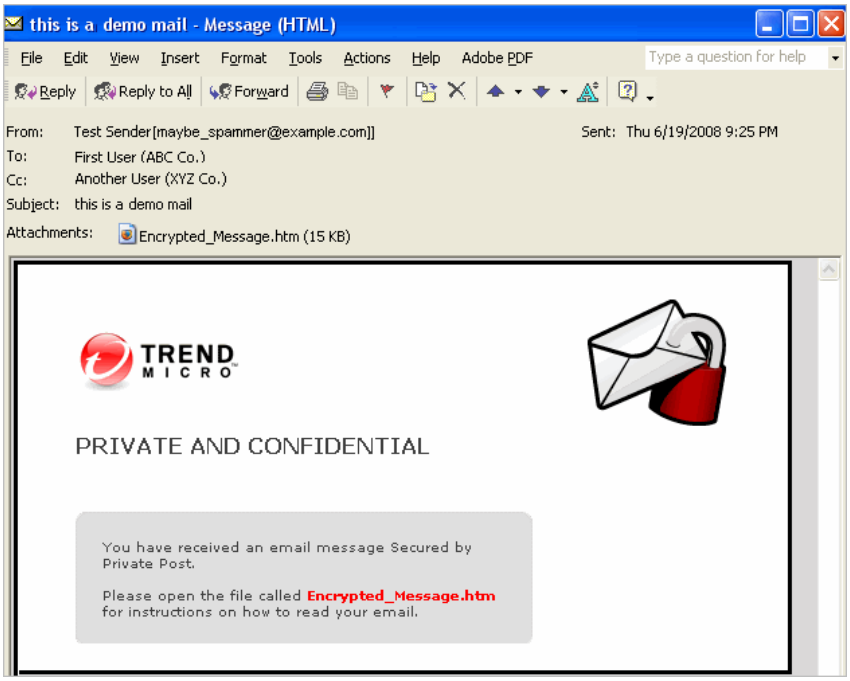
Ventajas y desventajas de la encriptación de correo electrónico

| **Ventajas** | **Desventajas** |
|---|---|
| 1. Seguridad mejorada: Según Li, H., Huang, Q., Shen, J. (2019) el cifrado del correo electrónico garantiza que el contenido de los correos electrónicos esté protegido contra el acceso no autorizado, lo que proporciona un mayor nivel de seguridad para la información confidencial.<br><br>2. Protección de la privacidad: Según Li, H., Huang, Q., Shen, J (2019) El cifrado garantiza que solo el destinatario previsto pueda acceder y leer el correo electrónico, evitando que personas o entidades no autorizadas intercepten o lean el contenido. | 1. Impacto en el rendimiento: De acuerdo con Li, H., Huang, Q., Shen, J (2019) los procesos de cifrado y descifrado pueden introducir cierta sobrecarga, lo que puede afectar al rendimiento de los sistemas de correo electrónico, especialmente cuando se trata de grandes volúmenes de correos electrónicos.<br>2. Problemas de compatibilidad: de acuerdo con Li, H., Huang, Q., Shen, J. (2019) es posible que los métodos de cifrado de correo electrónico no sean universalmente compatibles en diferentes clientes o plataformas de correo electrónico, lo que dificulta garantizar un cifrado y descifrado sin problemas para todos los usuarios. |

Por lo anteriormente expuesto, incluso si alguien intercepta el correo electrónico durante su transmisión, no podrá leerlo sin la clave privada, en la figura 3 se muestra un ejemplo práctico de encriptación de correo electrónico, en donde se aprecia un correo electrónico encriptado por la marca *Trend Micro.*

***Figura 3***

Encriptación de correo electrónico




Fuente: Trend Micro

### *f) Encriptación de Almacenamiento en la Nube*

Según Ikusi (2023) el cifrado de datos en la nube es el proceso de proteger la información contenida en los servidores virtuales y la forma de acceder a dicha información. La seguridad es una parte integral de la nube y esto incluye la protección de los datos, en la tabla 4 se visualiza las ventajas y desventajas que conlleva la encriptación de datos en tránsito.

### *Tabla 4*

Ventajas y desventajas de la encriptación de almacenamiento en nube

| Ventajas | Desventajas |
|---|---|
| 1. Almacenamiento eficiente de datos: De acuerdo con Li, H., Huang, Q., Shen, J. (2019) el almacenamiento en la nube proporciona una solución rentable para almacenar grandes cantidades de datos. El cifrado permite a los usuarios aprovechar el almacenamiento en la nube al tiempo que garantiza la confidencialidad de su información. | 1. Riesgo de revelar patrones de búsqueda: De acuerdo con Li, H., Huang, Q., Shen, J. (2019) en ciertos esquemas de cifrado, el patrón de búsqueda de los usuarios puede revelarse si el servidor en la nube se ve comprometido. Los adversarios podrían obtener información sobre el texto sin formato a partir de la frecuencia de búsqueda, comprometiendo la privacidad del usuario. La implementación y gestión de la encriptación puede |

| | |
|---|---|
| | ser compleja, especialmente en entornos empresariales. |
| 2. Reducción del riesgo de acceso no autorizado: De acuerdo con Li, H., Huang, Q., Shen, J. (2019) el cifrado agrega una capa adicional de seguridad, lo que dificulta que las personas no autorizadas accedan y descifren los datos cifrados almacenados en la nube. | 2. Gestión compleja de certificados: De acuerdo con Li, H., Huang, Q., Shen, J. (2019) algunos esquemas de cifrado, como el cifrado autenticado de clave pública con búsqueda de palabras clave (PAEKS), requieren una gestión compleja de certificados en una infraestructura de clave pública (PKI). Esto puede conducir a un aumento de los costes de mantenimiento y a la complejidad de la gestión. |

### *g) Encriptación de Mensajería Instantánea*

Según Google (2023), cuando envías mensajes encriptados de extremo a extremo con la app de mensajes, todos los chats (incluidos sus textos, archivos y contenidos multimedia) se encriptan para que los datos viajen entre dispositivos. La encriptación convierte los datos en texto codificado: un texto ilegible que solo se decodifica con una clave secreta. Este tipo de encriptación funciona de la siguiente manera:

- **Cifrado de Extremo a Extremo**: Se orienta a proteger solamente los datos de usuario de las comunicaciones, es decir, la información que tiene significado para los interlocutores, dejando en claro la información de señalización con los centros de conmutación de las redes (Fernandez, 1990).
- **Generación de Claves**: Se trata esencialmente de procesos de obtención de números aleatorios. En general, se pueden considerar varios procedimientos: generación manual, generación basada en medidas de fenómenos impredecibles, generación de números seudoaleatorios y generación basada en utilización de un sistema criptográfico (Fernandez, 1990). Cada usuario de la aplicación de mensajería tiene un par de claves: una clave pública y una clave privada. La clave pública se comparte con otros usuarios para cifrar los mensajes que se envían, mientras que la clave privada se mantiene en secreto y se utiliza para descifrar los mensajes recibidos.

Según Gunawan A., Prima S. (2022) los beneficios de la encriptación de mensaje de texto son los siguientes:

- Mayor seguridad: el cifrado garantiza que el contenido de los mensajes de texto permanezca confidencial y que personas no autorizadas no puedan acceder fácilmente a él
- Protección contra la interceptación: los mensajes cifrados son menos susceptibles a la interceptación y las escuchas, lo que proporciona una capa adicional de protección durante la transmisión.
- Compatibilidad con el servicio de SMS existente: el método de cifrado propuesto está diseñado para ser totalmente compatible con los servicios de SMS existentes, requiriendo una configuración mínima tanto por parte del remitente como del destinatario.

### *2.2.2 Bitlocker*

El cifrado de unidad BitLocker es una característica de seguridad integral del sistema operativo Windows 7 que ayuda a proteger los datos almacenados en unidades de datos fijas y extraíbles y en la unidad del sistema operativo (Jiménez, Orellana, 2012), esto ayuda a proteger los datos contra el acceso no autorizado, incluso si el dispositivo se pierde o es robado. Además, el cifrado de unidad *BitLocker* es una característica de protección de datos que se integra en el sistema operativo y soluciona las amenazas de robo o exposición de datos de equipos perdidos, sustraídos o retirados inadecuadamente (Microsoft, 2016), en donde los datos en la unidad de disco duro son los documentos confidenciales.

Bitlocker utiliza el estándar de cifrado avanzado (AES) como algoritmo de cifrado con longitudes de clave configurables de 128 o 256 bits además, bitLocker admite el método de cifrado XTS-AES (la elección entre usar 128 bits o 256 bits en el cifrado XTS-AES se refiere a la longitud de la clave utilizada en el algoritmo AES), que está disponible para dispositivos con Windows 10 o posterior y admite encadenamiento de bloques de cifrado (CBC) o robo de texto cifrado (XTS), Microsoft (2023).

Finalmente, el BitLocker también considera situaciones de pérdida de contraseña o problemas de hardware. Para abordar estos escenarios, permite a los usuarios generar una "clave de recuperación". Esta clave es esencialmente una copia de seguridad de la clave maestra, y se almacena de forma segura en caso de emergencia.

### 2.2.3 Tecnología de Trend Micro

Es una empresa líder en ciberseguridad que ofrece soluciones para proteger a las empresas y las personas de las amenazas cibernéticas. Esta marca ofrece una protección completa contra las amenazas cibernéticas gracias a su enfoque en tres áreas clave, confidencialidad, integridad y disponibilidad (Trend Micro, 2023). Las principales funciones son:

#### *a) Protección contra Malware y virus*

Existen decenas de miles de virus/malware, una cifra que va en aumento cada día. En la actualidad, los virus informáticos pueden dañar seriamente los equipos mediante el aprovechamiento de las vulnerabilidades de las redes corporativas, los sistemas de correo electrónico y los sitios Web (Trend Micro, 2022). La protección contra malware y virus es una de las funciones esenciales de cualquier suite de seguridad de Trend Micro. Esta función se enfoca en detectar, prevenir y eliminar programas maliciosos y amenazas cibernéticas que pueden comprometer la seguridad de los sistemas y datos.

#### *b) Prevención de Amenazas Avanzadas*

La prevención de amenazas avanzadas es una función fundamental en las soluciones de seguridad de Trend Micro, diseñada para identificar y mitigar amenazas sofisticadas y ataques dirigidos que pueden eludir las medidas de seguridad tradicionales, (Trend Micro, 2023).

#### *c) Prevención de Fugas de Datos (DLP)*

Ahora más que nunca, sus datos están en movimiento, ya sea en un ordenador portátil, una unidad flash, en el correo electrónico o moviéndose a través de infraestructuras físicas, virtuales y en la nube. En cualquier punto a lo largo del camino, sus datos financieros, información de cliente, propiedad intelectual o secretos comerciales podrían perderse o ser robados. Asegurar estos datos es aún más complicado debido a varios factores de riesgo creciente (Trend Micro, 2023); por lo tanto, la prevención de pérdida de datos (DLP) de Trend Micro es una función esencial que se enfoca en prevenir la fuga o filtración no autorizada de datos confidenciales y sensibles. Esta función es fundamental para garantizar que la información crítica de una organización no caiga en manos equivocadas.

***d) Prevención de Endpoints***

Esta protección es una de las funciones más críticas de Trend Micro, ya que se centra en proteger los dispositivos finales, como computadoras de escritorio, laptops, servidores y dispositivos móviles, contra una amplia gama de amenazas cibernéticas.

***e) Seguridad en la Nube***

Trend Micro (2023) menciona que al emplear servicios de hospedaje en la nube como AWS y Microsoft Azure para albergar aplicaciones y datos confidenciales o al hacer uso de la eficiencia proporcionada por Microsoft Office 365, Dropbox y demás proveedores de software como servicio (SaaS) basados en la nube, se evidencia una responsabilidad en la garantía de seguridad en el entorno cloud. La seguridad en la nube es una función esencial en las soluciones de Trend Micro, diseñada para proteger los activos y datos en entornos en la nube. A medida que las organizaciones migran cada vez más sus aplicaciones y datos a la nube, la seguridad en la nube se ha vuelto crítica para garantizar la protección contra amenazas cibernéticas.

***g) Seguridad de Red y Servidores***

La seguridad de red y servidores de Trend Micro se enfoca en proteger la infraestructura de red, servidores y aplicaciones de una organización contra una amplia gama de amenazas cibernéticas. Esto incluye la protección contra intrusiones, la gestión de vulnerabilidades y la prevención de amenazas en tiempo real.

## 2.3 Definición de términos básicos

- **Encriptación**. La encriptación es el procedimiento a través del cual se codifica una determinada información o texto en un formato ilegible, a menos que se posean los datos requeridos para su desciframiento. Justiniano C. (2015).

- **Prevención de Pérdida de Datos (DLP)**. Según Liu, S., & Kuhn, R. D. (2010) la prevención de la pérdida de datos (DLP) se define como "un conjunto de prácticas y herramientas que se emplean para salvaguardar la información confidencial de amenazas como la pérdida, el uso indebido o el acceso no autorizado”.

- **Malware**. Según Orihuela (2022) el término "malware" engloba una diversidad de software pernicioso, como virus, ransomware, spyware y gusanos informáticos, que se caracterizan por ser programas diseñados para infiltrarse de manera perjudicial en sistemas de información y obtener acceso no autorizado a dispositivos digitales, causando así daños y vulnerabilidades.

- **Vulnerabilidad**. Se refiere a cualquier debilidad que puede ser aprovechada para causar pérdida o daño en un sistema. De este modo, el punto más frágil de la seguridad de un sistema equivale al punto de mayor vulnerabilidad del mismo. Por otro lado, un ataque constituye cualquier acción que explota una vulnerabilidad" (Guerreiro, J., Batista, E., Monteiro, E., & Silva, L. M, 2018).

- **Autenticación (Token)**. Según Luján-Mora (2018) la autenticación por token se refiere al uso de un token digital como credencial para acceder a un sistema en lugar de nombre de usuario y contraseña. El token sirve para validar la identidad del usuario.

- **VPN**. Según Ronald S., Segundo M. (2019) una VPN o red privada virtual es una tecnología de red que extiende de forma segura una red local a través de una red pública como internet. Las VPN permiten que los equipos de una red corporativa u organizacional se comuniquen entre sí de manera segura sobre redes públicas, enviando y recibiendo datos como si estuvieran en una red privada. Esta tecnología posibilita funcionalidades clave como el acceso remoto protegido a la red de una empresa u organización.

- **TenableIO.** Teblable es una solución de gestión de vulnerabilidades basada en la nube que protege las redes en expansión y previene las filtraciones de datos con evaluaciones continuas de vulnerabilidades, Tenable (2022).

- **Prueba de Concepto (PoC).** Según Banda (2022) una prueba de concepto (PoC) es una demostración de la viabilidad de una idea o concepto. Es un paso importante en el desarrollo de un nuevo producto o servicio, ya que permite a los desarrolladores probar su idea y obtener comentarios de los usuarios.

- **Firewall**. Según Khoumsi, A., Erradi, M., & Krombi, W (2016) denomina al firewall como dispositivo que se colocan entre una red y el mundo exterior para proteger los datos confidenciales y funcionan analizando el tráfico de red y bloqueando el acceso no autorizado.

- **Ivanti**. Ivanti es una solución VPN segura, le permiten habilitar rápidamente a su personal remoto con una conectividad segura a las aplicaciones en las instalaciones y en la nube, Ivanti (2023).

- **Bitlocker**. Según Microsoft (2023) bitLocker es una función de cifrado de disco de Windows que proporciona cifrado para volúmenes completos, diseñada para proteger los datos mitigando el acceso no autorizado a datos en computadoras perdidas o robadas.

- **IP**. Según Coellar, J,. y Cedeño, J. (2013) una dirección IP es un número que identifica de forma única a cada dispositivo conectado a una red informática. Las direcciones IP se utilizan para identificar y localizar dispositivos en Internet.

# CAPÍTULO III: DESARROLLO DEL TRABAJO PRPOFESIONAL

## 3.1 Determinación y Análisis del Problema

En la era digital, las empresas dependen cada vez más de la tecnología para operar, por ejemplo: los dispositivos móviles, las redes inalámbricas y las aplicaciones en la nube son herramientas esenciales para las ventas, el marketing y la administración. Sin embargo, esta dependencia de la tecnología también aumenta la exposición de las empresas a los riesgos de seguridad y DLP. Los datos confidenciales, como información de clientes, finanzas y secretos comerciales, pueden ser robados, perdidos o expuestos a ataques cibernéticos. Los riesgos de seguridad y DLP pueden tener consecuencias graves para las empresas de ventas, Por ejemplo, pueden dañar la reputación de la empresa, perder clientes, incurrir en multas y otros costos financieros, y hasta incluso provocar la quiebra. Por lo tanto, es importante que las empresas de ventas implementen medidas de seguridad adecuadas para proteger sus datos confidenciales. Una de las medidas de seguridad más importantes es la encriptación y el DLP, esto incluye estar prevenido ante:

- Robo de dispositivos: Los dispositivos móviles de los empleados son un objetivo frecuente para los ladrones. Si un dispositivo móvil es robado, los datos confidenciales almacenados en él podrían caer en las manos equivocadas.
- Pérdida de datos: Los datos pueden perderse por accidente, como si un empleado accidentalmente elimina un archivo importante.
- Ataques cibernéticos: Los ataques cibernéticos son una amenaza creciente para las empresas de todos los tamaños. Los atacantes podrían intentar acceder a los datos confidenciales de la empresa utilizando técnicas como el phishing o el malware.

En la figura 4 se visualiza una reciente encuesta sobre los recientes ataques de ciberseguridad en empresas de Perú donde se observa que según un estudio reciente (Canalti, 2021) más del 30% de las compañías en la región de América Latina experimentaron un incremento en los incidentes de seguridad cibernética debido a la crisis del covid-19. Los ataques más comunes fueron aquellos como el phishing, y el sector bancario fue el más perjudicado, con un aumento del 52% en incidentes percibidos.

***Figura 4.***

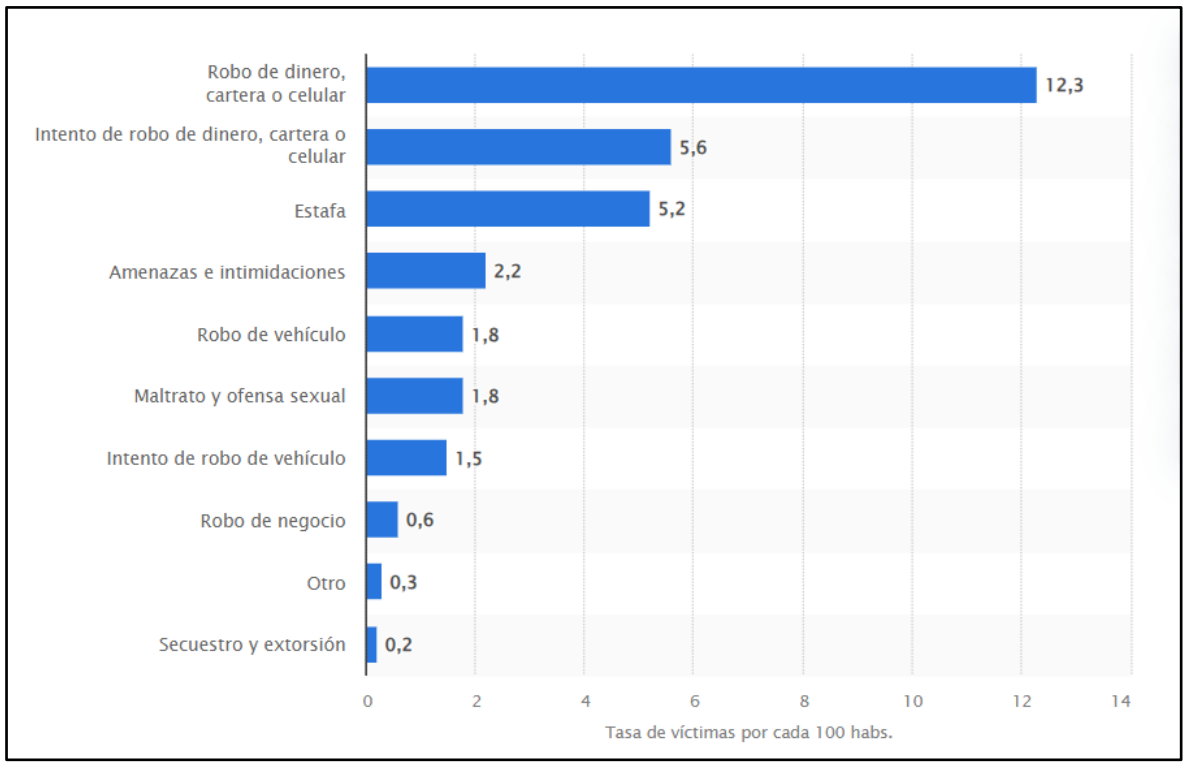
Tipos de Ciberataques más usados en Perú en época de pandemia.


Fuente: Canalti

También es importante recalcar que la delincuencia es un problema grave en Perú, y los robos son uno de los delitos más comunes, en la figura 5 se observa que de acuerdo con Statista (2023), el porcentaje de robos en Perú durante los meses de enero a junio de 2023 fue de 12,3%. Esto significa que aproximadamente 12 de cada 100 habitantes de áreas urbanas de Perú fueron víctimas de un robo durante este período.

***Figura 5.***

Delitos con mayor incidencia en zonas urbanas de Perú durante el primer semestre de 2023.




Fuente: Statista

### 3.2 Modelo de Solución Propuesto

La implementación de una solución integral de seguridad y prevención de pérdida de datos (DLP) en la empresa de ventas se basa en la adopción de tecnología Bitlocker y la implementación de políticas y medidas específicas. Esta solución aborda las situaciones problemáticas identificadas durante la estancia en la empresa, centrándose en dos aspectos clave: encriptación de disco y políticas DLP.

Esta solución contribuye significativamente a mejorar la seguridad y la prevención de pérdida de datos en una empresa de ventas al aplicar habilidades y conocimientos especializados en el ámbito de la ciberseguridad y la gestión de la información. La implementación de un sistema de encriptación con tecnología bitLocker es una medida crítica para mitigar los riesgos asociados a la exposición de datos confidenciales en un entorno empresarial cada vez más digitalizado.

El diseño de la solución integral de cifrado con tecnología bitlocker en dispositivos finales se llevó a cabo en las siguientes etapas:

### 3.2.1 Análisis de Requisitos

En un entorno empresarial altamente digitalizado, la información se considera un activo crítico que requiere protección contra posibles amenazas. La identificación de los requisitos de seguridad de los datos se llevó a cabo considerando que la información almacenada en los dispositivos y sistemas de la empresa era de vital importancia. Esta información incluye datos de clientes, detalles financieros, estrategias de ventas, comunicaciones internas y externas, y otros activos digitales que sustentaban la operación de la organización.

El análisis de requisitos se centró en reconocer la sensibilidad de estos datos y determinar cuáles de ellos necesitaban ser encriptados para garantizar su confidencialidad e integridad. Esto implicó considerar el valor de los datos, la posible exposición a riesgos de seguridad, las regulaciones vigentes y las expectativas de los clientes y socios comerciales. Por ejemplo, se identificaron datos personales de clientes, como nombres, direcciones y números de teléfono, como información de vital importancia que requería encriptación para cumplir con regulaciones como el Reglamento General de Protección de Datos (GDPR).

### 3.2.2 Determinación de características de accesibilidad

Durante el proceso de diseño, se definió con precisión qué usuarios aplicarían a la solución de encriptación, priorizando a los jefes y gerentes de la organización. La necesidad de esta segmentación se basó en el reconocimiento de la alta confidencialidad de la información que estos roles manejaban, como contratos, números financieros y otros datos sensibles, adicionalmente, se delinearon cuidadosamente los usuarios autorizados para acceder a la administración de la solución de encriptación, designando a dos miembros del equipo de ciberseguridad para tal propósito: el primero, el líder del equipo, y el segundo, aquel usuario que sobresale por su amplia experiencia y pericia en la materia.

### 3.2.3 Definición de arquitectura

La cantidad de equipos es un factor importante a considerar al diseñar una solución de cifrado para equipos finales, esto se debe a que, para cada cantidad, hay diferentes características y/o requisitos que deben cumplirse. Para el presente proyecto la cantidad de equipos a considerar para la solución de encriptación no es mayor a 400, en la tabla 5 se visualizan los requisitos para la implementación considerando la cantidad de equipos dicho anteriormente.

**Tabla 5**

Requisitos de Policy Server

| Dispositivos | Requisitos de *PolicyServer* | Requisitos de la base de datos SQL de *PolicyServer* |
|---|---|---|
| 1000 | Un servidor multifunción de base de datos SQL y front-end con un procesador Intel Xeon de cuatro núcleos a 2,2 GHz o superior<br>8 GB de RAM<br>disco duro de 120GB | Instalado en el servidor front-end de PolicyServer |

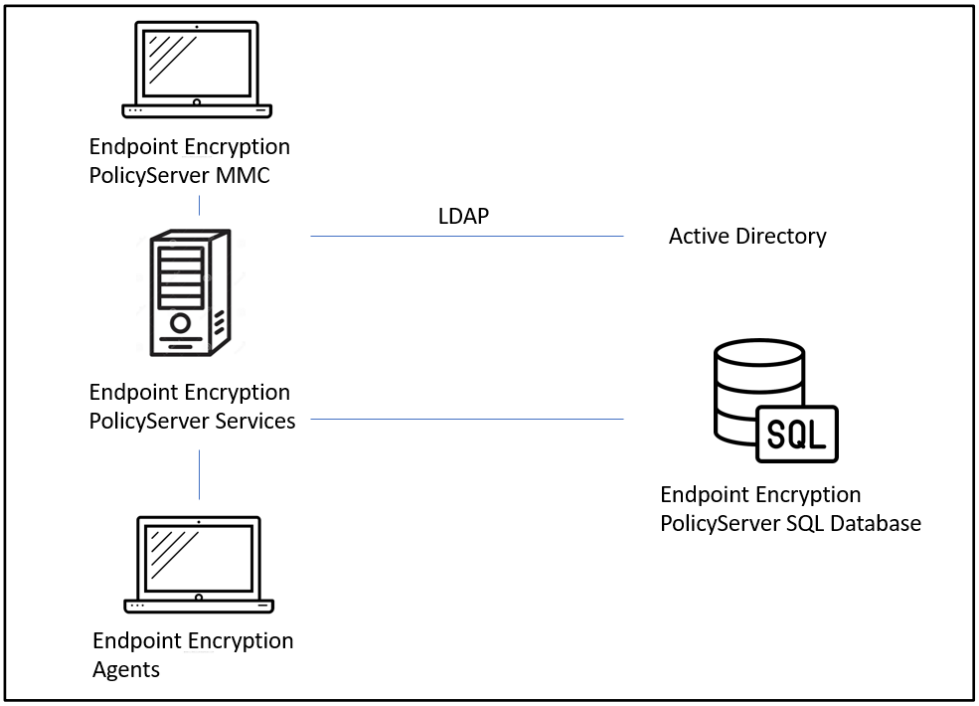
Adicionalmente, *Trend Micro* recomienda que, para entornos de red pequeñas, las bases de datos SQL de *PolicyServer* (agente se pueden instalar en el mismo servidor) y para implementaciones de *PolicyServer* en entornos de más de 1500 dispositivos, también recomienda tener al menos dos servidores dedicados, así mismo, los requerimientos del PolicyServer y los equipos finales a encriptar se aprecian en el anexo 1 y anexo 2 respectivamente. La estructura de la solución de cifrado con tecnología *Bitlocker* para una cantidad menor a 400 equipos se compone de los siguientes componentes:

- *PolicyServer*: Es un servidor que proporciona una plataforma centralizada para administrar y controlar la solución, incluyendo la configuración de políticas, la aplicación de cifrado y la generación de informes.
- Base de datos SQL: Almacena los datos de configuración y políticas de la solución.
- LDAP - *Lightweight Directory Access Protocol* - Protocolo Ligero de Acceso a Directorios: Es un protocolo que permite a los sistemas acceder a la información de usuarios y grupos almacenados en un directorio.
- Active Directory: Es un servicio de directorio de Microsoft que almacena información sobre usuarios, grupos, equipos y otros recursos de red.

En la figura 6 se visualiza la arquitectura propuesta para la solución de encriptación, para el presente proyecto la base de datos SQL estuvo integrada dentro del mismo servidor esto debido a la cantidad de equipos definidos inicialmente.

***Figura 6***

Arquitectura de la solución de encriptación.




Fuente: Propia

La arquitectura muestra un escenario simple para una cantidad de equipos menor a 400 equipos. En este escenario, el *PolicyServer* y la base de datos SQL se instalan en el mismo servidor. El funcionamiento de la arquitectura se describe a continuación:

- El *PolicyServer* se conecta al *Active Directory* para obtener información sobre los usuarios y grupos de la organización.
- El *PolicyServer* utiliza la información del *Active Directory* para crear políticas de cifrado para los dispositivos de la organización.
- Los agentes de Endpoint Encryption se conectan al *PolicyServer* y obtienen las políticas de cifrado.

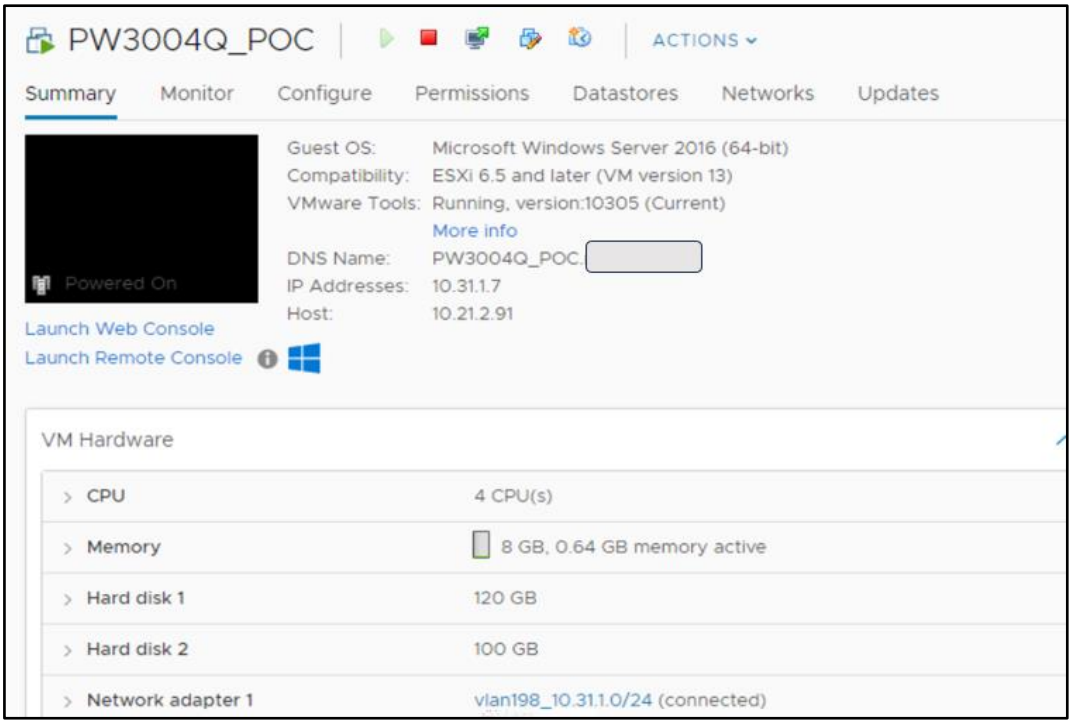
- Los agentes de *Endpoint Encryption* cifran los datos en los dispositivos según las políticas de cifrado.

### 3.2.4 Implementación del Servidor

Para el presente proyecto se creó un servidor on-premise en un ambiente PoC con las características adjuntas en la figura 7, en ella se visualiza el servidor con nombre PW3004Q_POC la cual se encuentra identificada con la IP 10.31.1.7, también se visualiza el sistema operativo Microsoft Windows Server 2016 (64 bit) con el cual se cumple los requisitos establecidos, así mismo, en la figura 8 se visualiza las características adicionales del servidor tales como, el espacio de su disco duro y la cantidad de RAM que este posee.

***Figura 7***

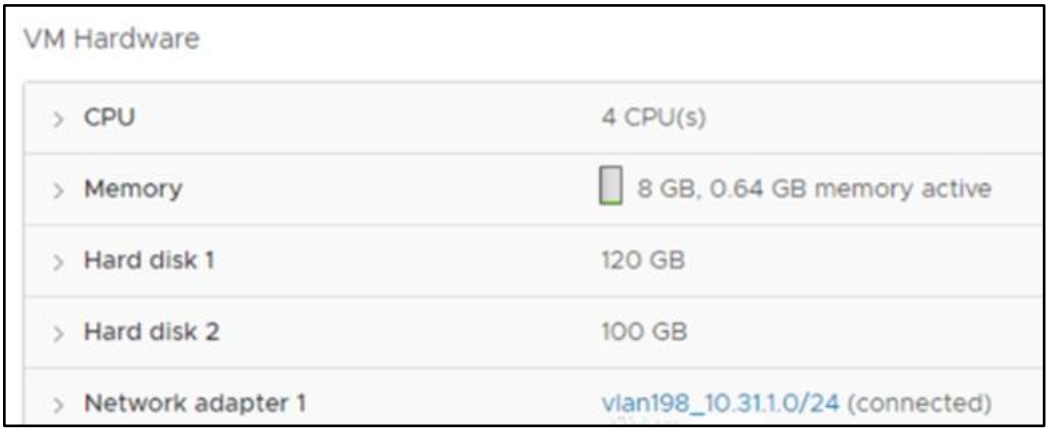
Creación del servidor PW3004Q




Fuente: Propia

***Figura 8***

Características hardware del servidor

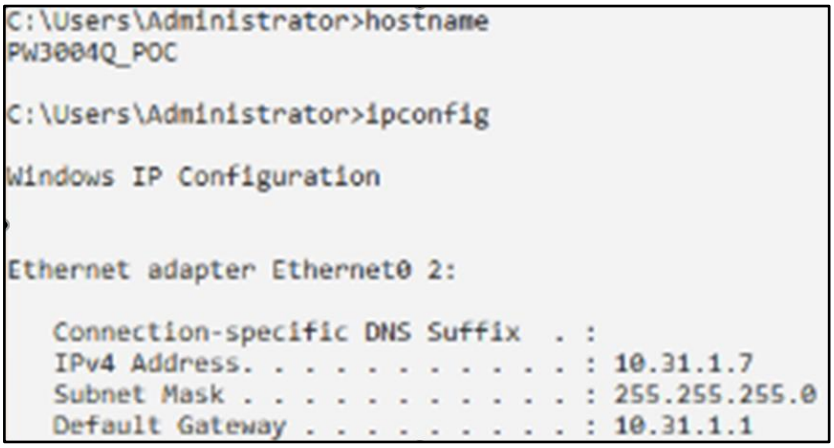



Fuente: Propia

Se realizó la creación del servidor y se validó la configuración de red de la misma, adicionalmente, en la figura 9 se visualiza la ejecución del comando “hostname” e 'ipconfig' en el símbolo del sistema (CMD) de un servidor Windows el cual proporciona información de la configuración de red del servidor.

***Figura 9***

Configuración de red en el servidor a través de ipconfig




Fuente: Propia

**a) Hardening del servidor**

Según Caiza Navas, A. G. (2019) el hardening o endurecimiento de la configuración de seguridad es una de las mejores prácticas recomendadas para proteger los sistemas contra ataques, ya que reduce las superficies vulnerables, mitiga los riesgos conocidos y dificulta la explotación de la infraestructura tecnológica, por lo que, el hardening del servidor es un componente crítico en la implementación de cualquier sistema de seguridad de la información. En este caso, el servidor con nombre "PW3004Q_POC" ubicado en el entorno POC con la dirección IP 10.31.1.7 ha sido sometido a un proceso de hardening con el objetivo de fortalecer su seguridad y resistencia frente a posibles amenazas y ataques.

El adecuado hardening del servidor proporciona protección en diferentes frentes de seguridad, como se detalla a continuación:

1. Protección contra Amenazas Cibernéticas.

El hardening garantiza que el servidor esté configurado de manera que sea menos vulnerable a ataques cibernéticos. La implementación de módulos de seguridad de *Trend Micro*, como antimalware, *activity monitoring e intrusion prevention*, añade una capa adicional de protección contra malware, actividad sospechosa y ataques de red. Esto es esencial para preservar la integridad de los datos y prevenir intrusiones no autorizadas.

2. Mantenimiento de la Confidencialidad y la Disponibilidad

El hardening contribuye a garantizar que los datos críticos de la empresa permanezcan confidenciales y estén disponibles cuando se necesiten. La integración de soluciones de *Trend Micro*, como el monitoreo de actividad y la prevención de intrusiones, ayuda a detectar y mitigar amenazas en tiempo real, lo que respalda la disponibilidad continua de los servicios.

3. Preparación del servidor para los escenarios de ataque.

La hardening no solo busca prevenir ataques, sino también prepararse para enfrentarlos. Al implementar medidas de seguridad sólidas y monitorear constantemente el servidor, se está en una mejor posición para detectar y responder de manera efectiva a incidentes de seguridad.

En la figura 10 se visualiza los agentes con las que cuenta el servidor para temas de hardening, en donde el módulo más importante es el “**anti-malware**” el cual es esencial debido a su capacidad para detectar y prevenir una amplia variedad de amenazas de malware, incluyendo virus, troyanos, *ransomware* y otras formas de software malicioso.

***Figura 10***

Módulos de seguridad de Trend Micro.


Fuente: Propia

### b) Identificación de Vulnerabilidades

La identificación de vulnerabilidades permite identificar posibles amenazas y debilidades en el servidor antes de que puedan ser explotadas por atacantes. Dado que el servidor es una parte fundamental de la infraestructura de la empresa de ventas, identificar y abordar vulnerabilidades potenciales es esencial para evitar interrupciones en las operaciones y la pérdida de datos.

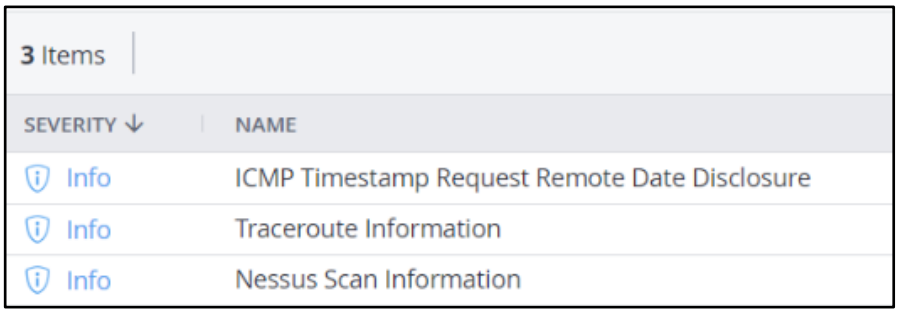
Durante el proceso de escaneo de vulnerabilidades, se revisan las configuraciones del servidor en busca de errores y configuraciones incorrectas. Esto incluye la verificación de políticas de seguridad, permisos, puertos abiertos y servicios en ejecución. Corregir estas configuraciones puede evitar posibles brechas de seguridad.

El escaneo de vulnerabilidades con Tenable permite una identificación proactiva de amenazas. La herramienta escanea el servidor en busca de posibles debilidades, configuraciones incorrectas y vulnerabilidades conocidas. Esto es especialmente crítico en un entorno donde la seguridad de los datos es primordial, ya que brinda la oportunidad de tomar medidas antes de que los atacantes puedan explotar estas debilidades.

Durante el proceso de escaneo, Tenable realiza un análisis exhaustivo de las configuraciones del servidor. Esto incluye la verificación de políticas de seguridad, permisos de usuario, puertos abiertos y servicios en ejecución. La herramienta también evalúa la exposición a vulnerabilidades conocidas y proporciona recomendaciones para corregir las configuraciones incorrectas. Corregir estas configuraciones no solo reduce la superficie de ataque, sino que también fortalece la seguridad general del servidor en la figura 11 se presenta la conclusión del escaneo al servidor PW3004Q mediante Tenable. En este escaneo, se identificaron únicamente vulnerabilidades informativas, lo que significa que no se detectaron vulnerabilidades críticas que requieran corrección

**Figura 11**

Escaneo al servidor PW3004Q utilizando la solución de Tenable.



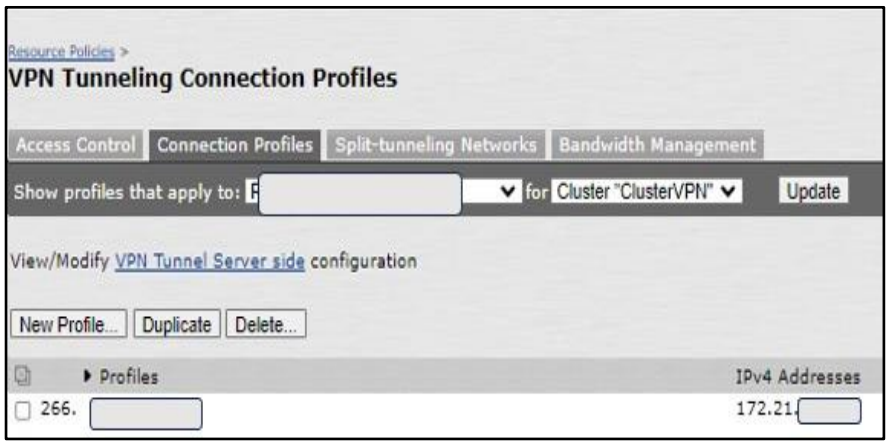

Fuente: Propia

### 3.2.5 Políticas de acceso y autorización

Las VPN (Redes Privadas Virtuales) son vitales en la seguridad y la privacidad de las comunicaciones en línea, y las soluciones de VPN de Pulse Secure son altamente valoradas en este contexto. Una VPN es un servicio que permite a las personas conectarse de forma segura a una red privada desde cualquier lugar del mundo. Esto es importante porque permite a los empleados trabajar desde casa o desde cualquier otro lugar sin comprometer la seguridad de los datos corporativos, en la figura 12 se visualiza la configuración de la IP asignada a un usuario dentro de la plataforma VPN de Pulse Secure.

**Figura 12**

Configuración de IP de un usuario conectado a la VPN




Fuente: Propia

Al conectarse a una VPN de Pulse Secure (o cualquier otra VPN), el dispositivo recibe una nueva dirección IP, para el presente proyecto se determinó a los usuarios que tuvieron acceso al servidor de encriptación, en la figura 13 se visualiza el acceso seguro de Ivanti conectado a una red mediante un túnel VPN.

**Figura 13**

Configuración del equipo conectado a la VPN

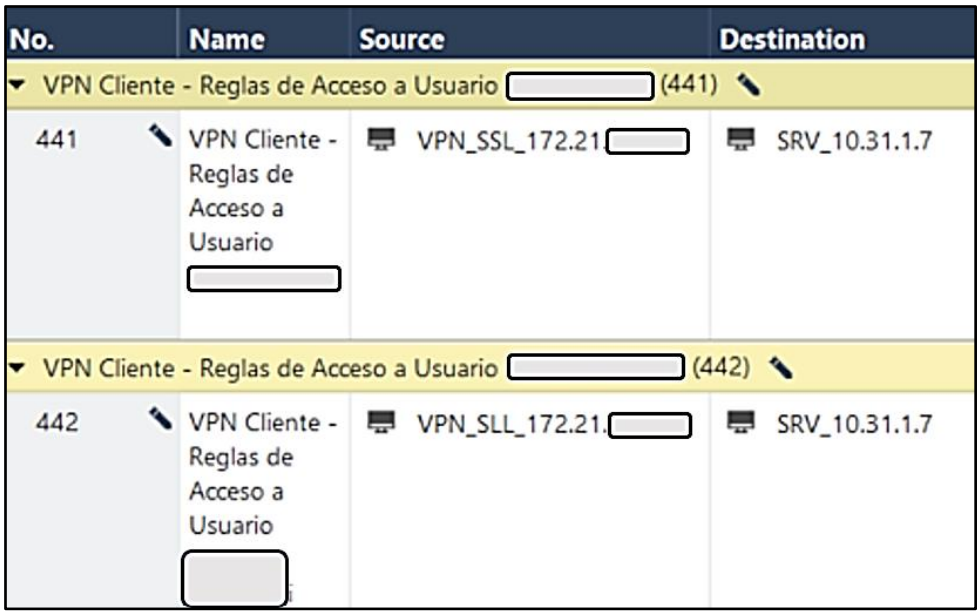

Fuente: Propia

Una vez reconocido el origen (IP VPN del usuario) y el destino (IP del servidor) es de suma importancia establecer las políticas de acceso y autorización que desempeñan un papel fundamental en la estrategia de seguridad de cualquier empresa, especialmente en el contexto de la implementación de un sistema de encriptación con tecnología de BitLocker. Estas políticas están diseñadas para garantizar que solo los usuarios autorizados tengan acceso a los recursos críticos, al tiempo que se mantienen altos niveles de seguridad y prevención de pérdida de datos (DLP).

Para garantizar un acceso controlado a los recursos del servidor, se han definido reglas de acceso en el firewall de Checkpoint. Estas reglas especifican quién puede acceder a qué servicios y desde qué ubicaciones, en la figura 14 se visualiza la regla creada en el firewall para que solo ciertos usuarios tengan acceso al servidor 10.31.1.7 (servidor PW3004Q) a través el puerto 3389 (windows remote desktop), debe considerarse que existe un tiempo de vigencia por cada regla creada.

**Figura 14**

Creación de regla el Firewall Checkpoint que permite conexión hacia el destino 10.31.1.7

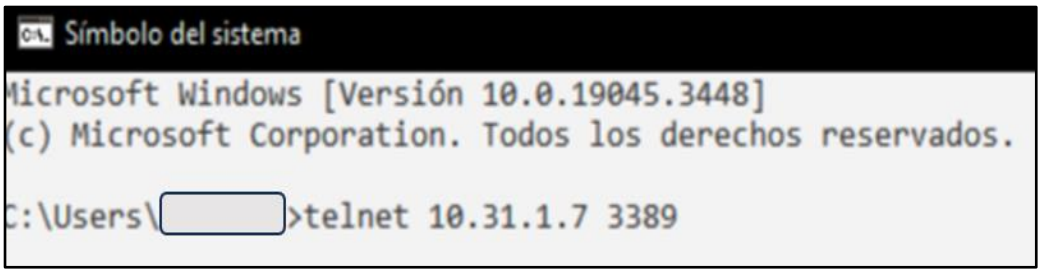



Fuente: Propia

Para validar la conexión establecida desde el origen (IP VPN del usuario) hacia el destino (IP del servidor PW3004Q) se realizaron pruebas para garantizar la efectividad de la solución propuesta y se muestra cómo se ha verificado que los usuarios autorizados puedan acceder a los recursos de manera segura. Para ello, se utilizó el comando Telnet para garantizar la conexión desde la IP VPN del usuario hacia el servidor destino (10.31.1.7), para esto utilizamos el comando “telnet 10.31.1.7 3389”. Cuando ejecutas el comando Telnet seguido de una dirección IP y un puerto, Telnet intentará establecer una conexión con ese servidor en ese puerto específico. Si la conexión es exitosa, Telnet te proporcionará una interfaz de línea de comandos a través de la cual puedes interactuar con el servidor o dispositivo remoto, en la figura 15 se visualiza el comando telnet realizado desde el símbolo del sistema (cmd) hacia el destino indicando el puerto, esto es para validar que el puerto indicado se encuentre abierto y la figura 16 se visualiza la conexión exitosa al servidor destino (10.31.1.7) mediante el puerto indicado (3389) usando el comando telnet.

***Figura 15***

Comando Telnet – Validación puerto




Fuente: Propia

***Figura 16***

Acceso exitoso mediate Telnet


Fuente: Propia

En la figura 17 se muestra la evidencia de tráfico registrado en el firewall, lo que demuestra que las políticas de seguridad están efectivamente implementadas. En esta figura, se observa que la regla permite el tráfico desde la dirección IP 172.21.x.x hacia el puerto 3389 del servidor con la dirección IP 10.31.1.7. Esto implica que cualquier dispositivo con la dirección IP de origen 172.21.x.x puede establecer una conexión con el servidor que se encuentra en la dirección IP 10.31.1.7 a través del puerto 3389.

**Figura 17**

Evidencia de tráfico exitoso hacia el servidor 10.31.1.7

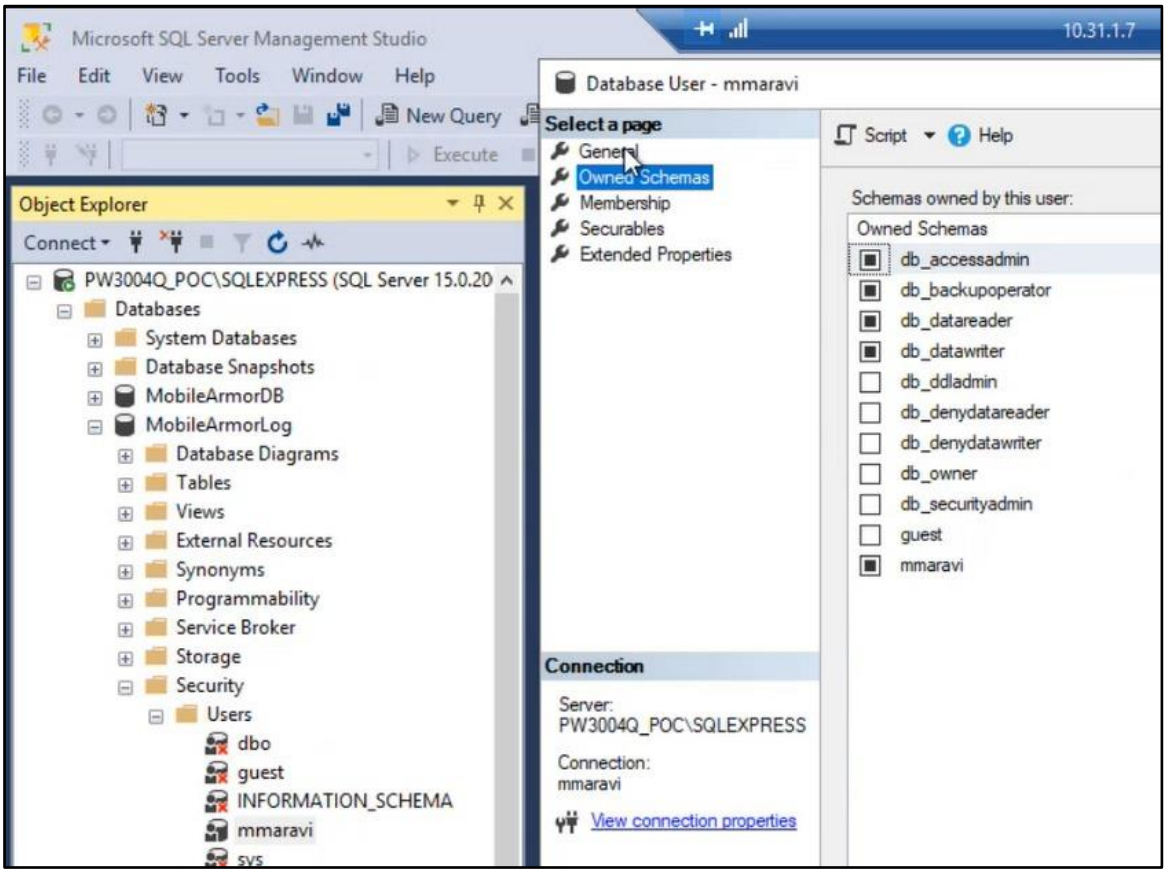

Fuente: Propia

### 3.2.6 Funcionamiento de la solución de encriptación

La implementación del servidor SQL para la solución de implementación es un componente esencial de la solución integral de seguridad y prevención de pérdida de datos (DLP). El servidor SQL se encargará de almacenar los datos de configuración y políticas de la solución, lo que garantizará un funcionamiento eficiente y seguro. La instalación del PolicyServer requiere una base de datos SQL Server para almacenar la configuración de políticas y otros datos. Se crean dos bases de datos: MobileArmorDB que almacena las políticas, configuración del sistema, roles, permisos de usuarios y MobileArmorLog encargada de almacenar los registros, reportes de auditoría y logs. En la figura 18 y figura 19 se muestra la ventana de propiedades del usuario en la base de datos SQL "MobileArmorLog" y "MobileArmorDB" del servidor "PW3004Q" respectivamente. Estos permisos permiten realizar cualquier tarea en la base de datos, incluidas la creación, modificación y eliminación de datos.

**Figura 18**

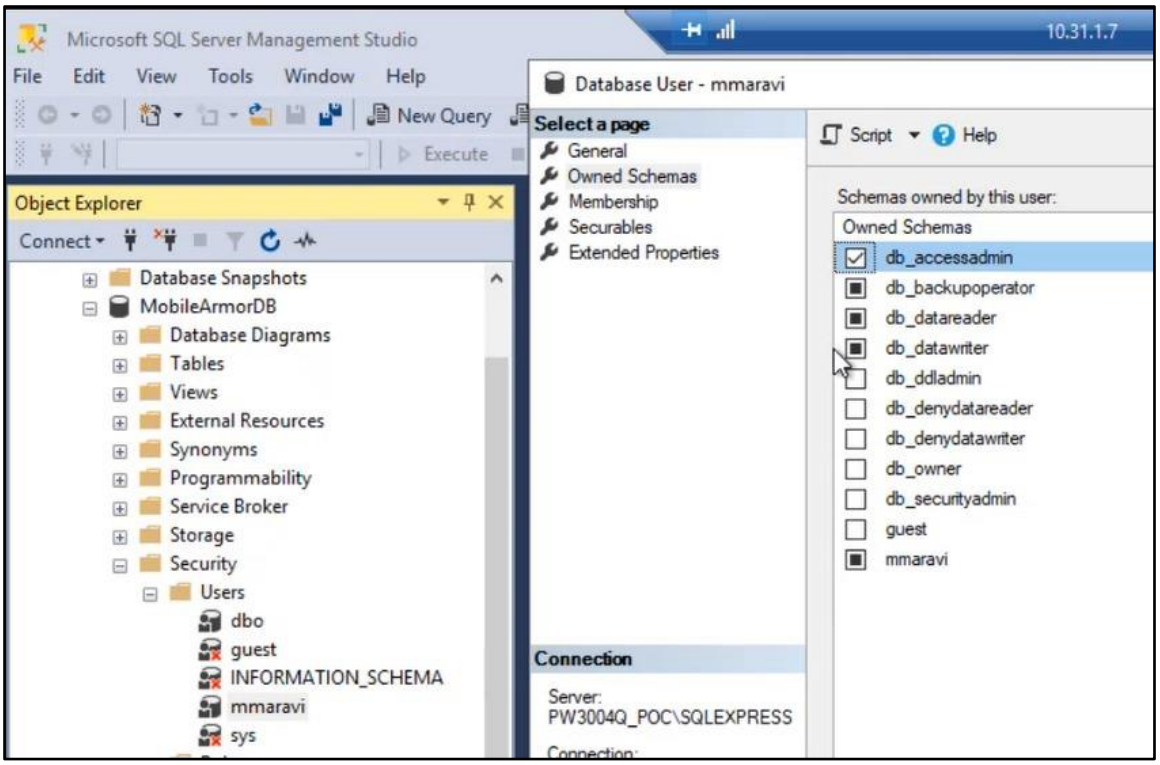
Permisos en la base de datos SQL "MobileArmorLog" del servidor "PW3004Q”




Fuente: Propia

**Figura 19**

Permisos en la base de datos SQL "MobileArmorDB" del servidor "PW3004Q”




Fuente: Propia

Adicionalmente la instalación de PolicyServer es un requisito esencial en la implementación de nuestra solución integral de seguridad y prevención de pérdida de datos (DLP). PolicyServer actúa como un componente central para administrar y controlar la solución, incluyendo la configuración de políticas, la aplicación de cifrado y la generación de informes.

Para el presente proyecto, se llevó a cabo la instalación de PolicyServer siguiendo los procedimientos recomendados por Trend Micro. A continuación, se detallan las acciones tomadas:

- Se descargó la última versión de Policy Server desde el sitio web oficial de Trend Micro. Esta versión fue seleccionada para asegurarse de que se estén utilizando las últimas actualizaciones y características de seguridad.

- Antes de la instalación, se realizó una revisión de los requisitos del sistema para asegurarse de que el servidor cumpliera con las

especificaciones recomendadas por Trend Micro. Esto incluyó la verificación de hardware, sistema operativo y recursos disponibles.

- Se realizó una configuración inicial de PolicyServer, que incluyó la conexión con el Active Directory para obtener información sobre usuarios y grupos de la organización, en la figura 20 se visualiza la creación de la regla desde el origen (servidor) hacia el destino (AD) en donde la acción del tráfico es ser aceptada.

***Figura 20***

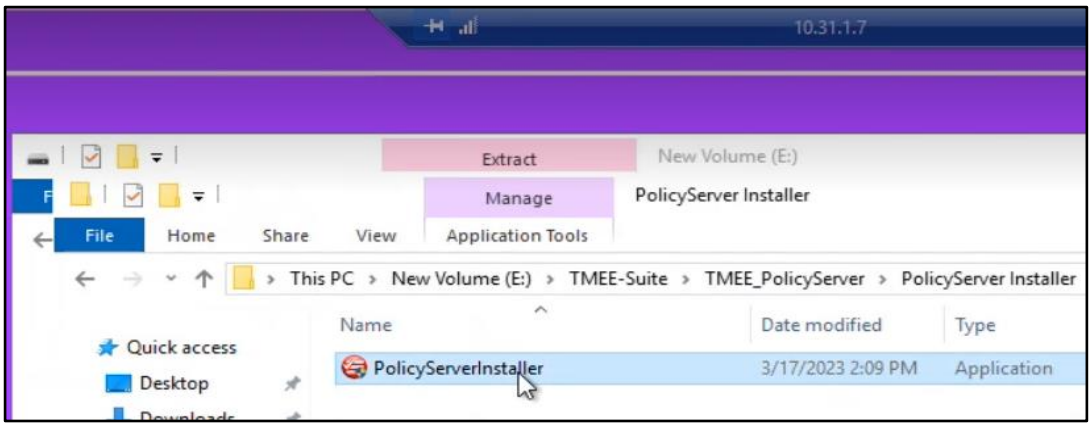
Regla creada en el Firewall desde el servidor hacia el AD


Fuente: Propia

- Se ejecutó el instalador de PolicyServer en el servidor designado para esta función. Durante la instalación, se configuraron las opciones necesarias, como la ubicación de instalación y los ajustes de red, en la figura 21 se observa al agente PolicyServer para ser instalado.

***Figura 21***

Agente PolicyServer



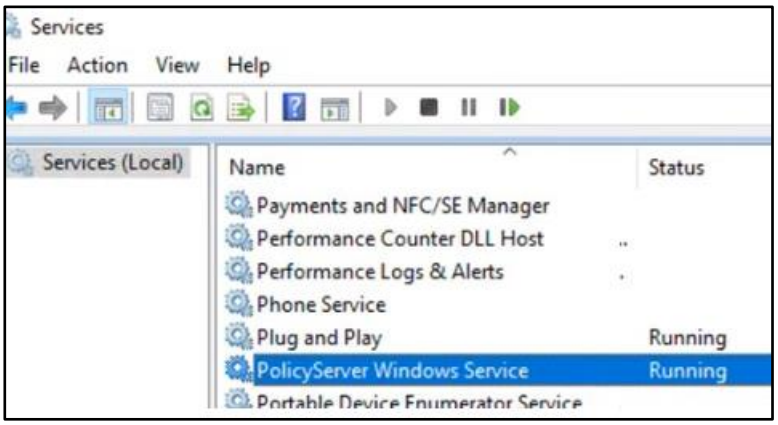

Fuente: Propia

- Se inició con el proceso de instalación del agente ya antes mencionado (en este proceso se consideró a usar la licencia exclusiva

para solución adquirida anteriormente de un paquete de soluciones por Trend Micro por lo que no representó un costo adicional) y se validó que el servicio del agente esté activo y corriendo, en la imagen 22 se visualiza el servicio del agente PolicyServer activo y en estado running.

***Figura 22***

Servicio del PolicyServer activado

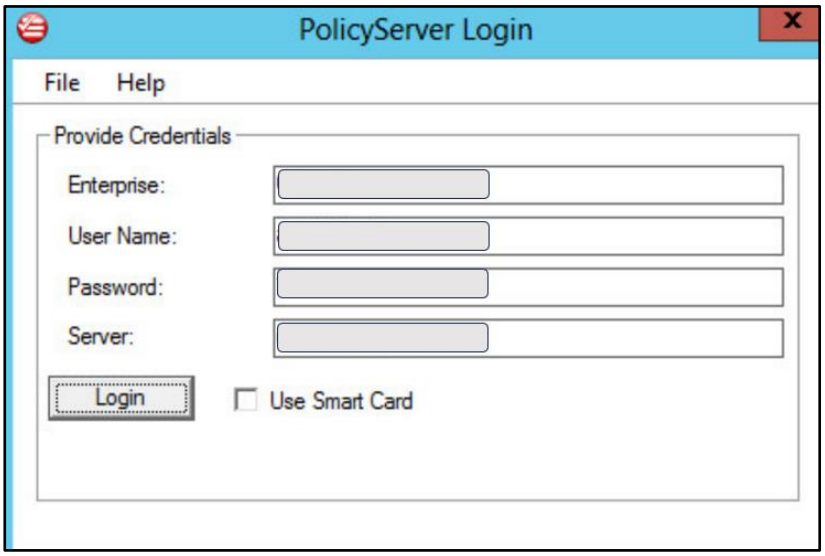



Fuente: Propia

- Una vez realizado con éxito la instalación del agente PolicyServer en el servidor y haber validado que el servicio esté activo, se ingresó las credenciales de usuario administrador local el cual a su vez nos abrirá el PolicyServer MMC, en la figura 23 se observa la pantalla de inicio para administrar la plataforma.

***Figura 23***

Inicio de sesión del PolicyServer




Fuente: Propia

- Después de acceder con los datos solicitados en el PolicyServer, se configuró la política de Full Disk Encryption de Full Disk Encryption por lo que se activó dicha opción, en la figura 24 se observa el acceso exitoso al PolicyServer MMC y las políticas que por default vienen.

***Figura 24***

Configuración de políticas “Full Disk Encryption”


Fuente: Propia

- Luego de realizar la instalación del agente, se establecieron políticas de cifrado iniciales en PolicyServerMMC para los dispositivos de la organización, (cabe indicar que la configuración de estas políticas se llevó a cabo en un servidor publicado en el cual solo se tendrá acceso a través del servidor antes creado) asegurando así que los datos

estén protegidos de acuerdo con las necesidades y regulaciones de seguridad, en la figura 25 se visualiza el mensaje de encriptación exitosa con tecnología Bitlocker y sincronizada con el agente PolicyServer y en la figura 26 se visualiza la encriptación exitosa al equipo con el método de encriptación de XTS - AES 256.

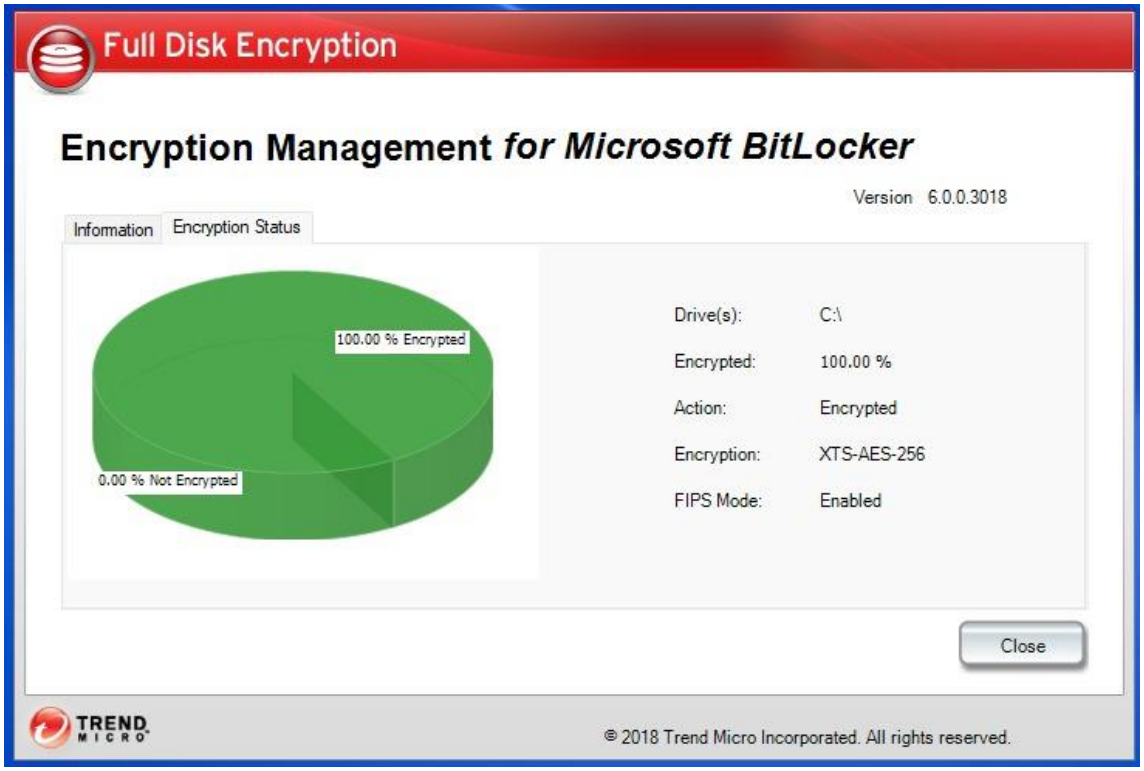
***Figura 25***

Mensaje de encriptación con Bitlocker en sincronización con el agente PolicyServer


Fuente: Propia

***Figura 26***

Encriptación exitosa al equipo




Fuente: Propia

- Validación del cifrado del disco en el equipo, en la figura 27 se observa la correcta encriptación de disco del equipo.

***Figura 27***

Validación de la encriptación bitlocker activada en el equipo del usuario.


Fuente: Propia

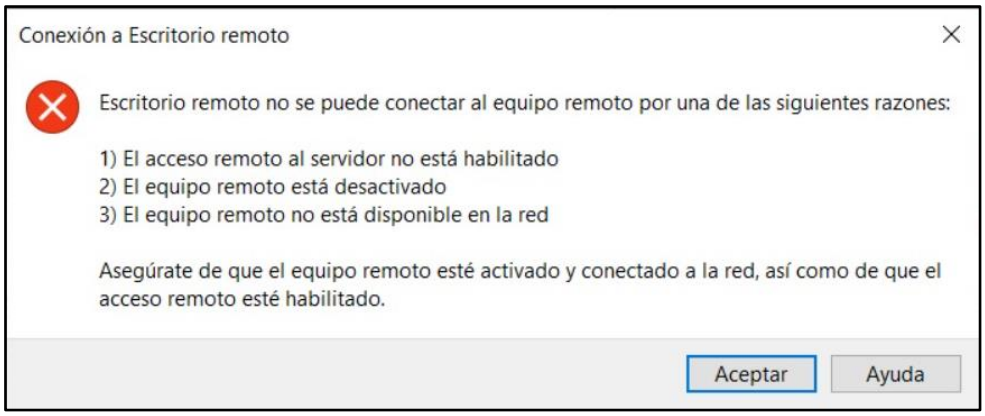
## 3.3 Resultados

### *3.3.1 Políticas de acceso*

En este apartado, se menciona la importancia de las políticas de acceso y autorización en la estrategia de seguridad de la empresa. Se ha creado una regla en el firewall de Checkpoint para permitir que solo ciertos usuarios tengan acceso al servidor 10.31.1.7 a través del puerto 3389 (Windows Remote Desktop). Esto garantiza un acceso controlado a los recursos del servidor y evita que usuarios no autorizados ingresen. Se ha proporcionado evidencia visual de la creación de esta regla en la figura 13, así mismo se realizó la validación de conexión desde un origen diferente reafirmando de esta manera un control de acceso seguro hacia el servidor destino, en la figura 28 se observa el error que se presenta al momento de acceder por escritorio remoto hacia el servidor destino desde un origen no autorizado.

***Figura 28***

Error de conexión por escritorio remoto.




Fuente: Propia

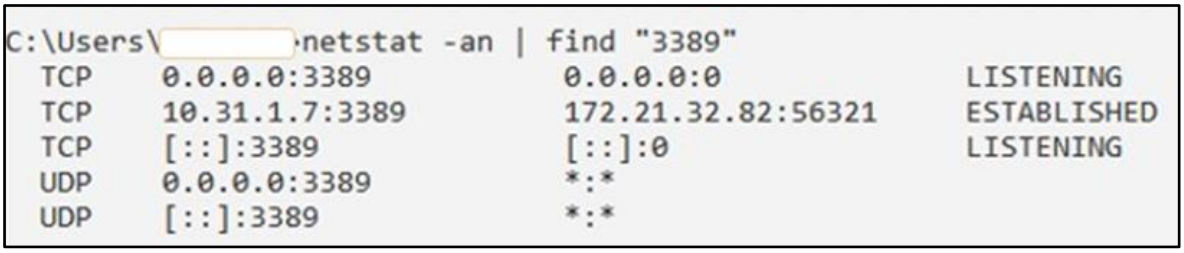
### *3.3.2 Validación de conexión*

Se detallan las pruebas realizadas para garantizar la efectividad de la solución propuesta en términos de acceso y autorización. Se ha utilizado el comando Telnet para validar que el puerto 3389 está abierto y que los usuarios autorizados pueden acceder al servidor de manera segura. Las figuras 15 y 16 muestran el comando Telnet utilizado y la conexión exitosa al servidor, así mismo

se realizó la validación mediante el comando *netstat -an | find "3389"* que sirve para mostrar una lista de todas las conexiones activas en el equipo, en la figura 29 se visualiza una conexión en estado listening, lo que significa que la computadora está lista para aceptar conexiones entrantes en ese puerto, mientras que la otra conexión está en estado established, lo que significa que hay una conexión activa entre dos computadoras.

***Figura 29***

Conexiones activas en el puerto 3389



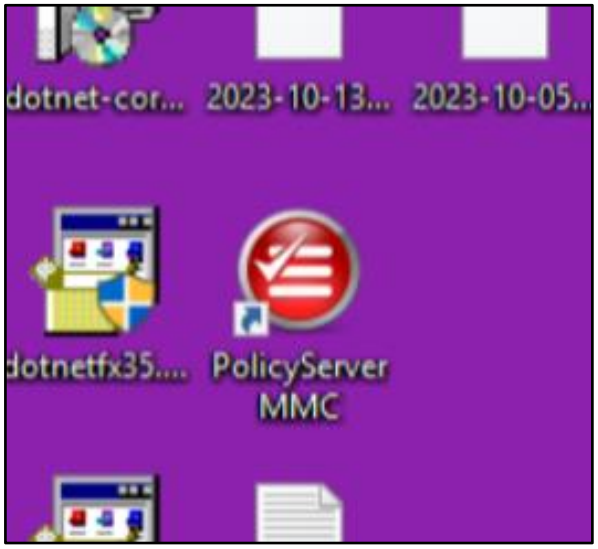

Fuente: Propia

### *3.3.3 Instalación de PolicyServer*

Se describe el proceso de instalación del PolicyServer, que actúa como un componente central para administrar y controlar la solución, incluyendo la configuración de políticas, la aplicación de cifrado y la generación de informes. Las acciones tomadas durante la instalación, como la descarga de la última versión, la revisión de requisitos del sistema y la configuración inicial, se detallan. Se proporciona evidencia visual en las figuras 19, 20, 21, 22 y 23, así mismo, se deja constancia de la instalación del PolicyServer MMC en el servidor PW3004Q en la figura 30 en la cual se observa que el agente antes mencionado se encuentra debidamente instalado.

***Figura 30***

Evidencia de instalación del PolicyServer MMC



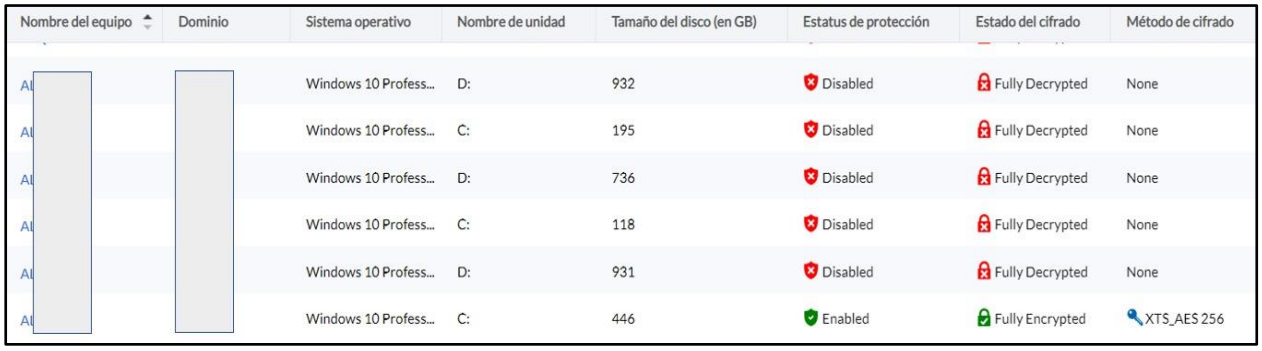

Fuente: Propia

### *3.3.4 Validación de encriptación*

En este apartado, se confirma la implementación de políticas de cifrado en PolicyServerMMC para proteger los dispositivos de la organización. Se detalla la inclusión de equipos en la política de encriptación y se muestra la exitosa encriptación de un equipo utilizando el método de encriptación XTS - AES 256. Las figuras 25 y 26 presentan detalles sobre los equipos incluidos en la política y la validación exitosa de la encriptación en un equipo, así mismo en la figura 31 se visualiza el estado de encriptación en estado activado y desactivado de los equipos de la compañía.

***Figura 31***

Equipos con encriptación de disco activos y no activos



| Nombre del equipo | Dominio | Sistema operativo | Nombre de unidad | Tamaño del disco (en GB) | Estatus de protección | Estado del cifrado | Método de cifrado |
|---|---|---|---|---|---|---|---|
| [redacted] | [redacted] | Windows 10 Profess... | D: | 932 | Disabled | Fully Decrypted | None |
| [redacted] | [redacted] | Windows 10 Profess... | C: | 195 | Disabled | Fully Decrypted | None |
| [redacted] | [redacted] | Windows 10 Profess... | D: | 736 | Disabled | Fully Decrypted | None |
| [redacted] | [redacted] | Windows 10 Profess... | C: | 118 | Disabled | Fully Decrypted | None |
| [redacted] | [redacted] | Windows 10 Profess... | D: | 931 | Disabled | Fully Decrypted | None |
| [redacted] | [redacted] | Windows 10 Profess... | C: | 446 | Enabled | Fully Encrypted | XTS_AES 256 |

Fuente: Propia

## CONCLUSIONES

1. El diseño de la arquitectura planteada en el presente trabajo de investigación varía de acuerdo al total de equipos que se planea trabajar, ya que al ser mayor los dispositivos que cuenten con el agente de encriptación el servidor de base de datos SQL debiese estar instalada en otro servidor.

2. Las políticas de accesos establecidas a nivel firewall para la solución de encriptación con tecnología *BitLocker* dependerán del tiempo de vigencia que se les otorgue debido a que si esta cuenta con un tiempo definido esta caducará haciendo imposible el acceso a la solución en un futuro.

3. El sistema de encriptación es única y exclusiva para sistemas operativos Windows, sea el caso de requerir o utilizar un sistema operativo diferente se deberá utilizar otro agente exclusivo para dicho sistema operativo.

## RECOMENDACIONES

- Diseñar la arquitectura de manera que sea escalable y pueda adaptarse fácilmente a un aumento en la cantidad de equipos.

- Implementar un sistema de alertas o recordatorios que notifiquen al personal de seguridad antes de la caducidad de las políticas, permitirá una renovación oportuna y evitará interrupciones innecesarias en el acceso a la solución de encriptación.

- Crear una estrategia integral de seguridad que abarque todas las plataformas en caso de tener la intención de utilizar múltiples sistemas operativos.

## REFERENCIAS BIBLIOGRÁFICAS


Asurza Cáceres, J. (2022). *Diseño de una arquitectura de seguridad informática para incrementar la seguridad de información en la empresa bafing S.A.C. en 2021.*

Herrera Montano, I., García Aranda, J.J., y Ramos Diaz, (2022). Survey of Techniques on Data Leakage Protection and Methods to address the Insider threat. Cluster Comput 25, 4289–4302 (2022)

Mori Acero, S. (2019). Optimización del algoritmo estándar de encriptación avanzada (AES) para la protección de la información. [Tesis de pregrado, Universidad Peruana Los Andes]. Repositorio

Padilla Vilema, A. E. (2018). Implementación de un esquema de seguridad de aseguramiento lógico en estaciones utilizando un software de protección final para una entidad financiera.

Li, H., Huang, Q., Shen, J. (2019). Designated-server identity-based authenticated encryption with keyword search for encrypted emails. Information Sciences, 481(), 330–343. doi:10.1016/j.ins.2019.01.004

Saenz .L. (2019). Técnicas de transparencia y encriptación de información.

Justiniano C. (2015). Comparación de rendimiento de intercambio de datos con json encriptado.

Liu, S., & Kuhn, R. D. (2010). Data loss prevention. IT Professional, 12(2), 10-13. doi:10.1109/mitp.2010.52

Orihuela. Q. (2022). Programa de seguridad de información ante ciber ataques de ingeniería social para empleados de una compañía de telecomunicaciones de Lima.

Guerreiro, J., Batista, E., Monteiro, E., & Silva, L. M. (2018). Cyber Threats Information Sharing: Survey and Research Directions. En WorldCIST'18 2018 6th World Conference on Information Systems and Technologies (pp. 1195-1204). Springer, Cham.

Ronald S., Segundo M. (2019). Implementación de una VPN con open source para la gestión de aplicaciones de intranet en la Universidad Nacional Pedro Ruiz Gallo.

Radwan, M. A. (2016). Modelo de Encriptación Simétrica Basada en Atractores Caóticos. Ingeniería, 20(1), 1-10.

Nyarko, R. (2018). Security of Big Data: Focus on Data Leakage Prevention (DLP).

Herrera Montano, I. (2022). Survey of Techniques on Data Leakage Protection and Methods to address the Insider threat. Cluster Computing, 25(6), 4289-4302

Rudnytskyi, V., Korchenko, O., Lada, N., Ziubina, R., Wieclaw, L., & Hamera, L. (2022). Cryptographic encoding in modern symmetric and asymmetric encryption. Journal of Ambient Intelligence and Humanized Computing, 13(11),12

Khoumsi, A., Erradi, M., & Krombi, W. (2016). A formal basis for the design and analysis of firewall security policies. Journal of King Saud University – Computer and Information Sciences, 28(4), 427-436.

Ivanti. (2023). Habilite a su personal remoto con una conectividad segura https://www.ivanti.com/es/products/secure-connectivity.

Microsoft. (2023). Introducción a BitLocker https://learn.microsoft.com/es-es/windows/security/operating-system-security/data-protection/bitlocker/

Microsoft. (2023). Dirección IP https://learn.microsoft.com/es-es/purview/sit-defn-ip-address

Google. (2023). Cómo aumenta la seguridad la encriptación de extremo a extremo de Mensajes
https://support.google.com/messages/answer/10262381?hl=es-419#:~:text=La%20encriptaci%C3%B3n%20convierte%20los%20datos,con%20el%20que%20intercambias%20mensajes.

Caiza Navas, A. G. (2019). *Diseño de un proceso de hardening de servidores para una institución financiera del sector público*.

Tenable Io. (2023). Tenable Vulnerability Management
https://es-la.tenable.com/products/tenable-io

Trend Micro. (2023). Protegemos el mundo conectado
https://www.trendmicro.com/es_es/about.html

IBM. (2021). Cifrado de datos en reposo (data-at-rest)
https://www.ibm.com/docs/es/xiv-storage-system?topic=STJTAG/com.ibm.help.xivgen3.doc/Gen3/PO/xiv_gen3_po_ch_data_at_rest_encryption.htm

Avast. (2020). Cifrado de datos en tránsito.
https://blog.avast.com/es/data-in-transit-encryption

Ikusi (2023). Cifrado de datos: beneficios de su aplicación en la nube
https://www.ikusi.com/mx/blog/cifrado-de-datos-beneficios-de-su-aplicacion-en-la-nube/

Statista (2023). Crímenes con mayor tasa de víctimas en áreas urbanas de Perú entre enero y junio del 2023
https://es.statista.com/estadisticas/1290030/tasa-de-victimas-por-hecho-delictivo-peru/#:~:text=Per%C3%BA%3A%20tasa%20de%20v%C3%ADctimas%20por%20hecho%20delictivo%20en%202023&text=Entre%20enero%20y%20junio%20de,un%20robo%20de%20estas%20caracter%C3%ADsticas.

Microsoft (2023). Cifrado
https://learn.microsoft.com/es-es/purview/encryption

Vaheedbasha, S., Natajaran, K. (2022). Flexible and cost-effective cryptographic encryption algorithm for securing unencrypted database files at rest and in transit - ScienceDirect

Trend Micro (2023). Anti-malware y Advanced Threat Protection https://www.trendmicro.com/es_es/business/capabilities/antimalware-atp.html

Coellar, J,. y Cedeño, J. (2013) Propuesta para la transición de IPV4 a IPV6 en el Ecuador a través de la Supertel.

# ANEXO

## Anexo A. Requerimientos del servidor de gestión (Policy Server)

| Devices | PolicyServer Front-end Requirements | PolicyServer SQL Database Requirements |
|---|---|---|
| 1,000 | • One front-end and SQL database multi-role server with an Intel Xeon quad-core 2.2 GHz processor or above<br>• 8 GB RAM<br>• 120 GB hard drive | Installed on PolicyServer front-end server |
| 4,000 | • One front-end and SQL database multi-role server with an Intel Xeon quad-core 2.2 GHz processor or above<br>• 8 GB RAM<br>• 150 GB hard drive | Installed on PolicyServer front-end server |
| 8,000 | • Two front-end servers each with an Intel Xeon quad-core 2.2 GHz processor or above<br>• 4 GB RAM<br>• 40 GB hard drive | • One SQL database server with an Intel Xeon quad-core 2.2 GHz processor or above<br>• 8 GB RAM<br>• 150 GB hard drive |
| 20,000 | • Four front-end servers each with an Intel Xeon quad-core 2.2 GHz processor or above<br>• 4 GB RAM<br>• 40 GB hard drive | • Two SQL database servers (one for the policy database and one for the log database) each with an Intel Xeon quad-core 2.2 GHz processor or above<br>• 8 GB RAM<br>• 180 GB RAID 5 hard drive |
| 40,000 | • Eight front-end servers each with an Intel Xeon quad-core 2.2 GHz processor or above<br>• 4 GB RAM<br>• 40 GB hard drive | • Two SQL database servers (one for the policy database and one for the log database) each with an Intel Xeon quad-core 2.2 GHz processor or above<br>• 16 GB RAM<br>• 350 GB shared SAN RAID 5 hard drive |

## Anexo B. Requerimiento de clientes a cifrar a través de MS BitLocker

| Specification | Requirements |
|---|---|
| Processor | Intel Core 2 Duo 2.0 GHz processor or equivalent |
| RAM | Requirements are the based on Windows system requirements:<br>• 64-bit systems: 2 GB<br>• 32-bit systems: 1 GB |
| Disk space | • 30 GB<br>• 20% free disk space |
| Hard disk | • Standard drives supported by Windows<br>**Important:**<br>Encryption Management for Microsoft BitLocker installation is only supported on endpoints with 1 physical hard disk drive (multiple partitions are supported). |
| Network connectivity | Connectivity with PolicyServer |
| Operating system | • Windows™ Embedded POSReady 7 (32-bit/64-bit)<br>• Windows™ 11 Enterprise and Professional editions (64-bit)<br>• Windows™ 10 Enterprise and Professional editions (32-bit/64-bit)<br>• Windows™ 8.1 Enterprise and Professional editions (32-bit/64-bit)<br>• Windows™ 8 Enterprise and Professional editions (32-bit/64-bit)<br>• Windows™ 7 Enterprise and Professional editions (32-bit/64-bit) |