NOMBRE DEL TRABAJO

Implementación de un sistema de protección de fuga de datos en puntos finales, por medio de la aplicación de una directiva DLP de la marca Trellix

AUTOR

Jorge Manuel Susanibar Herrera

RECUENTO DE PALABRAS

18168 Words

RECUENTO DE CARACTERES

95146 Characters

RECUENTO DE PÁGINAS

99 Pages

TAMAÑO DEL ARCHIVO

25.9MB

FECHA DE ENTREGA

Feb 28, 2024 7:41 PM GMT-5

FECHA DEL INFORME

Feb 28, 2024 7:42 PM GMT-5

- 13% de similitud general

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

- **13% Base de datos de Internet**
- **Base de datos de Crossref**
- **0% Base de datos de trabajos entregados**
- **3% Base de datos de publicaciones**
- **Base de datos de contenido publicado deCrossref**

UNIVERSIDAD NACIONAL TECNOLÓGICA DE LIMA SUR

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

(Art. 45º de la ley Nº 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. 10º 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: Susanibar Herrera Jorge Manuel
D.N.I.: 77282544
Otro Documento: ----------
Nacionalidad: Peruana
Teléfono: 934876594
e-mail: 2014201053@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 protección de fuga de datos en puntos finales, por medio de la aplicación de una directiva DLP de la marca Trellix
Fecha de Sustentación: 16 de diciembre del 2023
Calificación: Aprobado con Distinción
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

UNIVERSIDAD NACIONAL
TECNOLÓGICA DE LIMA SUR

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

Atribuciones de acceso restringido:

Las atribuciones de acceso son para Restricted Access, la cual es para documentos restringidos.

Motivos de la elección del acceso restringido:

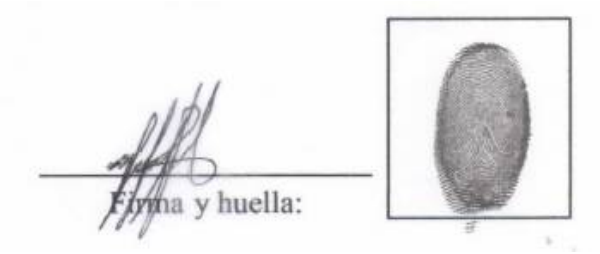
El motivo de la elección de acceso restringido al trabajo de suficiencia profesional, es debido a que en dicho trabajo se presenta información vital y personal de la empresa en donde se realizó el trabajo de suficiencia, por tal motivo la información dentro del trabajo es de carácter sensible.

Susanibar Herrera Jorge Manuel

APELLIDOS Y NOMBRES

77282544

DNI



Lima, 01 de Marzo 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 PROTECCIÓN DE FUGA DE DATOS EN PUNTOS FINALES, POR MEDIO DE LA APLICACIÓN DE UNA DIRECTIVA DLP DE LA MARCA TRELLIX”

TRABAJO DE SUFICIENCIA PROFESIONAL

Para optar el Título Profesional de

INGENIERO ELECTRÓNICO Y TELECOMUNICACIONES

PRESENTADO POR EL BACHILLER

SUSANIBAR HERRERA, JORGE MANUEL
ORCID: 0009-0005-2043-2577

ASESOR

QUISPE AGUILAR, MAX FREDI
ORCID: 0000-0002-4199-0974

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 16:44 horas del día 16 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	:	DR. MARK DONNY CLEMENTE ARENAS	CIP Nº 181400
Secretario	:	MG. LUDWIG PASCUAL LÓPEZ HUAMAN	CIP Nº 310375
Vocal	:	MG. MARTHA ROXANA QUISPE AYALA	CIP Nº 124612

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 **JORGE MANUEL SUSANIBAR HERRERA**
Sustentó su Trabajo de Suficiencia Profesional: **IMPLEMENTACIÓN DE UN SISTEMA DE PROTECCIÓN DE FUGA DE DATOS EN PUNTOS FINALES, POR MEDIO DE LA APLICACIÓN DE UNA DIRECTIVA DLP DE LA MARCA TRELLIX**

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

Condición APROBADO CON DISTINCION Equivalencia MUY BUENO .....de acuerdo al Art. 65º del Reglamento General para el Otorgamiento de Grado Académico y Título Profesional de la UNTELS vigente.

Siendo las 17:19 horas del día 16 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
DR. MARK DONNY CLEMENTE ARENAS
CIP N° 181400

SECRETARIO
MG. LUDWIG PASCUAL LÓPEZ HUAMAN
CIP N° 310375

VOCAL
MG. MARTHA ROXANA QUISPE AYALA
CIP N° 124612

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 categoria y antigüedad. En caso de ausencia de dos o más miembros del jurado, la sustentación será reprogramada durante los 05 días siguientes.

DEDICATORIA

A mi familia y amigos cercanos por apoyarme en cada momento crucial en mi vida y mostrarme con su ejemplo lo importante que es el seguir adelante.

AGRADECIMIENTO

A mi familia, amigos y compañeros del trabajo por alentarme a cumplir mis sueños y en especial a L. Suárez por su apoyo incondicional.

ÍNDICE

LISTADO DE FIGURAS

LISTADO DE TABLAS

RESUMEN

En el presente trabajo de titulación se realizó la implementación de una directiva de Data Loss Prevention (DLP) con sus respectivas reglas de bloqueo de acuerdo a lo requerido por la empresa para su funcionamiento del día a día en las diferentes gestiones del área en la cual fue implementada.

Dichas reglas se enfocan en la prevención de fuga de información a través de diferentes medios de transferencia de datos, tales como: los periféricos de salida y transferencia de datos (puerto USB), envió de información a través de mensajería instantánea (correo electrónico) y transferencia de información a través de la tecnología Bluetooth.

La configuración antes indicada se aplicó en el área de ingeniería a fin de poseer una mayor seguridad y control ante posibles ataques internos de fuga de información los cuales podrían repercutir en posibles pérdidas monetarias y de activos informáticos a la empresa.

En una primera etapa se procedió a crear la Directiva DLP con sus respectivas reglas y se aplicó la configuración a la máquina virtual “WIN10-19045-22H”, con lo cual se obtuvo excelentes resultados en cada escenario de prueba; para posteriormente proceder a realizar la implementación de la directiva y sus reglas en los equipos empresariales.

Luego del proceso de implementación en los equipos empresariales del área de ingeniería aplicando un monitoreo constante al cabo de un periodo de 3 meses. Se pudo observar en el panel de administración de eventos relacionados a DLP, más de 2500 registros de alertas detonadas por la infracción de las reglas configuradas en la directiva, así como el usuario que originó la alerta y la fecha en la cual surgió.

INTRODUCCIÓN

Junto con los avances tecnológicos que se han estado presentando durante la última década, surgieron diferentes formas de extraer información de entidades públicas o privadas, lo cual conlleva a un riego de vulnerabilidad de las organizaciones ya que terceros pueden obtener información delicada de los clientes afectando la integridad y confidencialidad de la empresa.

Con la intención de mantener la información protegida se crean las normativas internacionales como el ISO27001 e ISO27002 que se enfocan en la confidencialidad, integridad y disponibilidad de la información, así como las leyes de protección de la información que son creadas en cada país específicamente.

Para el año 2023 el Perú está dentro del top de los 5 países de Latinoamérica con más ciberataques registrados por lo cual se ve la necesidad por parte de las empresas de encontrar una forma o medio como mitigar estos riesgos y mantener su información protegida.

Debido a la situación presentada se optó por aplicar una directiva DLP de la marca Trellix la cual se centra en un diseño de red que utiliza un servidor donde se va almacenar todos los registros de usuarios pertenecientes a la empresa (Active Directory), un servidor SQL el cual contendrá todos los registros correspondientes a la consola ePO y un tercer registro que contendrá todos los eventos relacionados al DLP.

Cabe indicar que el DLP de la marca Trellix se encuentra dentro del top 3 respecto a la clasificación de Gartner el cual nos presenta los mejores softwares utilizados a nivel internacional que se orientan a la protección de datos y posibles fugas de información así mismo se contó con la facilidad de tener instalado la solución ePO el cual es la consola principal de administración de los eventos DLP por lo cual se pudo obtener una licencia permanente correspondiente a dicho módulo.

CAPÍTULO I. ASPECTOS GENERALES

1.1 Contexto

Debido al constante crecimiento de las tecnologías, surgen los ciberdelincuentes cuyo afán se centra en robar información confidencial y vital a los usuarios de las empresas que cuentan con credenciales de acceso a información imprescindible de las organizaciones en las cuales laboran.

Al ver que el aspecto digital en el mundo se está acrecentando; Securesoft tiene como Misión el estar presente en la transformación Digital de sus clientes, aportando con sus servicios ya sea a través de productos, servicios de ciberseguridad o también consultoría. De este modo busca garantizar ingresos rentables para sus accionistas, desarrollo profesional para el personal de la empresa y un servicio óptimo para sus clientes.

Cabe resaltar que la visión de la empresa está enfocada en ser el líder en el mercado relacionado a la ciberseguridad en todo Latinoamérica para el 2025.

Los servicios ofrecidos por la empresa Securesoft van desde consultoría para la evaluación de Hardening, Capacitación sobre Etical Hacking, análisis de vulnerabilidades, análisis forense, análisis de código fuente, entre otros.

Otro servicio brindado es el servicio de cyberSOC el cual consiste en el monitoreo y notificación del estado de salud de las plataformas administradas, así como también el alertamiento en caso surja algún evento de seguridad o de ciber inteligencia.

Adicional a ello otro servicio ofrecido es el de Ingeniería de los productos, en cual se le brinda soporte al cliente con respecto a las plataformas administradas, dicho soporte puede abarcar configuraciones en las soluciones, integraciones con otras soluciones o implementaciones de las soluciones adquiridas por los clientes.

1.2 Delimitación temporal y espacial del trabajo

1.2.1 Temporal

El proyecto se desarrolló entre los meses de mayo a julio del 2023. Dicho proyecto se divide en 3 etapas acentuadas: levantamiento de información, implementación en equipos de pruebas y validación en equipos reales.

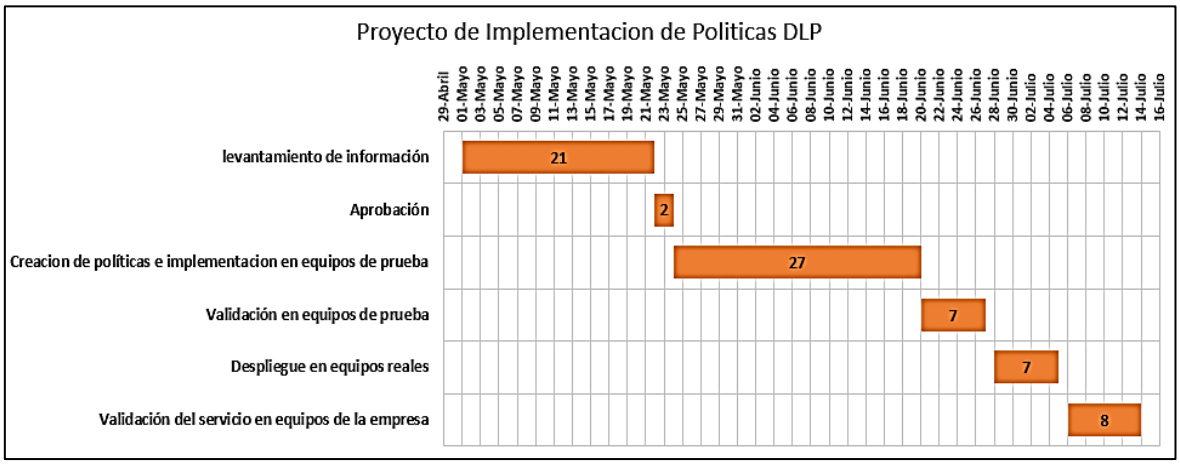


Figura 1. Cronograma del proyecto.
Fuente: Elaboración Propia

1.2.2 Espacial

La realización del proyecto se realizó en el edificio 325 piso 14, ubicado en la avenida Manuel Olguin distrito de Surco, dicho lugar es administrado por la empresa Securesoft.

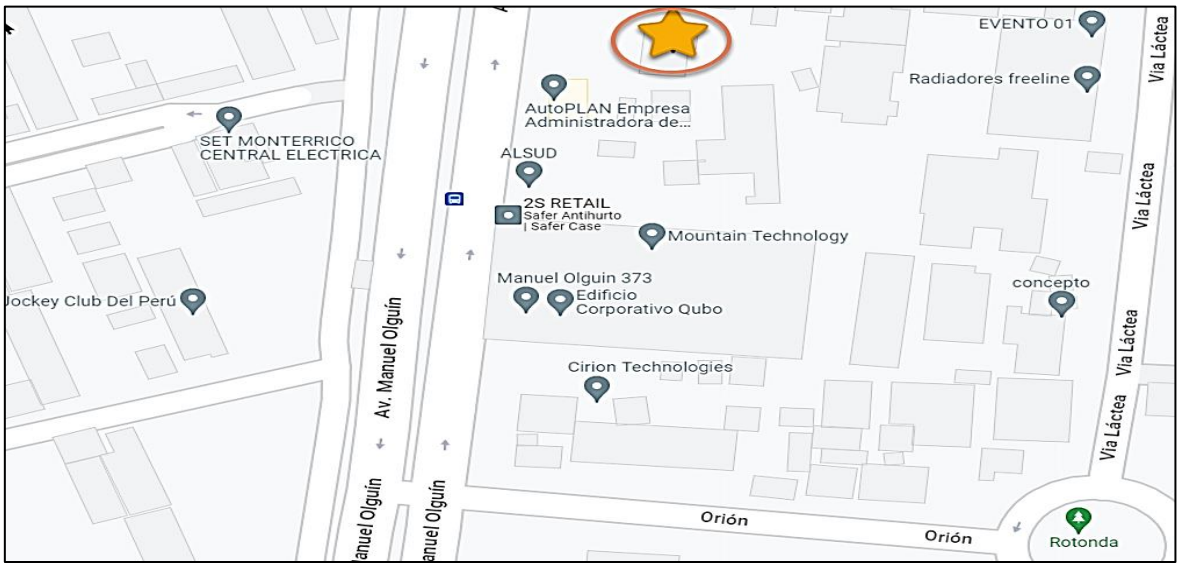


Figura 2. Plano de ubicación de la empresa
Fuente: Elaboración Propia

1.2.3 Teórico

En el trabajo presentado se aplicó las reglas de bloqueo de unidades externas (a través de puertos USB), el bloqueo de correos si se encuentran dentro de la base de datos de lista negra, así como también el bloqueo de bluetooth para los equipos que tengan instalado el agente Trellix con el módulo DLP.

1.3 Objetivos

1.3.1 Objetivo general

Implementar un sistema de Protección a los puntos finales de la empresa, asegurando la información sensible ante cualquier amenaza externa o interna que pueda incurrir a pérdidas potenciales de información o activos.

1.3.2 Objetivo específico

- Análisis de la red y diseño de directiva Trellix con módulo DLP a fin de proteger la información vital de la empresa Securesoft.
- Implementación de la directiva DLP Trellix a los puntos finales, a fin de proteger la información vital dentro de la empresa Securesoft.
- Validar una correcta aplicación y funcionamiento de los niveles de protección en los puntos finales a fin de prevenir posibles fugas de información.

CAPÍTULO II. MARCO TEÓRICO

2.1 Antecedentes de la Investigación

2.1.1 Antecedentes Internacionales

(Godínez Chávez & Olvera Espinoza, 2017) en su tesis titulada “Implementación de un sistema DLP (Data Loss Prevention), México, para optar el título de Ingeniería en computación. Plantearon que las vulnerabilidades no solo se presentan en grandes empresas las cuales tienen los recursos necesarios para poder combatir y prevenir este tipo de amenazas, si no también sucede en mayor medida en las empresas medianas y pequeñas, ya que estas no cuentan con un sistema de prevención ante el robo de su información y no están bien informadas respecto a este tipo de vulnerabilidades ante las cuales están expuestas. Por lo cual hacen uso de políticas DLP en la solución Symantec para poder prevenir y monitorear este tipo de vulnerabilidades, generando un índice de seguridad óptima; concluyen que el uso de políticas DLP utilizando soluciones como Symantec mejora la seguridad informática y además es rentable.

En el trabajo antes presentado, se encontraron similitudes con el nuestro, debido a que en ambos trabajos se hace uso de soluciones DLP para subsanar el problema de la fuga de información, con la diferencia que en el trabajo antes mencionado se hizo uso de la solución Symantec. Así mismo con ello se puede confirmar que el uso de DLP es una solución viable y rentable

(Lagua Gavilanes, 2021) en su proyecto titulado “Herramientas Data Loss Prevention (DLP) OpenSource, Para seguridad de la información”, Ecuador, para optar el grado de Magíster en Ciberseguridad. Expuso que en la actualidad la información digital es uno de los activos más importantes que tienen las empresas, ya sean que estén orientadas a la educación, economía, política, entretenimiento, etc. Ante esta situación también existen riesgos que ponen en peligro la Seguridad de la información de dichas empresas, por lo cual Lagua hace uso de múltiples metodologías, tales como el deductivo, inductivo y experimental a fin de poder implementar un prototipo de un DLP de código abierto. Realizo su aplicación a la infraestructura de la PUCESA, con lo que el autor concluye que en la actualidad los DLP OpenSource tienen múltiples limitaciones además de estar siendo comprados

por otros fabricantes de marcas conocidas debido a que los DLP de código abierto están causando mucho revuelo en el mercado de esta solución.

En el trabajo antes mencionado se hizo uso de DLP al igual que en nuestro proyecto, con la diferencia que el autor utilizo el tipo de DLP de código abierto lo cual difiere con lo realizado en nuestro trabajo de implementación brindándonos otro enfoque. Así mismo gracias a lo concluido por el auto en su tesis y en base a sus resultados; podemos resaltar que es preferible utilizar softwares DLP de código de paga, debido a que estos no cuentan con tantas limitaciones.

(Vaca Escobar, 2019) en su trabajo titulado “Modelo de gestión de seguridad lógica de la información en la protección de los datos sensibles de los distritos de educación del Ecuador”, Ecuador, para optar el grado de Maestría en gerencia de sistemas de información. Expuso que los ciberdelincuentes hacen uso de diferentes métodos o materiales para poder tener acceso a información vital de las empresas. Entre alguno de estos métodos se encuentran el uso de Keyloggers (software que guarda un registro de lo que se digite en el teclado a fin de obtener información sobre activos valiosos), el uso de ataques de fuerza bruta (Consiste en probar diferentes combinaciones de contraseñas a fin de obtener accesos), entre otro tipo de métodos. Por lo cual el sistema de seguridad informática (SI) debe ser un proceso sistemático y reconocido por toda la empresa a fin de mantener la seguridad de la información lo más segura posible. Ante ello Vaca propuso un modelo de seguridad con el fin de proteger datos confidenciales aplicando un modelo de gestión Siendo dicho modelo un marco que integra rasgos, indicadores, entre otros, con lo que se podría tener referencias de buenas prácticas del cuidado de la información manejo de Normas y estándares Internacionales tales como, la ISO 27001 y la Ley Federal de protección de Datos Personales en Posesión de Particulares (LFPDPPP) de México. Concluyo que al implementar el modelo propuesto logro disminuir el 46% de los posibles riesgos y superficies de ataques a los datos personales o activos.

En el trabajo antes mencionado, al igual que en nuestro proyecto se tomó como referencia normas y estándares internacionales, así mismo dicho trabajo difiere con el nuestro en el sentido que el auto no se enfocó en el uso de Herramientas que apoyen a la seguridad. Al contrario, enfatizó la importancia de un buen sistema de

seguridad y políticas que apoyen y respalden dicho esquema, con lo cual podemos rescatar que el uso de normas y estándares acompañados de una buena herramienta de seguridad de la información como lo es el DLP puede mejorar en una gran escala la seguridad de los activos informáticos.

2.1.2 Antecedentes Nacionales

(Salinas Tomapasca, 2020) en su tesis titulada “Modelo de Ciberseguridad para cajas municipales en tiempos de Transformación digital un nuevo enfoque”, Trujillo, para optar el grado de magíster en Ingeniería de sistemas con mención en gerencia de sistemas de información. Expuso que una empresa debe cuidar su información sensible de ataques externos empleando una seguridad perimetral, la cual involucra los enrutadores que se encargan de dar paso al tráfico de red para no terminar en redes no confiables. Dicho sistema de seguridad se complementa con el cortafuegos, el cual tiene una serie de reglas que permitirá o denegará el paso del tráfico de red. El autor planteo el uso de un sistema de detección de intrusos, el cual es usado para localizar actividades sospechosas dentro la red y por último planteo el uso de un sistema de prevención de intrusiones, el cual aparte de poder detectar alguna intrusión, se defiende de forma automática sin interactuar directamente con el administrador. Por el lado interno de la seguridad de la información se plantea el modelo de *Zero Trust* en donde se establece la disminución de privilegios excesivos a los usuarios ya que si no se tiene cuidado los usuarios pueden descargar cualquier programa desde la red y con llevar a una vulnerabilidad. Salinas implemento el modelo de seguridad de Zero Trust basado en NIST y recomendó la implementación de este, a fin de proteger los datos empresariales y personales en los dispositivos de forma interna y así establecer una seguridad más solida

En el trabajo antes mencionado, al igual que en nuestro trabajo se resaltó la importancia de mantener segura la información del personal, así como la información de los clientes y de la empresa, pero a diferencia nuestra el autor aplica otro tipo de solución a fin de disminuir la superficie de vulnerabilidad en su empresa. Podemos observar un enfoque diferente debido a que no solo se debe tener en cuenta la protección contra amenazas internas si no también las amenazas externas deben ser consideradas; dicho punto de vista se podría tener en cuenta

al momento de realizar una mejora en la configuración de algunas reglas de DLP a futuro.

(Asurza Cáceres, 2022) en su tesis titulada “Diseño de una arquitectura de seguridad informática para incrementar la seguridad de información de la empresa Bafing S.A.C en 2021”, Lima, para optar el título profesional de Ingeniero de Sistemas Empresariales. Expuso que ante las innovaciones en tecnología las cuales contribuyen al desarrollo de las empresas y al trabajo, se les otorga a las computadoras un valor como activo muy importante debido a que el personal de las empresas almacena información imprescindible dentro de ellas. Por ello surge la necesidad de mantener controlada y supervisada la información que se transmite a través de los ordenadores de la empresa. Asurza estableció en su trabajo una arquitectura de seguridad, La cual tenía reglas y normas en el control de la información, además realizo la selección de la herramienta a utilizar mediante entrevistas y consultas a especialistas. Con su arquitectura de seguridad logro incrementar el nivel de integridad, confidencialidad y disponibilidad de los datos protegidos, aumentando el alcance de protección en los activos.

En el trabajo antes expuesto se presentó la importancia de la protección de la información y el uso de herramientas que apoyen a dicha causa al igual que en nuestro trabajo, con la diferencia que el autor hizo uso de dos soluciones diferentes las cuales son: el Kaspersky y el Mvision DLP a fin de buscar una combinación adecuada. Debido a ello, se debe resaltar que no es cuestión de buscar el mejor software en el mercado, sino buscar el mejor que se acomode a nuestras necesidades y haga frente a las posibles amenazas a las cuales podríamos estar expuestos.

2.2 Bases Teóricas

2.2.1 Ciberseguridad

En la actualidad el uso de la tecnología ha aumentado drásticamente y con ello se genera información o activos digitales, los cuales son transferidos constantemente por la red tanto de la misma empresa como en la nube. En este proceso existen vulnerabilidades tanto en la red como en los dispositivos que contengan dicha información, la cual puede ser aprovechada por ciberdelincuentes que podrían infiltrarse en las organizaciones y esto conllevaría a la caída de los entes

empresariales. Por ello la ciberseguridad, consiste en la protección de información en redes y programas haciendo uso de herramientas de detección, gestión de riegos y la misma tecnología a fin de prevenir y hacer frente a posibles ataques informáticos. Así mismo el proceso de ciberseguridad está formado por tres entidades (Kiser, 2020).

- **Personas:** Son parte del organismo empresarial, mientras formen parte de la institución, deben tener en cuenta y aplicar una cultura de seguridad de sus activos informáticos, tal como respaldar su información, cambiar sus contraseñas periódicamente, estar atentos a posibles correos o adjuntos maliciosos, etc.
- **Procesos:** Las organizaciones deben tener implementado ciertos procesos o marcos bien establecidos con los cuales puedan seguir y hacer frente a posibles ataques a su ciberseguridad, este factor es vital que este implementado y sea conocido a fin sufrir una mínima afectación ante un ataque de ciberseguridad exitoso.
- **Tecnología:** Este factor es utilizado a través de las herramientas que se aplican para proteger los dispositivos que pueden ser afectados, entre las principales herramientas utilizadas encontramos los firewalls, proxy, antimalware, antivirus, DLP o incluso antispam

En la Figura 3 podemos ver algunas de las formas de ataque más comunes que emplean los ciberdelincuentes para poder lograr su cometido.

Cualquier equipo que no cuente con un sistema de ciberseguridad es vulnerable a ataques como denegación de servicios (DDoS), el cual es dirigido a páginas web o servidores en donde el propósito de este tipo de ataque cibernético consiste en saturar de solicitudes a la página o al servidor haciendo que utilice al máximo sus recursos y funcione con lentitud o incluso se caiga. Otro tipo de ataque muy común es el phishing, el cual consiste en el uso de correo electrónico para poder extraer información importante de parte del usuario. También el correo es usado para poder enviar archivos adjuntos como malwares o spyware los cuales al momento de ser ejecutados el ciber atacante logra ingresar a los equipos y desde ahí explotar otras vulnerabilidades presentes (Diogenes & Ozkaya, 2018).

Otro tipo de ataques usados con frecuencia son los ataques de fuerza bruta, los cuales consisten en descifrar la contraseña del usuario a través de algoritmo de prueba y error; por lo cual se recomienda no utilizar la misma contraseña en diferentes dispositivos, así como tampoco utilizar la misma contraseña en equipos personales para acceder a equipos de la empresa (Diogenes & Ozkaya, 2018).

Todos los tipos de ataques antes mencionados, tienen un factor en común el cual es la persona que es el eslabón más débil y por el cual los ataques mencionados anteriormente, así como otros no mencionados surten efecto (Diogenes & Ozkaya, 2018).

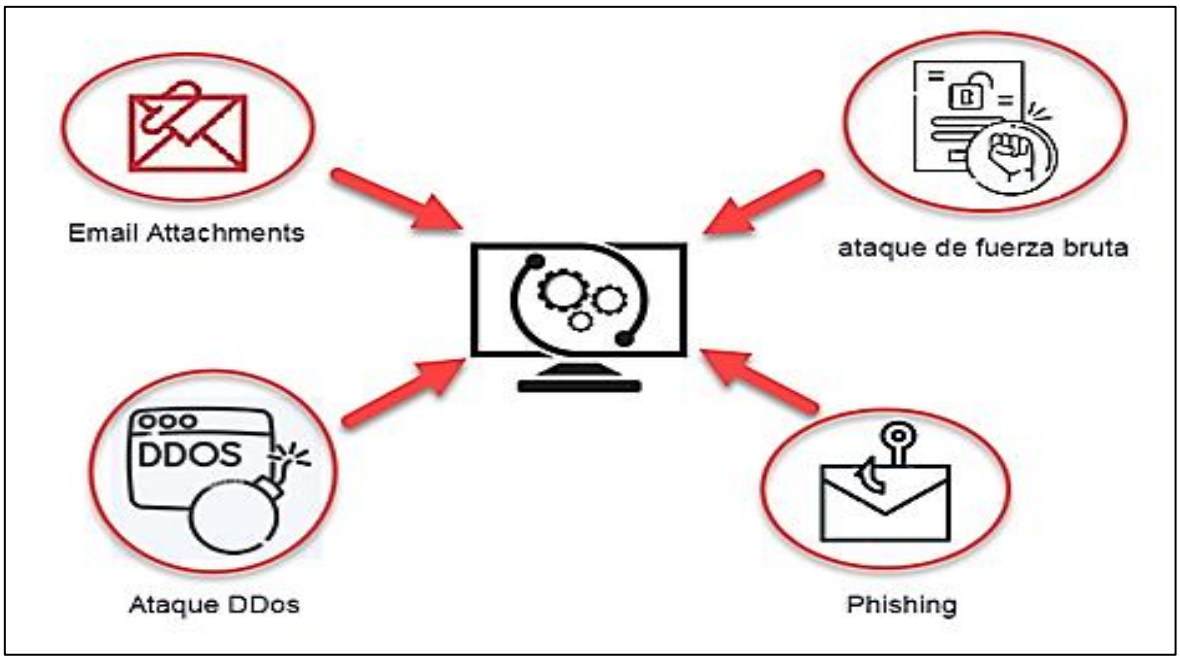


Figura 3. Ataques más comunes en la ciberseguridad.
Fuente: Elaboración propia

2.2.2 Seguridad informática

La seguridad informática es el tipo de seguridad que se encarga de mantener seguro el medio informático, además este tipo de seguridad se encarga de establecer normas y procesos que contribuyan a tener un sistema informático seguro y confiable. Normalmente este tipo de seguridad es confundida con la seguridad de la información, pero, aunque suenen similares tienen aspectos fundamentales que lo diferencian ya que la seguridad de la información se enfoca en todo aquello que está relacionado con la información. Cabe resaltar que la seguridad informática tiene como tarea principal disminuir los riesgos tanto en la

transferencia de información, así como en otros aspectos. Este tipo de seguridad involucra tres aspectos (Romero Castro et al., 2018).

- **Los usuarios:** Es el aspecto de la seguridad informática que no se puede predecir o controlar su acción, por lo cual en muchos aspectos se debe cuidar los activos informáticos de las mismas personas.
- **La información:** Es lo más importante dentro de lo que es la seguridad informática y es lo que se desea resguardar, por ello se plantea, implementa y aplica diferentes métodos para mantenerla segura.
- **La infraestructura:** Es el aspecto de la seguridad de la información en el cual se aplica más control, pero este no está excluido de posibles acontecimientos que podrían afectarlo. Tal sería el caso de la usurpación de identidad de un usuario con lo cual se podría dar un acceso no permitido dentro de la infraestructura del sistema de seguridad.

A) Mecanismos preventivos en seguridad informática

Este aspecto comprende las revisiones periódicas, así como las posibles mejoras en software o hardware involucrados en los sistemas. Los mecanismos preventivos muchas veces son menospreciados, pero muchos posibles o exitosos ataques informáticos pueden ser evitados o disminuidos su impacto en la empresa si se tuviera buenos mecanismos preventivos implementados. Muchas veces este tipo de mecanismo no son valorados, pero se le debe dar la importancia correspondiente. Entre los mecanismo de prevención más comunes tenemos: respaldo de información, actualización de sistemas operativos, uso de antivirus, uso de contraseñas, etc (Romero Castro et al., 2018).

B) Mecanismos correctivos en seguridad informática

Este tipo de mecanismos se aplican después de que algún tipo de ataque informático a ocurrido. Además este tipo de mecanismo llega a ser muy costoso debido a que se tiene el problema de estar vulnerable frente al ataque por lo cual en muchas situaciones se pagara a expertos para solucionar la situación, se compraran soluciones o se aplicaran parches que ayuden a solucionar la vulnerabilidad presentada (Romero Castro et al., 2018).

C) Mecanismos detectivos en seguridad informática

Este tipo de mecanismo es el más complejo y tienen como objetivo detectar la superficie de ataque que fue aprovechada por los intrusos, adicional a ello busca conocer lo que fue afectado para que de este modo se pueda partir solucionando o restableciendo lo afectado (Romero Castro et al., 2018).

D) Tipos de seguridad de la información

Existen 3 tipos de seguridad informática muy marcadas los cuales son: externo, interno y electrónica o lógico. En la seguridad Externa e interna el factor humano y su acción son una gran falla en la seguridad en muchas ocasiones, debido a que el comportamiento y proceder de las personas es impredecible y no se puede controlar (Baca Urbina, 2016).

- **Seguridad Externa:** Se enfoca en el control y monitoreo de los accesos del personal autorizado a la información valiosa de la empresa. Con el fin de lograr ello, busca evitar que cualquier persona no autorizada o que este usurpando una identidad logre tener acceso a dicha información, hace uso de diferentes herramientas como equipo de reconocimiento facial, de huella digital, cámaras de vigilancia, etc.
- **Seguridad Interna:** Consiste en la seguridad ante algún tipo de ataque de parte del mismo personal de la empresa. En este tipo de ataque algún usuario puede borrar, copiar o modificar los activos informáticos de la organización, con el objetivo de favorecer con ello a otras empresas o alguna otra entidad que se pueda beneficiar con la información extraída o borrada, por lo cual este tipo de situaciones se debe evitar a toda costa.
- **Seguridad lógica:** También llamada electrónica, está enfocada en todos aquellos riegos que pueden surgir del internet y que pueden comprometer a los ordenadores y explotar vulnerabilidades.

Un sistema de seguridad que se puede considerar confiable y protegido, debe cumplir con múltiples aspectos de la información, entre los más resaltantes tenemos la Integridad, disponibilidad y confidencialidad. Así mismo se hace uso de las normas ISO, entre las cuales tenemos la ISO 27001 en la cual se nos presenta los requerimientos para establecer y mantener un sistema de gestión de seguridad de la información (SGSI) (Baca Urbina, 2016).

En la Figura 4 podemos observar una representación gráfica de los tipos de seguridad informática.

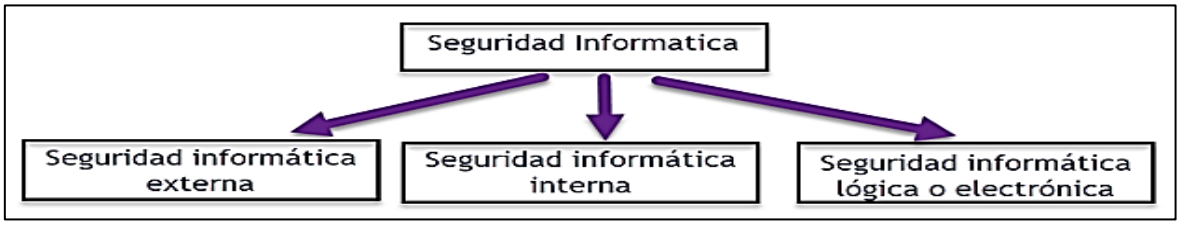


Figura 4. Tipos de seguridad informática
Fuente: Elaboración propia

2.2.3 Normas ISO

Este tipo de normas son de uso voluntario y son elaboradas y aprobadas por expertos a nivel internacional. Estas normas están orientadas a presentarnos la mejor forma para realizar algún tipo de proceso o actividad, por ello existen múltiples tipos de normas ISO aplicadas a casi todos los procesos; entre las más comunes tenemos los estándares aplicados a gestión del ambiente, gestión energética, seguridad de la salud, estándares de seguridad, entre otros (ISO, s/f).

Tabla 1
Normas ISO y su aplicación al desarrollo sostenible.

NORMAS ISO Y SU APLICACION AL DESARROLLO SOSTENIBLE	
OBJETIVO DE APLICACIÓN	CANTIDAD
Sin pobreza	388
Hambre cero	592
Buena salud y bienestar	3524
Educación de calidad	630
Igualdad de genero	232
Agua pura y desinfectada	696
Energía accesible y limpia	1082
Crecimiento económico y trabajo honrado	2810
Industria, infraestructura e innovación	14289
Reducción de la desigualdad	644
Comunidades sostenibles	2775
Consumo y producción responsable	3141
Acción climática	1398
Vida bajo el agua	384
Vida en la tierra	1191
Paz y justicia	232
Alianzas para las metas	11
TOTAL	34019

Fuente: Elaboración propia

Entre las normas ISO orientadas a la gestión de seguridad tenemos las siguientes:

A) ISO 27000

La norma 27000 nos expone un análisis superficial de los sistemas de gestión de seguridad de la información (SGSI) o por su denominación en inglés *Information Security Management System* (ISMS). También nos da a conocer términos y nos expone sus conceptos que son utilizados en los SGSI, la norma 27000 es aplicable a todos los tipos de organizaciones indiferente de su tamaño y de su ocupación, así también su aplicación se realiza con el fin de normalizar los procesos en las organizaciones (Organización Internacional de Normalización [ISO], 2018).

B) ISO 27001

La norma ISO 27001 es un estándar internacional que establece los requisitos para la implementación, mantenimiento y mejora continua de un Sistema de Gestión de la Seguridad de la Información (SGSI). Las organizaciones que aplican este estándar, se entiende que están respetando y haciendo cumplir las buenas prácticas con lo relacionado a la seguridad de los activos informáticos. Con la aplicación del ISO 27001 se logra en las organizaciones la adaptabilidad frente a ciberataques, protección para toda la organización, ahorro de costos frente a ataques al estar preparados, así como la aplicación de los tres principios para la seguridad de la información los cuales son confidencialidad, integridad y disponibilidad (Organización Internacional de Normalización [ISO], 2022b).

Un aspecto resaltante de la norma ISO 27001 es la aplicación de la triada CIA, dicha triada está formada por:

- **Confidencialidad:** La información de la empresa solo tiene que ser accesible para los usuarios autorizados o sistemas autorizados dado que si no se cumple estas normas se puede producir robo o pérdida de información (ISO, 2022b).
- **Integridad de la información:** La información almacenada de la empresa que sea de sus clientes o que se utiliza para el negocio, no debe sufrir ninguna modificación o alteración ya que esta podría causar problemas entre las áreas internas que utilizan esta información o generar desconfianza para con los clientes (ISO, 2022b).

- **Disponibilidad de la información:** La información tiene que estar disponible en cualquier momento para los usuarios que laboran dentro de la empresa así como para los clientes, a fin de satisfacer las necesidades bajo las cuales la información es requerida (ISO, 2022b).

En la Figura 5 podemos visualizar una representación gráfica de la llamada triada CIA que se explica en detalle en la ISO 27001.

Figura 5. Dimensiones de la seguridad
Fuente: Elaboración propia

C) ISO 27002

La norma ISO 27002 es otro estándar para la seguridad de la información que ha publicado la organización internacional de normalización y la comisión electrotécnica internacional. La versión más reciente de la norma es ISO 27002:2022**.** La norma ISO 27002 se encuentra enfocada en presentar un conjunto de buenas prácticas, referencias, así como una guía de implementación sobre el control de la información en los sistemas informáticos. Esta norma está orientada a ser utilizada en organizaciones que estén aplicando la norma ISO 27001 (Organización Internacional de Normalización [ISO], 2022a).

D) Relevancia de la norma ISO 27001 y 27002

Todo sistema de seguridad tiene que cumplir ciertas reglas y/o normas que sirvan para la protección de datos o de información que el usuario necesita al momento de acceder a las herramientas digitales ya sea por ámbito laboral o personal.

Las leyes establecidas para dicho propósito se centran en la norma ISO 27000, ISO 27001 e ISO 27002, las cuales a lo largo del tiempo se ha ido actualizando de acuerdo al avance de las tecnologías informáticas. Así mismo cabe resaltar que las normas ISO 27001 e ISO27002 se complementan entre sí, por lo cual deben actuar en forma conjunta.

Cabe mencionar que las organizaciones no solo están regidas bajo la aplicación de normas ISO o políticas de seguridad, ya que en los diferentes países se tienes leyes que aplican una sanción ante la modificación, robo, secuestro de información personal o de alguna organización sea pública o privada.

2.2.4 Ley N°30171

En el Perú se tiene la Ley de Delitos Informáticos (Ley N° 30171), la cual sanciona las conductas ilícitas que afectan los sistemas y datos informáticos a través del uso indebido de tecnologías de información o de comunicación. Esta ley es la modificación de la Ley 30096, Se realizaron varias modificaciones, entre las cuales las más resaltantes son (Ley de delitos informáticos, 2014):

- Con referente al acceso ilícito, si este conlleva el traspasar un perímetro de seguridad de forma intencional, conllevaría una pena privativa de la libertad de hasta 4 años o en su menor medida una multa y una privación de la libertad de hasta 90 días.
- Con relación a los datos informáticos, la persona que deliberada e intencionalmente realiza la eliminación, modificación o introducción de datos de forma ilícita, podría obtener una pena privativa de su libertad de entre 3 a 6 años o en su menor medida entre 80 a 120 días con una multa adicional.
- Con relación a proposiciones con fines sexuales a través de la tecnología hacia menores de edad, el contactar con menores de 14 años a través de la tecnología para obtener material pornográfico o realizar actividades sexuales podría conllevar a una pena privativa de la libertad entre 4 a 8 años.
- Con relación al fraude informático, la persona que busque obtener un beneficio al vulnerar una red de seguridad, con el objetivo de modificare, borrar, encriptar o clonar información vital podría obtener una pena privativa de su libertad de hasta 8 años o en menor medida hasta 140 días con una multa adicional.

- Con relación a la intercepción de datos, el que deliberadamente interfiera una conversación por llamada a fin de escuchar y obtener información privilegiada podría obtener una pena privativa de su libertad de hasta 10 años según el valor establecido a la información extraída durante la intercepción.

Así mismo se agregó en la ley el artículo 12, que trata sobre la excepción de la responsabilidad penal, con lo cual si una persona vulnera un sistema de seguridad y esta acción es realizada de forma autorizada o realizada a modo de pruebas a fin de encontrar vulnerabilidades en los sistemas y protegerlos; a dicha persona no se le atribuirá una sanción penal (Ley de delitos informáticos, 2014).

Dentro de una organización, no solo hace falta la aplicación de las Normas ISO para buscar de este modo tener un sistema de gestión de seguridad informática confiable y bien establecido, también hace falta la aplicación de políticas de seguridad las cuales deben ser desarrolladas en función de las vulnerabilidades que enfrenta cada organización. La elaboración de las políticas de seguridad son responsabilidades de los altos ejecutivos, así como su aplicación y conocimiento por toda la organización. Dentro de todo este panorama de seguridad para la información, las organizaciones utilizan herramientas para hacer cumplir las políticas de seguridad, así como las normas ISO establecidas. Entre alguna de las herramientas utilizadas tenemos el uso de FW, proxys a nivel de protección externa y softwares de cifrado de datos o uso de DLP a fin de proteger la información de ataques internos (Baca Urbina, 2016).

2.2.5 Fuga de datos

Cada vez la tecnología avanza más rápido y con ella la importancia que esta tiene en la vida de todas las personas. Desde escolares hasta gerentes o dueños de empresas, todos en la actualidad tenemos acceso a una computadora o celular en los cuales podemos almacenar desde tareas hasta información valiosa de cuentas bancarias, contraseñas de equipos empresariales o incluso códigos militares.

Por lo cual es necesario que dicha información sea protegida ante alguna posible fuga de datos o también llamada fuga de información.

La palabra Fuga proviene del latín "fugare" que significa huida o persecución, por lo cual podemos considerar que la fuga de información es un acto en el cual se da una persecución y huida de dicha información, así mismo en muchos casos durante la fuga de información se llega a revelar secretos de estado, información importante de las organizaciones o algún tipo de ventaja que poseía el organismo vulnerado. Por lo cual ante la vulneración de la brecha de seguridad del organismo afectado, se tendrá como consecuencia una persecución en búsqueda de la información extraída a fin de recuperarla y de encontrar al culpable de haber extraído la información o también por haberla publicado y compartido sin consentimiento (Cano Mora, 2013).

Podemos realizar un sin número de esfuerzos, medidas y contramedidas a fin de evitar la fuga de información vital en las organizaciones, pero debemos tener en cuenta el factor y la importancia del ser humano dentro de todo este aspecto, ya que las personas están expuestas a almacenar y compartir información importante como aspecto intrínseco de su comunicación con otros seres humanos. Si el revelar información vital o importante conlleva algún tipo de pena o sanción para la persona, esto podría limitar su proceder pero no en su totalidad, debido a que el compartir información forma parte de la comunicación con otros seres humanos (Cano Mora, 2013).

La fuga de información se presenta de diferentes formas, como podría ser a través de medios físicos como es la extracción por USB o dispositivos de almacenamiento, a través de grabaciones analógicas o digitales de alguna conversación importante o explotando algún tipo de vulnerabilidad y fallas en los sistemas de seguridad. Por lo cual las maneras de extraer información son múltiples y el principal medio para poder realizarlo gira en torno a las mismas personas, por ello las medidas que se tomen deben centrarse en torno al humano, reconociéndolo como un punto débil en el marco de la seguridad (Cano Mora, 2013).

Existen diferentes herramientas utilizadas por las empresas para poder prevenir, combatir y monitorear posibles amenazas de fuga de datos.

A nivel externo se puede utilizar firewall, proxys entre otros y a nivel interno se puede utilizar softwares de encriptación o DLP; siendo la utilización de softwares

DLP la opción que está tomando mayor fuerza en las empresas en cuanto a protección interna se refiere.

A) Gestión de Fuga de Datos

Para poder gestionar fugas de información es necesario tener algún software que puedan actuar cuando esté sucediendo una fuga de información o que pueda monitorear comportamientos sospechosos de posibles sucesos de fuga de información. También se debe tener un proceso de cómo actuar frente a una fuga de información; a continuación describiremos las 6 etapas propuestas por el centro de respuesta a incidentes de seguridad de referencia para los ciudadanos y entidades privadas operado por el instituto Nacional de Ciberseguridad de España (Instituto Nacional de Ciberseguridad [INCIBE], 2020):

- **Fase Inicial:** Se detecta el posible incidente de fuga de información, es importante que esta detección sea temprana a modo de poder tomar medidas lo antes posible.
- **Fase de lanzamiento:** Se reúne el personal encargado para hacer frente a la fuga de datos, se planifica las acciones a tomar con respecto a la fuga información.
- **Fase de auditoria:** Se realizan las auditorías internas y externas.
- **Fase de evaluación:** El grupo encargado de hacer frente a la fuga de datos, se reúne para dar el alcance sobre las auditorias y planificar el accionar contra la fuga de información.
- **Fase de mitigación:** Se pone en marcha las acciones a fin de poder solucionar lo antes posible la fuga de información, así como también se notifica a los afectados por dicho incidente.
- **Fase de Seguimiento:** Se notifica los resultados de las acciones realizadas, así como también se expone las consecuencias del incidente, adiciona a ello se implantarán nuevos métodos para evitar que otro suceso de fuga de información similar vuelva a ocurrir.

En la Figura 6 podemos visualizar un diagrama de flujo correspondiente a la gestión de un incidente de fuga de datos.

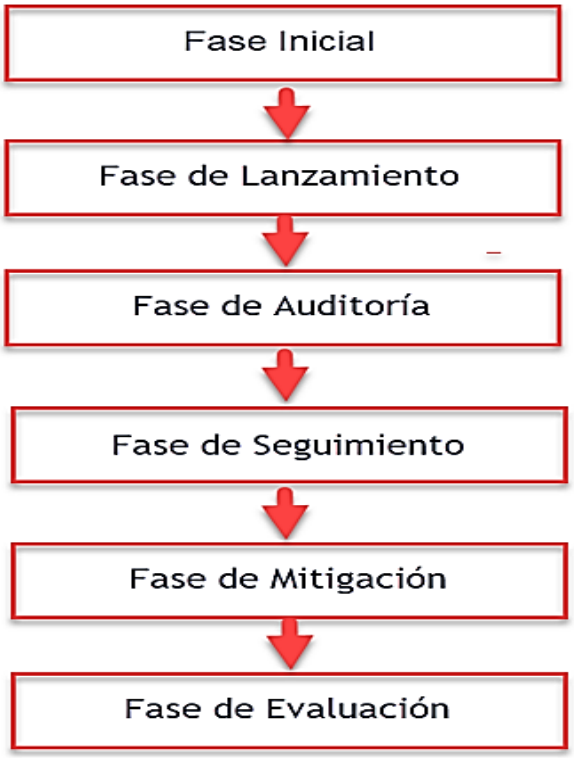


Figura 6. Proceso de Gestión de fuga de datos
Fuente: Elaboración propia

Dentro de los sistemas de seguridad, se hace uso de herramientas tales como softwares enfocados en la protección contra la fuga de información a nivel interno, dentro de las cuales encontramos a la herramienta de Data Loss Prevention (DLP).

2.2.6 DLP

Los softwares de Data Loss Prevention o mejor llamados DLP, realizan el sondeo y protección de los datos en cualquier parte de la red en la cual el software esté implementado. Este tipo de software se puede aplicar a todo tipo de datos, desde información personal hasta información considerada como valiosa como en el caso de los datos financieros de una organización. Así mismo el DLP supervisa el movimiento de la información permitiéndola o denegándola, de este modo evita fugas conscientes o inconscientes, disminuyendo en gran medida la posibilidad de un evento de fuga de la información (Clementelli, 2023).

A) Funciones de un DLP

Entre las funciones más importantes que competen a un DLP encontramos las siguientes (Clementelli, 2023):

- **Identificación de información valiosa y sus movimientos:** Dentro de esta función encontramos los datos que cruzan el internet, pasando por aplicaciones o algún dispositivo. También se encuentran los datos estáticos que están almacenados en los dispositivos protegidos y también encontramos la información que está en movimiento o es compartida a través de USB, impresoras o fax.
- **Monitoreo del entorno:** Dentro de las funciones que competen a un DLP está el monitorear del entorno de los datos, con lo cual puede detectar quien accede a la información o impedir que algún usuario o programa pueda mover o extraer información sin autorización, infringiendo alguna regla que se haya configurado y así obtener una respuesta por parte del DLP.
- **Reacción automática en función de las políticas:** Esta respuesta se realiza en función de la configuración de la política que se esté infringiendo. Se podría detener la acción que se está realizando o se podría poner en cuarentena el archivo que se está transfiriendo o incluso dejar que suceda la acción que se está ejecutando, todo dependerá de la configuración de la política que se está violando.
- **Provee de capacitación al personal:** Cuando se genera una infracción de alguna política, el DLP alerta al usuario mediante una notificación sobre una infracción de política, así mismo también cual fue la causa por lo cual esta notificación apareció. Con ello educa al personal sobre las políticas de DLP establecidas en la organización, así mismo se debe considerar que un buen DLP notifica al usuario rápidamente y escala la notificación a los gerentes de la empresa.

B) DLP moderno vs DLP heredado

A continuación presentaremos las principales controversias con respecto a los DLP modernos y los DLP heredados (Clementelli, 2023):

- Si bien los DLP heredados brindan una protección a los equipos cuando están dentro de la organización, los DLP modernos no se limitan bajo esta condición, ya que proveen de una protección y funcionamiento integral, tanto dentro como fuera de la organización.
- Los DLP modernos no necesitan montar una infraestructura compleja ya que la mayoría de sus funciones se realizan en la nube, a diferencia de los DLP

heredados los cuales necesitan de una infraestructura adecuada para cumplir con todas las funciones.

- Los DLP modernos con su funcionamiento en la nube, disminuye el consumo de los recursos que se necesita en los equipos finales, aunque esta diferencia con respecto a los DLP heredados aun no esta tan grande, se proyecta a que con el paso del tiempo se hará más notoria.
- Debido a la tendencia en aumento de tener las soluciones en la nube, la integración del DLP moderno con otras soluciones es más fácil que la integración con los DLP heredados.
- Debido a que los DLP heredados han estado mucho más tiempo en el mercado, sus códigos, algoritmos y políticas son más maduros respecto a la detección y prevención de transferencias de información no autorizados, por ello aun en muchos casos son preferidos por las organizaciones.

C) Tipos de DLP

Existen 3 tipos de DLP:

- DLP enfocado en la protección de puntos finales.
- DLP que se orienta hacia la protección de la información en la red de las organizaciones.
- DLP de uso aplicado en servicios o datos sensibles en la nube.

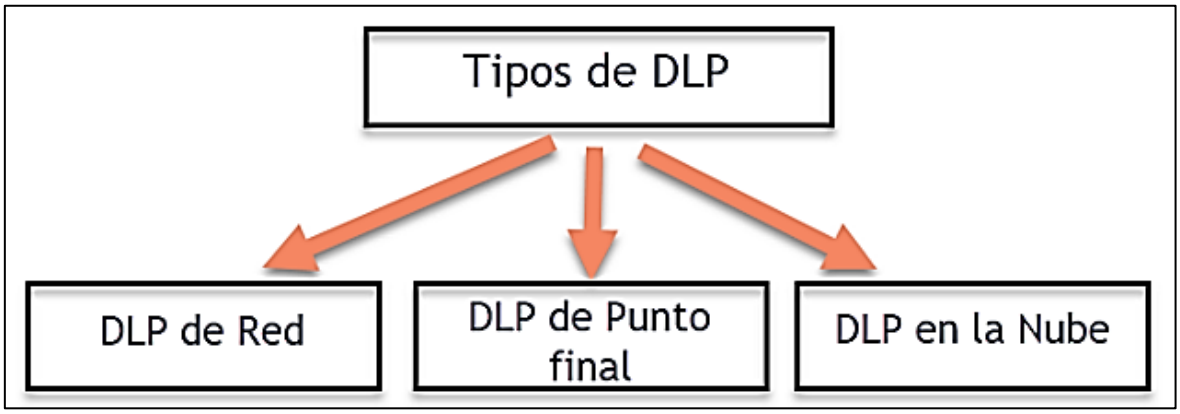


Figura 7. Tipos de DLP
Fuente: Elaboración propia

Con lo antes mencionado con relación al concepto, funciones y tipos de DLP se determina que el uso de esta solución para proteger la fuga de información es una alternativa viable y recomendada, usada en muchas organizaciones que buscan

cuidar sus activos ante algún tipo de ataque, pero surge una interrogante más, la cual es ¿Cuál es el mejor DLP del mercado?

Gartner, empresa enfocada en brindar información objetiva con respecto a las diferentes soluciones aplicadas dependiendo de las necesidades de los organismos y empresas, nos brinda el cuadrante mágico de Gartner, el cual es usado como referencia a nivel internacional para escoger la mejor solución con respecto a la necesidad que se quiera afrontar. No obstante, en los últimos años Gartner no ha elaborado un cuadrante mágico con respecto a las soluciones DLP, pero si ha realizado un informe de guía de mercado con las soluciones mejor clasificadas. Entre las mejores soluciones consideradas en el informe de guía de mercado tenemos: DLP ForcePOint, Symantec Data Loss Prevention y Trellix Data Loss Prevention Endpoint encabezando la lista como las soluciones recomendadas (Gartner, s/f).

Tabla 2
Las mejores 10 soluciones DLP

Top 10 mejores DLP		
Solución	Ranking	N° de valoraciones
DLP de ForcePOint	1	460
Symantec Data Loss Prevention	2	339
Trellix Data Loss Prevention (DLP) Endpoint	3	245
GTB Technologies DLP	4	85
Proofpoint Enterprise Data Loss Prevention (DLP)	5	71
Digital Guardian	6	61
Endpoint Protector	7	45
Nightfall	8	40
Spirion	9	37
DoControl Saas Security Platform	10	22

Fuente: Elaboración propia

2.2.7 Agent Handler

Los Agent Handler son usados para distribuir el tráfico que se genera entre el agente y el servidor ePO on-premise de Trellix, en lugar que el agente se comunique directamente con el servidor ePO se comunicara con el Agent Handler cuando esté fuera de la red empresarial. El agent Handler proporciona actualizaciones de agente, actualizaciones de firmas, actualizaciones de tareas o

de directivas, las cuales este recoge del servidor ePO y se las envía a los agentes que tiene conectado fuera del alcance del servidor (Trellix, 2022).

2.2.8 Agente ePO

El agente ePO viene a ser el ente comunicador entre la consola ePO (ya sea on-premise o sea cloud) y el punto final.

Sirve como interconexión para poder recibir actualizaciones de firmas, tareas, cambios de políticas o también llamada directivas, instalación de productos y también para poder enviar y recoger eventos. Antes de realizar la instalación del agente se debe tener en claro sus requerimientos para poder ser instalado en los puntos finales (Trellix, 2017).

2.3 Definición de Términos Básicos

- **Antispam:** Son el tipo de softwares que se enfoca en el control y tratamiento de los correos no deseados que muchas veces son utilizados como medio para generar una vulnerabilidad.
- **Ataque DDoS:** Son las siglas que se le da al ataque de denegación de servicios, el cual consisten en saturar los recursos de un sitio web o un servidor con el objetivo de que este no funcione correctamente (Romero Castro et al., 2018).
- **Ataque Informático:** Consiste en hacer uso de una vulnerabilidad detectada por el atacante o cibercriminal, con la intención de hacer que los equipos atacados funcionen de forma incorrecta a su estado normal y el atacante pueda extraer información importante la cual podría ser vendida o negociada para poder ser recuperada.
- **Brecha de seguridad:** Es la simbología que se utiliza cuando se quiere dar a entender que un sistema de seguridad o un equipo en específico presenta algún tipo de vulnerabilidad que puede ser explotable en un ataque informático.
- **Cibercriminal:** Persona que hace uso de la tecnología y de las vulnerabilidades que presenta un sistema de seguridad para poder extraer activos valiosos como lo es la información y generar desestabilidad.

- **Ciberseguridad:** Consiste en la protección de la información de una persona u organización buscando enfatizar los 3 aspectos más importante de esta los cuales son: integridad, disponibilidad y confidencialidad de la información; para ello hace uso de herramientas, métodos y la tecnología (Kiser, 2020).
- **Cifrado de datos:** Método utilizado para proteger la información frente a algún tipo de acceso por una persona ajena y sin permiso (Baca Urbina, 2016).
- **DLP:** Son las siglas de Data Loss Prevention o en español prevención de perdida de datos, tal como su nombre lo indica es un software de protección de datos que mediante su aplicación por medio de políticas o reglas configuradas pueden garantizar su propósito (Samaniego Mena & Ponce Ordóñez, 2021).
- **Firewall:** Es un tipo de software que se centra en la seguridad de la red, su propósito está enfocado principalmente en el tráfico, permitiendo o denegando el flujo de este a través de reglas establecidas (Samaniego Mena & Ponce Ordóñez, 2021).
- **Fuga de datos:** Consiste en el movimiento de la información vital o importante de un órgano o empresa hacia un ente externo que es controlado por un ciber atacante (INCIBE, 2020).
- **Proceso sistemático:** Comprende un conjunto de etapas o fases a seguir con el fin de lograr un objetivo final, que es la culminación del proceso.
- **Proxy:** Es un equipo que actúa como conexión entre el cliente y el servidor, donde su acción consiste en recibir las solicitudes del usuario y este lo envía al servidor al cual quiere conectarse (Samaniego Mena & Ponce Ordóñez, 2021).
- **Sistema de Gestión de Seguridad de la Información (SGSI):** Es un sistema enfocado en la seguridad de la información, el cual comprende planificación organización, implementación supervisión y mejora de la seguridad para la información que se esté resguardando (Samaniego Mena & Ponce Ordóñez, 2021).

- **Transmisión de datos:** Consiste en el envío y recepción de información utilizando diferentes tipos de medios, como ethernet, fibra, bluetooth, infrarrojo, etc.
- **Vulnerabilidad:** Es algún tipo de falencia que pueda tener un servidor, página web, punto final u otro recurso; el cual pueda ser explotada como una falla y pueda ser considerado una superficie de ataque (Samaniego Mena & Ponce Ordóñez, 2021).

CAPÍTULO III. DESARROLLO DEL TRABAJO PROFESIONAL

3.1 Determinación y Análisis del problema

Dado a los avances tecnológicos que se han estado presentado a lo largo de los últimos años, surgen grupos de ciberataques y espionaje los cuales buscan infiltrarse en las redes empresariales con el fin de capturar datos vitales de dichas empresas y de esta forma obtener beneficios extorsionando a los propietarios, tal es el caso del grupo Sowbug que para el año 2017 se encontró infiltrado en entidades de gobiernos en Sudamérica (Perú, Argentina , Brasil y Ecuador) y también en Asia; según comento la Sociedad de ciberseguridad estadounidense Symantec (Gestión, 2017).

Según la solución Kaspersky al mes de septiembre del presente año, El Perú ocupa el 5to lugar de la totalidad de las amenazas cibernéticas presentadas a nivel de América del Sur con un porcentaje del 6.38% de Usuarios registrados que han experimentado algún tipo de ataque cibernético el cual ha sido detectado por escaneo en tiempo real (On-access scan)(Kaspersky, s/f).

Tabla 3
Top de los 5 países con más alertas de ataques cibernéticos

América del Sur		
Ítem	Países	% de usuarios
1	Bolivia	10.34%
2	Venezuela	8.80%
3	Ecuador	6.81%
4	Brasil	6.72%
5	Perú	6.38%

Fuente: Elaboración propia

El Perú fue nombrado por Eset en el año 2021 como el país con más ataques de Ransomware el cual consiste en extraer información importante y a la vez impide el acceso de los usuarios a dicha información, a nivel de Latinoamérica el Perú tiene el 30% de los ataques totales. así mismo fuimos considerados el país con más Criptominería de la región (eBIZ Latin America, 2022).

Con la pandemia el uso de los ordenadores y con la llegada del teletrabajo que se estableció con mayor fuerza surgió un aumente de exposición ante posibles ataques cibernéticos y al no tener una cultura de la seguridad de la información se vio reflejado en el aumento de casos de ciberataques y de robo de la información en las empresas. (eBIZ Latin America, 2022).

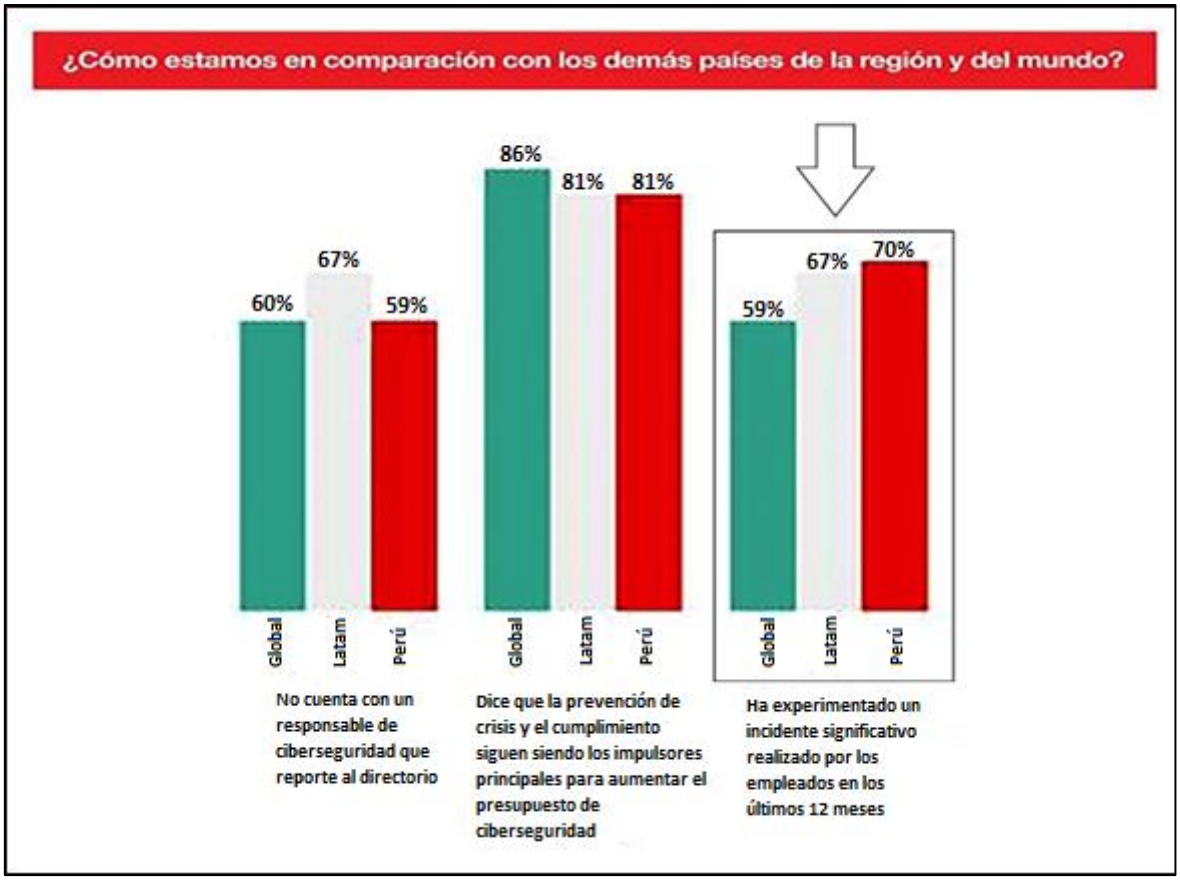


Figura 8. Índice de eventos cibernéticos del Perú vs el mundo
Tomado de (Gestión, 2020)

En la Figura 8 nos detalla que entre los años 2019-2020 la encuesta global de seguridad de la información por parte de la empresa líder en consultoría y asesoramiento (EY) presentada en el diario Gestión, nos indicó que en el Perú en los últimos 12 meses las empresas habían presentado al menos un incidente de ataque informático. Dicho incidente involucro a personal de la empresa, el cual del total de empresas el 70% indico que había pasado por esta situación, este es un índice grande y un porcentaje mayor incluso que el porcentaje a nivel de Latam o a nivel global.

Con respecto a la fuga de información en las empresas y entidades gubernamentales, la Asociación Bancaria del Perú, reporto al consejo de ministros y ministerio de justicia que se estaba subastando en un sitio virtual información personal que es administrada por entidades públicas como la RENIEC O SUNARP. En dicho sitio web se podía conseguir información de figuras públicas o con un cargo gubernamental, hasta se pudo encontrar información personal del expresidente Pedro Castillo, en donde se podía observar información bancaria, datos personales, números de teléfono, etc. (Medrano Marin, 2022)

Así mismo Según lo notificado por el Diario Gestión, El ministerio de Justicia (MINJUS) se encuentra trabajando en la actualización de normas frente al uso de datos de los clientes por parte de las empresas, a fin de garantizar el uso debido de dicha información sin dejarla expuesta antes posibles fugas de datos sensibles (Azurín, 2023).

Ante toda la problemática antes mencionada, Securesoft en su búsqueda de ofrecer siempre el mejor servicio de Ciberseguridad en el mercado en el cual se encuentra y a fin de eliminar posibles vulnerabilidades en su red interna, reforzo su sistema de seguridad frente a ciberataques y disminuyó la superficie de posibles ataques que puedan surgir internamente.

Se aplico una política(directiva) de DLP de la marca Trellix en sus equipos del área de ingeniería, con el objetivo de mantener aún más segura la información de sus clientes y de las plataformas que son administras por la empresa.

La elección del producto DLP Trellix se realizó considerando que la empresa ya contaba con el antivirus de Trellix aplicado a sus equipos, así mismo el DLP de Trellix está en el ranking 3 de los mejores productos DLP en el mercado según lo clasificado por Gartner. Adicional a ello se validó que otras soluciones como Trend Micro y Cortex no pueden bloquear correos electrónicos salientes tal como se evidencia en el Anexo 1 y Anexo 2.

Cabe indicar que el DLP de la marca Trellix cuenta con una ventaja respecto a los productos clasificados en el ranking 2 y ranking 1, ya que este funciona como un apartado adicional del antivirus Trellix por lo cual su licencia de funcionamiento no se renueva es de una única compra a diferencia de los otros productos DLP.

La gran mayoría de DLP en el mercado, son soluciones independientes y deben renovar sus licencias cada 6 meses o cada año según sea su contrato con la marca.

3.2 Modelo de Solución Propuesto

A continuación, se da una representación mediante diagramas de flujo de las etapas realizadas en el proyecto a fin de cumplir con los objetivos antes mencionados.

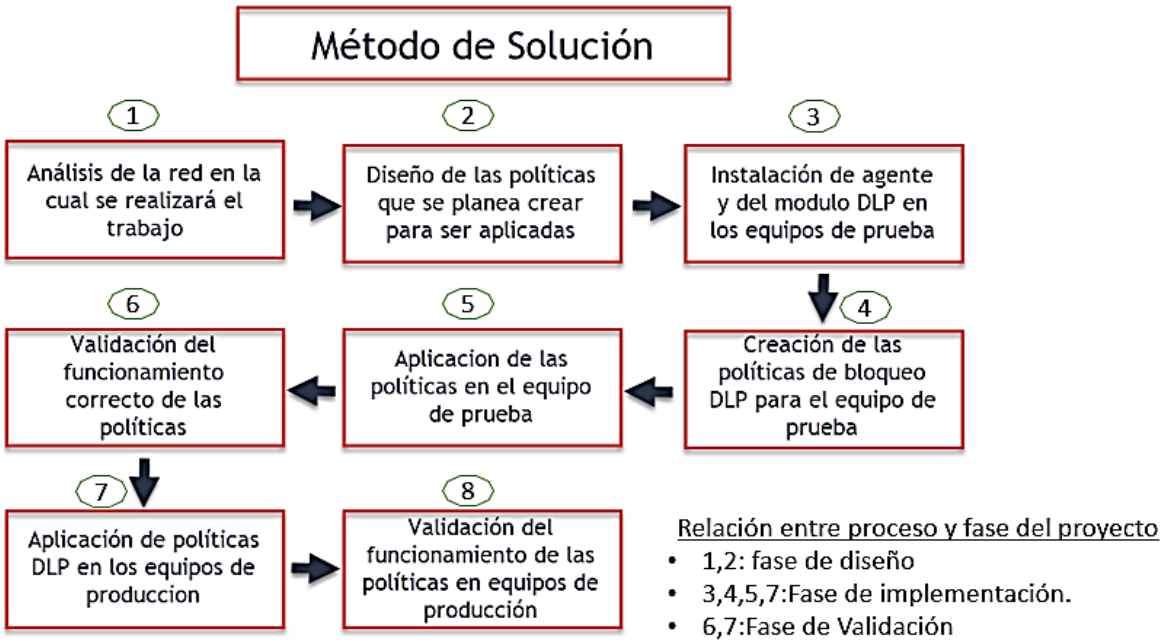


Figura 9. Método de Solución
Fuente: Elaboración Propia

3.2.1 Análisis de la red en la cual se realizará el trabajo

En la Figura 10 podremos ver el esquema de red, para los equipos y la conexión que se presenta para la consola ePO y el funcionamiento del DLP de la marca Trellix.

La consola ePO presenta una conexión con una base de datos SQL para su almacenamiento de eventos y tareas, esta comunicación se da a través del puerto TCP 443.

Así mismo, posee un servidor de directorio activo, en el cual se encontrarán los usuarios registrados en la empresa, la comunicación con el directorio activo se da a través del puerto TCP 389.

También posee conexión con los firewall interno y externo de la empresa los cuales se encuentran en el Data Center ubicado en el edificio, estos le permiten su conexión con las Vlan ubicadas dentro de la empresa, así como también con los equipos que están fuera trabajando en home office y se encuentran conectados por VPN.

También se tiene en uso un servidor de almacenamiento de log DLP, para todos los eventos que surjan en los equipos en los cuales se tenga instalado este módulo.

Los puntos finales presentan 2 tipos de comunicación; se comunican con la consola ePO a través del puerto TCP 443 mediante el cual los puntos finales enviaran información a la consola ePO sobre algún evento sucedido y también recibirán tareas programadas, actualización de directivas o actualización de productos que sean configurados en la consola.

También se comunican con el servidor de almacenamiento de log DLP a través del puerto TCP 445 en el cual se almacenará eventos específicamente del tipo DLP generando así una base de datos de eventos.

Cabe mencionar que los equipos que se encuentren fuera de la red de la empresa trabajando en home office para poder conectarse a la consola ePO hacen uso de un servidor llamado Agent Handler, el cual recibe cualquier tipo de actualización o tarea de parte de la consola ePO y la envia a los equipos fuera de la empresa, así como también este recibe los eventos de los puntos finales fuera de la red y la envía a la consola ePO.

En la red empresarial se validó que hay varias Vlan creadas por departamento, entre las que aremos énfasis son la Vlan de ingeniería on-site y Vlan de ingeniería remoto, dentro de las cuales se encuentran los equipos de los ingenieros que poseen los accesos a las consolas de diferentes soluciones de los clientes, así como también poseen credenciales de acceso.

Debido a lo antes mencionado, las reglas DLP se enfocaron en dichos puntos finales para evitar fugas de información y cerrar posibles brechas de fallo en la seguridad de la empresa.

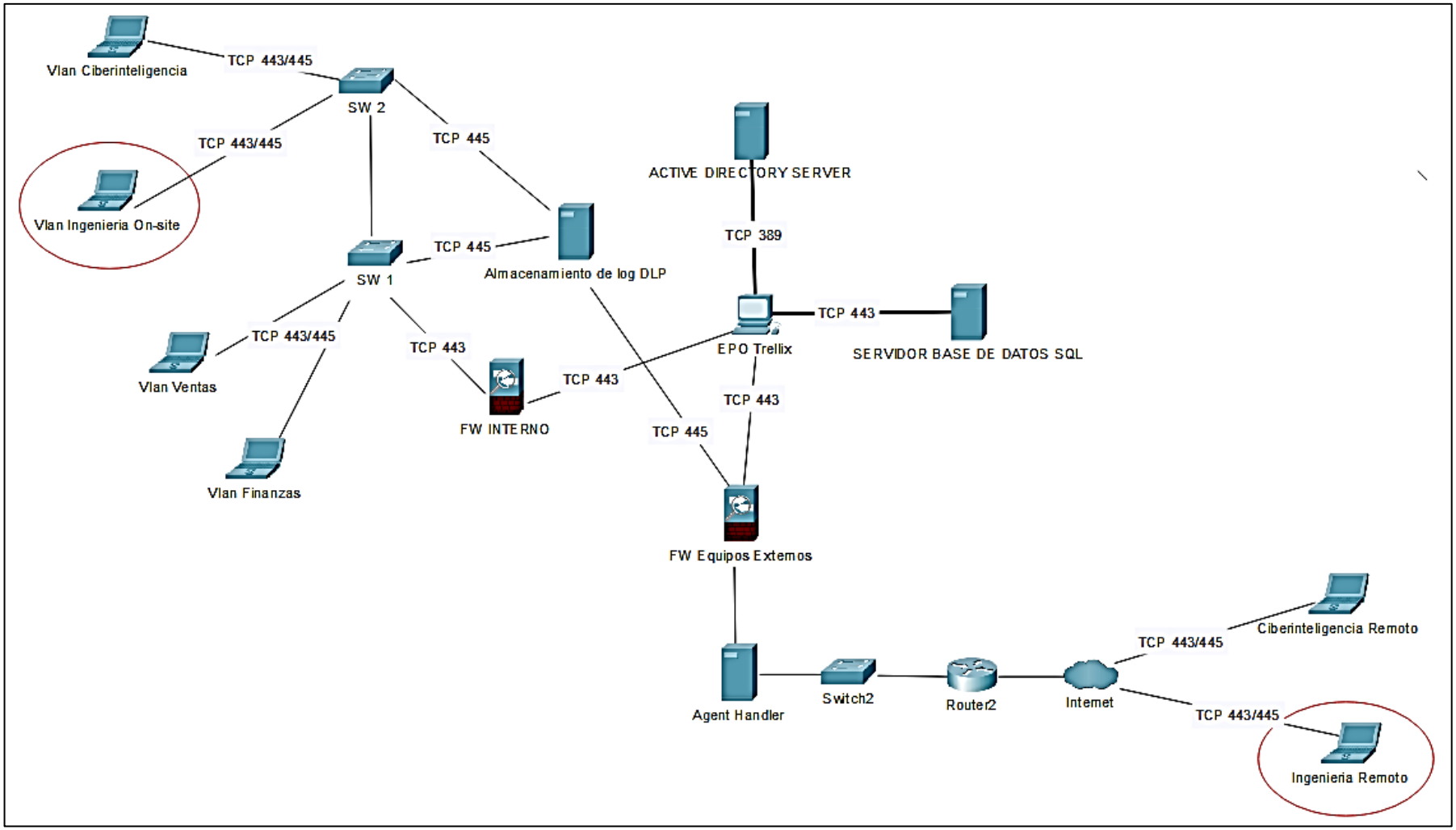


Figura 10. Diagrama de red
Fuente: Elaboración propio

3.2.2 Diseño de las reglas que se planea crear para ser aplicadas

Para el presente trabajo se tuvo en consideración las necesidades y funciones desempeñadas por el personal del grupo de ingeniería para poder diseñar reglas de bloqueo que puedan apoyar en la detección y bloqueo de posibles fugas de información con el DLP de Trellix.

Se realizo la creación de 3 tipos de bloqueo, entre los cuales tenemos:

- Bloqueo de puertos USB: La cual consiste como lo dice su nombre, en bloquear los puertos USB para transferencia de datos a través de ellos y de esta forma no se pueda extraer la información directamente usando dispositivos de almacenamiento como USB, discos extraíbles, entre otros.

Cabe recalcar que el acceso para dispositivos como mouse, teclados o audífonos que utilizan los puertos USB no fueron bloqueados, la aplicación de esta regla se realizó directamente para la transferencia de información a dispositivos de almacenamiento.

Cuando se creó la regla de bloqueo de puertos USB se visualizó de la siguiente forma en la consola tal como se ve en la Figura 11.

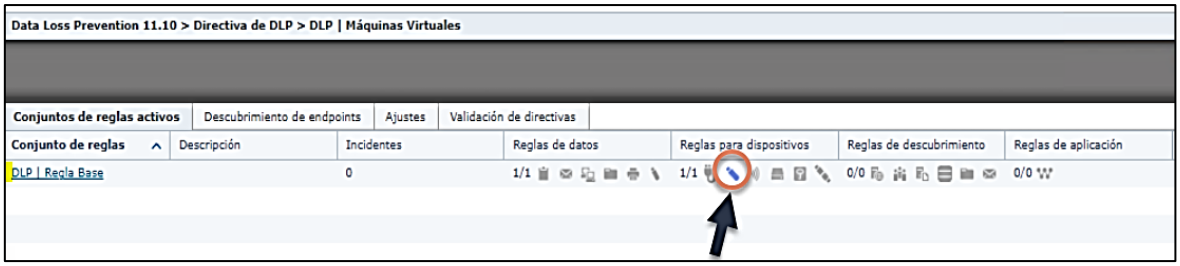


Figura 11. Regla de bloqueo USB en la consola
Fuente: Elaboración propia

- Bloqueo de salida de correos: Esta regla se enfocó en bloquear él envió de información utilizando el correo electrónico, ya que uno de los medios más comunes utilizados para enviar información a nivel de una organización es utilizando el correo electrónico.

Solo se realizó el bloqueo de correo a dominios populares como Gmail, Hotmail, Outlook, entre otros y de este modo no perjudicar con las labores del personal que hace uso de esta herramienta.

Cuando se creó la regla de bloqueo de salida de correos, se visualizó de la siguiente forma en la consola tal como se ve en la Figura 12.

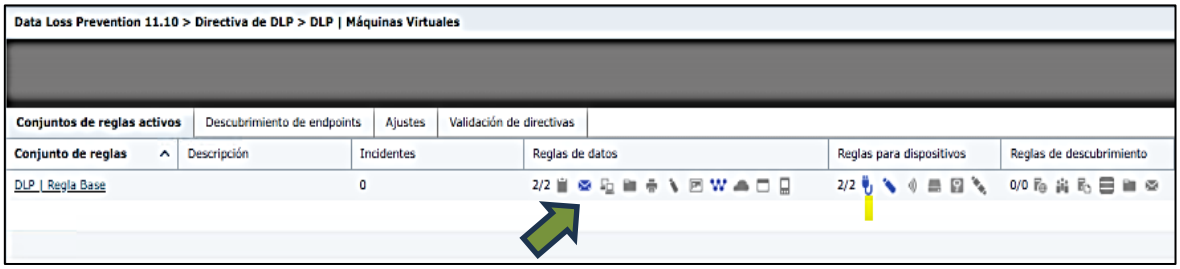


Figura 12. Regla de bloqueo de correo en la consola
Fuente: Elaboración propia

- Bloqueo de Bluetooth: Esta regla se creó con el objetivo de impedir la transferencia de datos por medio de la comunicación por bluetooth ya que este medio también es una forma usada en los incidentes de fuga de información.

Cuando se creó la regla de bloqueo bluetooth, se visualizó de la siguiente forma en la consola tal como se ve en la Figura 13.

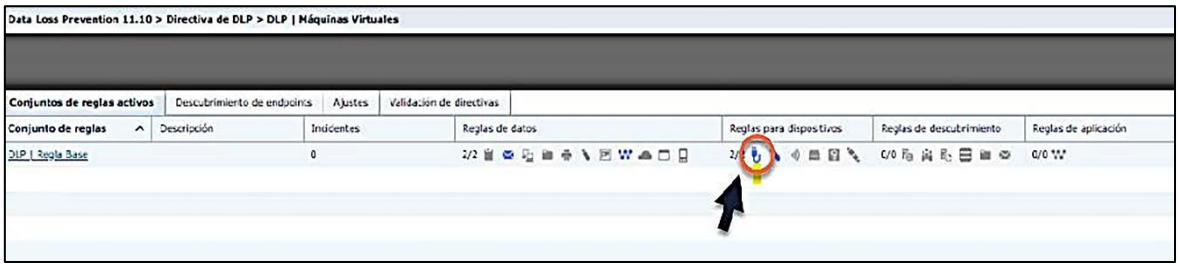


Figura 13. Regla de bloqueo de bluetooth en la consola
Fuente: Elaboración propia

3.2.3 Instalación de agente y modulo DLP en los equipos de prueba

En esta sección se realizó la instalación del agente y del módulo DLP en equipos de prueba, pero antes de realizar alguna instalación, se debe considerar si el equipo en el cual se va a instalar el agente, es compatible con este.

Al considerar solo los sistemas operativos compatibles, es posible evitar errores al momento de realizar la instalación del agente y encontrarnos con problemas de incompatibilidad, alto consumo o errores en el funcionamiento de las reglas DLP aplicadas en los equipos.

Para ello podemos validar en la Tabla 4 la compatibilidad entre el agente y los sistemas operativos más comunes.

Tabla 4
Compatibilidad del agente Trellix con los sistemas operativos

Compatibilidad de agente con los S. O	
Sistema Operativo	Versión del agente 5.7.7-5.8.0
Windows 11 versión 23H2	Yes
Windows 11 versión 22H2	Yes
Windows 10 Enterprise 2021 LTSC	Yes
Windows 10 version 22H2	Yes
Windows 10 version 21H2	Yes
Windows 10 version 21H1	Yes
Windows 8.1	Yes
Windows 8	Yes
Windows Point of Service 1.1	No
Windows 7 x32 and x64	Yes
Windows Vista x32 and x64	No
Windows XP x32 and x64	No
Windows Server 2022	Yes
Windows Server 2019	Yes
Windows Server 2016	Yes
Windows Server 2012 R2	Yes
Windows Server 2012	Yes
Windows Server 2008 R2	Yes
Windows Server 2008	No
Windows Storage Server 2008	No
Windows Storage Server 2003	No
Windows Server 2003	No
Windows Server 2003 R2	No
Windows 2003	No

Fuente: Elaboración propia

En el siguiente punto podemos ver algunos ejemplos del agente Trellix en sistemas operativos compatibles y no compatibles.

A) Compatibilidad con Sistema Operativo Windows 8

De acuerdo a la Tabla 4 en la Figura 14 se pudo observar que el Windows 8 es un Sistema Operativo que es compatible con la versión 5.7.9.139 del agente de Trellix es por ellos que se creó una máquina virtual para proceder a realizar la instalación del Agente y así poder validar su compatibilidad y demostrar que era posible la aplicación de las reglas de bloqueo DLP.

En la Figura 14 se visualiza la máquina virtual creada y el S.O instalado a fin de realizar las pruebas.

Figura 14. Validación de Sistema Operativo Windows 8
Fuente: Elaboración Propia

En la Figura 15 se observa el momento en donde se realizó la instalación del agente Trellix en la máquina virtual.

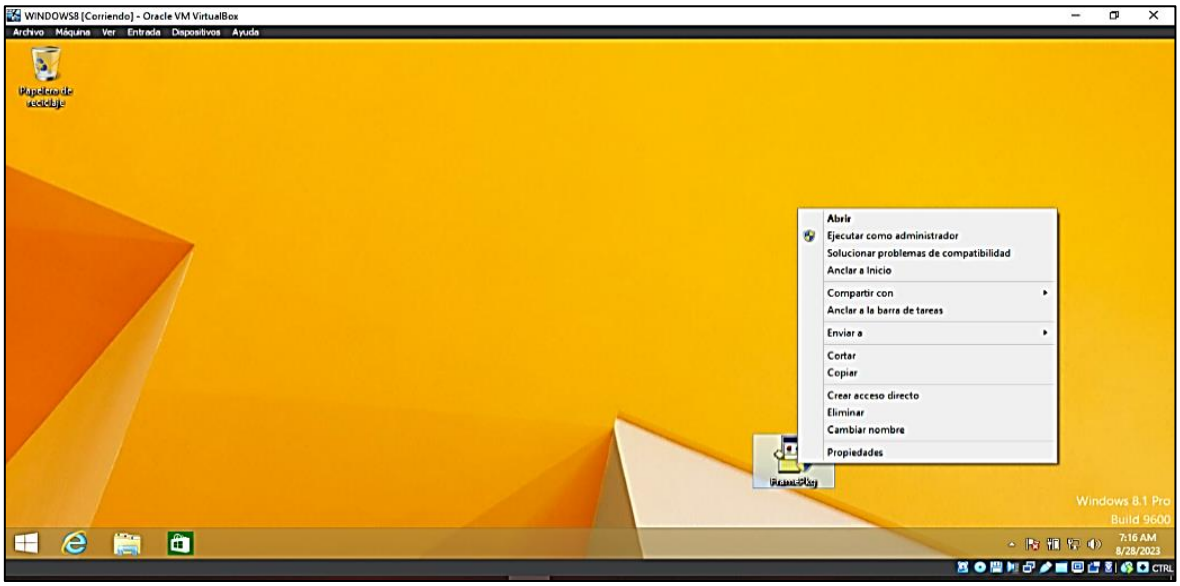


Figura 15. Instalación de agente Trellix Windows 8
Fuente: Elaboración Propia

En la Figura 16 observamos la instalación del agente Trellix finalizada con éxito debido a la compatibilidad que se tiene.

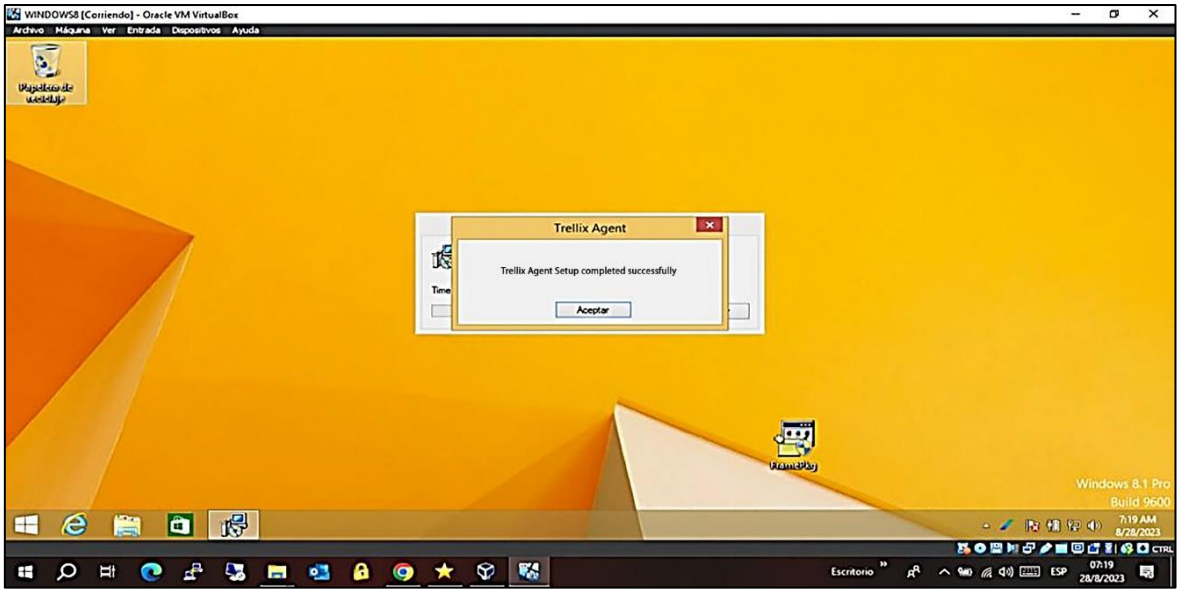


Figura 16. Validación de instalación correcta Windows 8
Fuente: Elaboración Propia

En la Figura 17 se pudo visualizar en el monitor del agente el envío y recepción de información entre el agente y la consola de administración.

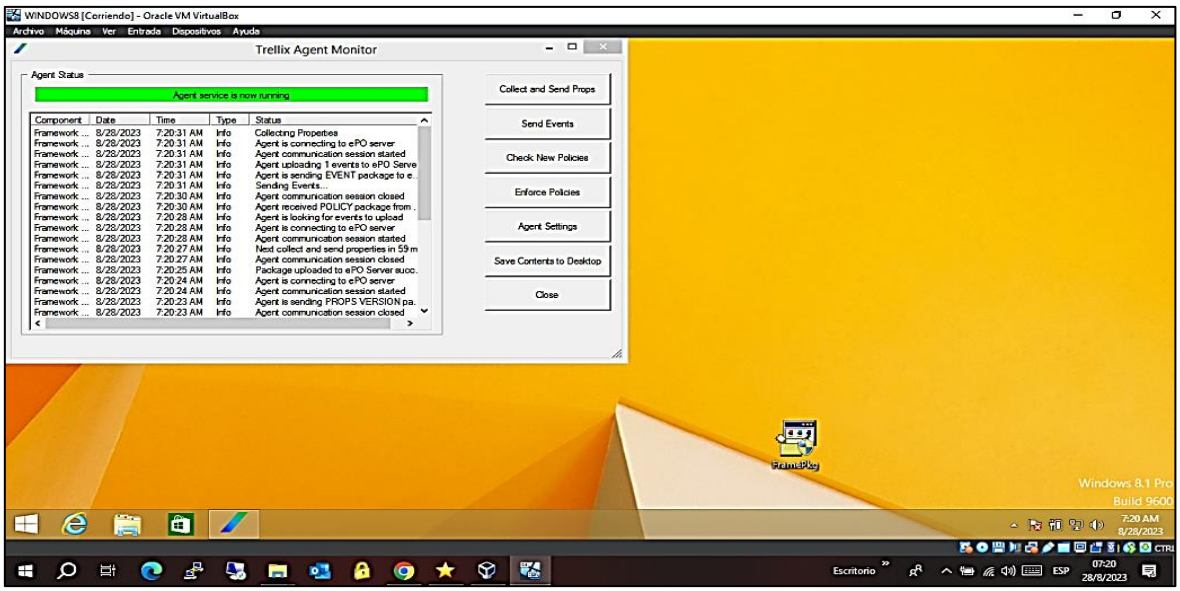


Figura 17. Validación de comunicación agente-consola Windows 8
Fuente: Elaboración Propia

B) Compatibilidad con Sistema Operativo Windows Server 2008

En la Figura 18 se muestra otra máquina virtual que tenía como Sistema Operativo un Windows Server 2008, de acuerdo a la Tabla 4 no tiene compatibilidad con el agente es por ello que se esperó que la instalación del agente no fuera satisfactoria, generando algún tipo de error.

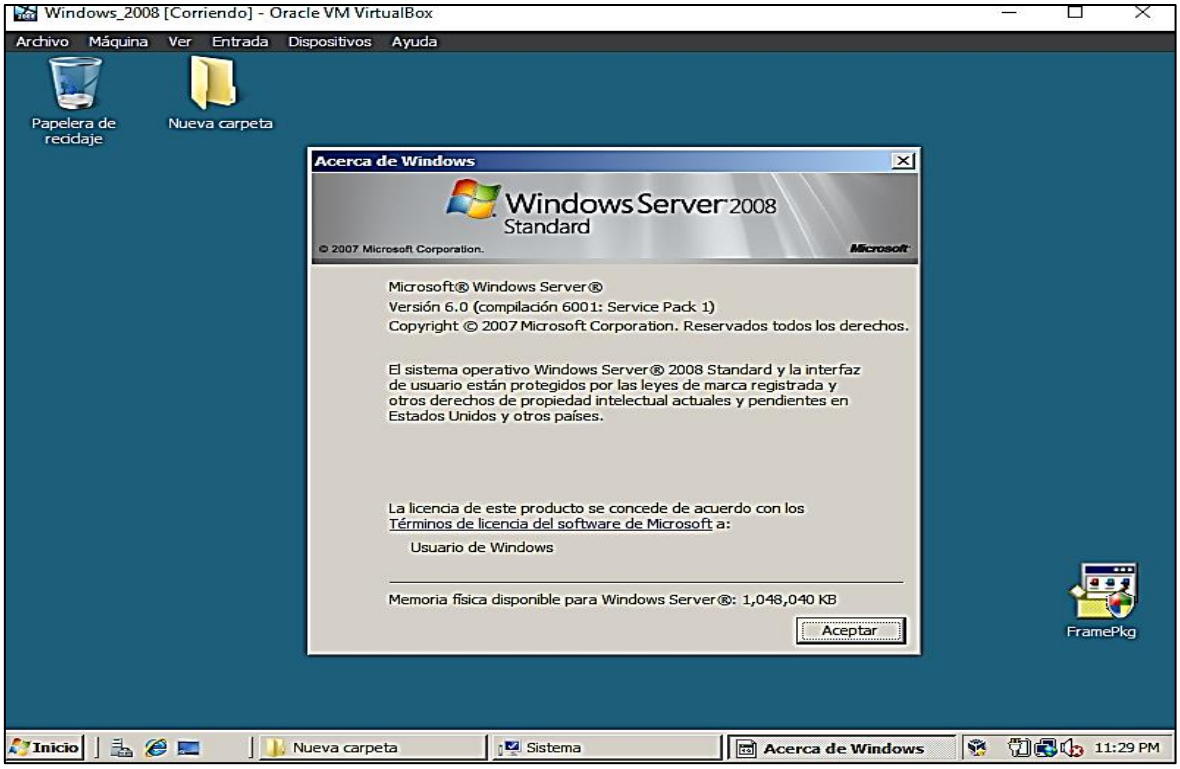


Figura 18. Validación de Sistema Operativo Windows server 2008
Fuente: Elaboración Propia

En la Figura 19 mostramos el momento en donde se realizó la instalación del Agente Trellix. En ese momento se validó que, al intentar ejecutar el instalador del agente, este no logro levantar. Se intento ejecutar en modo administrador y en modo normal, pero en ninguna de las dos opciones se tuvo respuesta alguna.

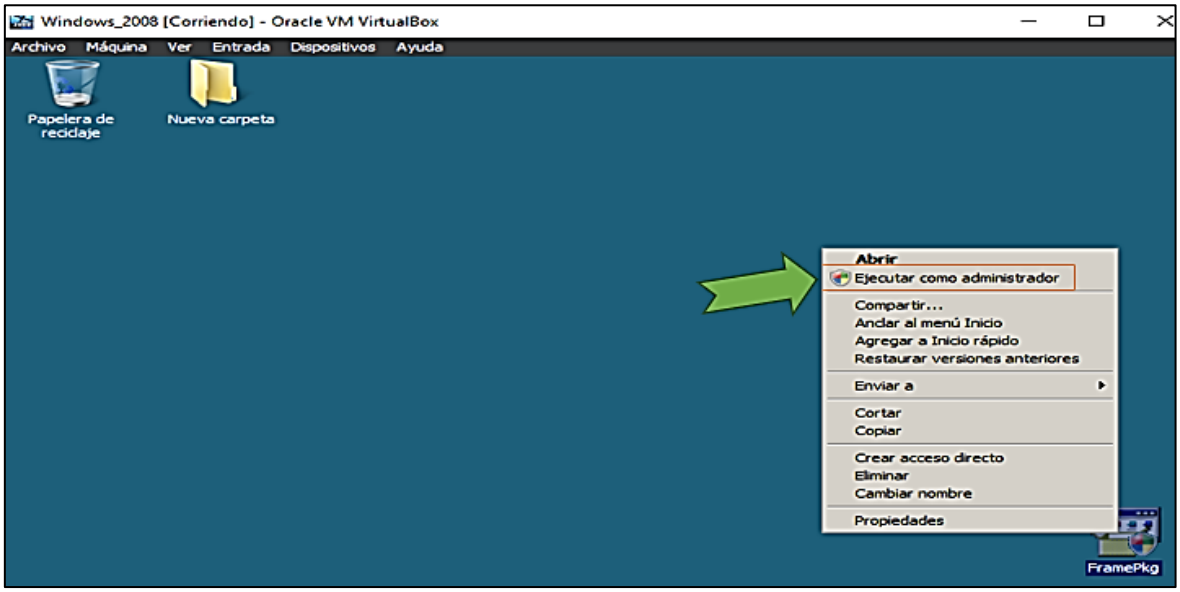


Figura 19. Instalación de agente Trellix Windows server 2008
Fuente: Elaboración Propia

C) Compatibilidad con Sistema Operativo Windows 10

Se levanto otra máquina virtual con un sistema operativo Windows 10 y de acuerdo a la Tabla 4 es un Sistema Operativo que es compatible con la versión 5.7.9.139 del agente de Trellix, en las Figuras 20 y 21 podemos observar ello.

Figura 20. Validación de Sistema Operativo Windows 10
Fuente: Elaboración Propia

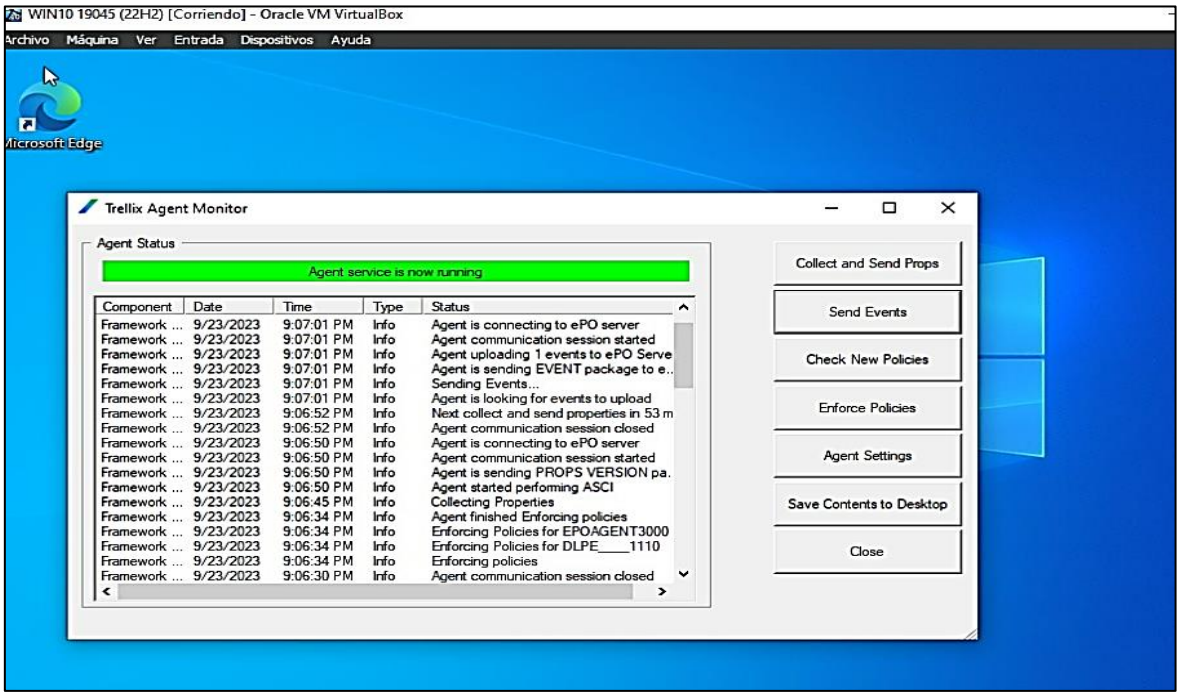


Figura 21. Validación de comunicación agente-consola (Windows 10)
Fuente: Elaboración Propia

Luego de haber realizado la instalación del agente, se realizó el despliegue del producto DLP a la máquina virtual desde la consola de administración directamente, según como vemos en la Figura 22.

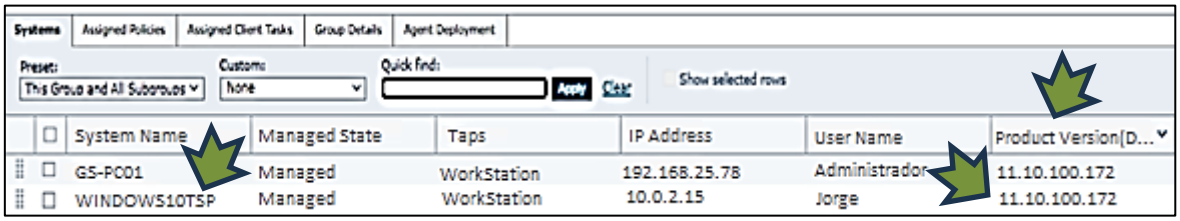


Figura 22. Validación del módulo DLP en la máquina de prueba
Fuente: Elaboración propia

3.2.4 Creación de la directiva de bloqueo DLP para el equipo de prueba

La creación de la directiva de prueba se realizó en la consola ePO que se tenía disponible en la empresa para realizar laboratorios y también se tenía disponible una licencia por un lapso de 3 meses la cual fue aprovechada para realizar las pruebas necesarias con las reglas de bloqueo que se configuraron.

Posterior al proyecto se procedió a renovar la licencia de prueba por un lapso de 3 meses más para realizar pruebas por otro personal para otro proyecto.

En la Figura 23 se puede visualizar la licencia de prueba que se renovó después de la culminación de nuestro proyecto.

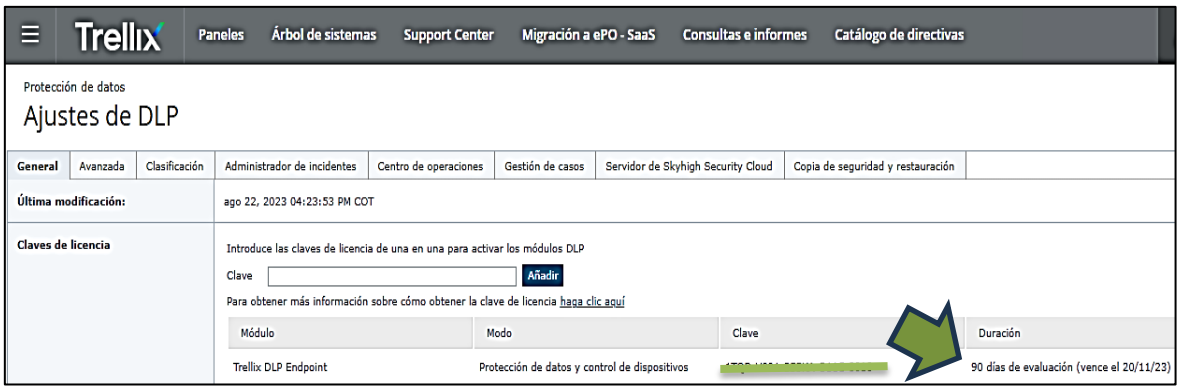


Figura 23. Licencia de prueba del módulo DLP
Fuente: Elaboración propia

Se procedió a validar en la consola las directivas DLP aplicadas por defecto a nuestro equipo de prueba.

Tal como vemos en la Figura 24 existen 3 tipos de directivas de DLP que se aplican a cada equipo que tenga el producto DLP, de las cuales nos enfocamos en la llamada “Directiva de DLP”, la cual se duplico y modifico para configurar las reglas de bloqueo que se aplicaron.

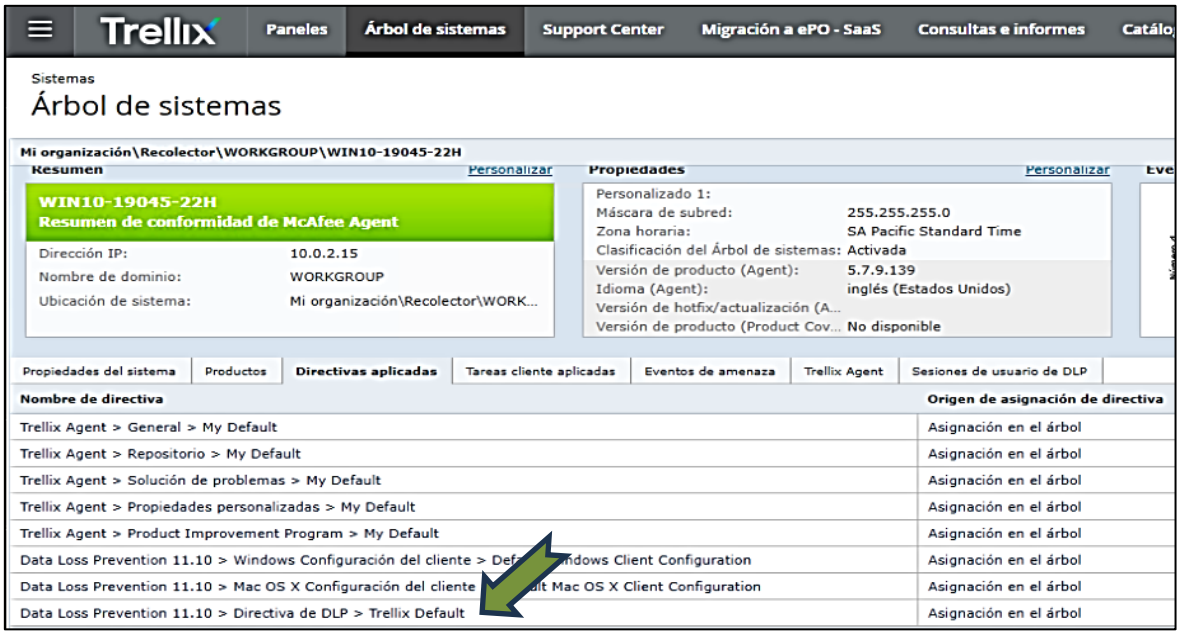


Figura 24. Directivas DLP por defecto
Fuente: Elaboración propia

Se procedió a duplicar la “Directiva de DLP” la cual se llamó “DLP | Máquinas Virtuales” tal como lo muestra la Figura 25, en esa directiva se creó las reglas de bloqueo.

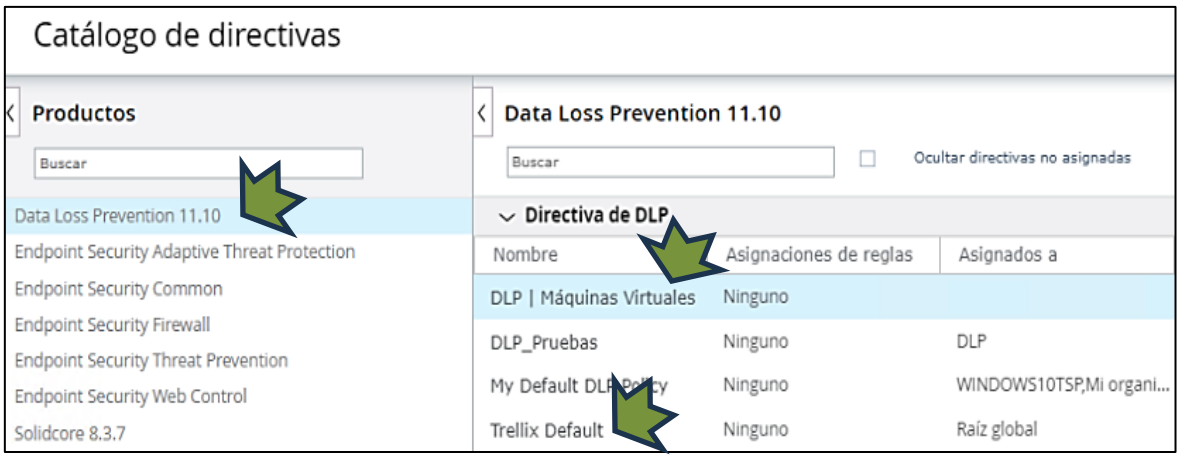


Figura 25. Directiva creada para las pruebas
Fuente: Elaboración propia

Dentro de la directiva llamada “DLP | Máquinas Virtuales” se procedió a crear el grupo para contener las reglas de bloqueo tal como vemos en la Figura 26.

Para el presente trabajo, se realizó el enfoque en las reglas de datos y en las reglas para dispositivos donde se estableció el bloqueo de puertos USB, bloqueo de bluetooth y bloqueo de correos salientes a dominios específicos.

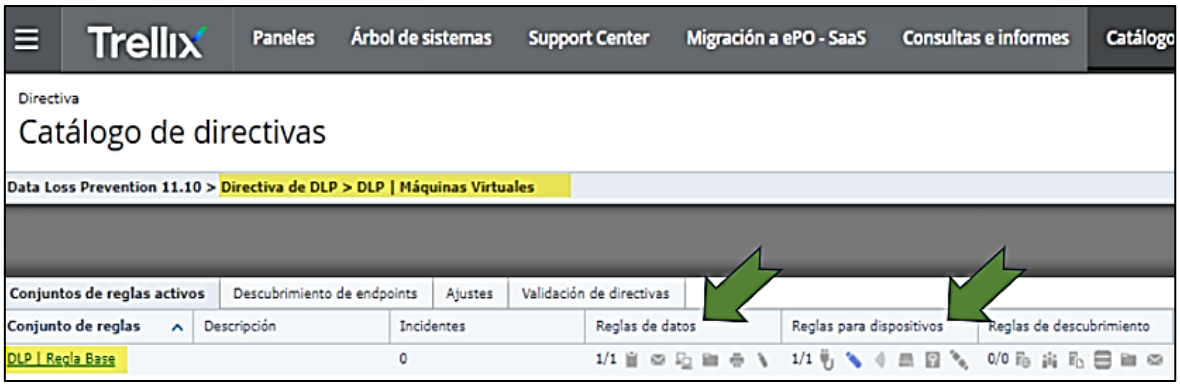


Figura 26. Grupo de reglas de prueba
Fuente: Elaboración propia

A) Bloqueo de correo electrónico Saliente

El bloqueo de correos electrónicos salientes fue muy importante llevarlo a cabo, dado que de esta forma se protege la información valiosa que los usuarios de las laptops tenían almacenada en sus equipos y pudieran ser enviados a un correo electrónico con dominio no conocido o permitido.

Para la configuración de este tipo de bloqueo por parte del DLP se ingresó a la Directiva de prueba creada tal como se muestra en la Figura 27.

Figura 27. Configuración de la directiva de prueba para bloqueo de correo
Fuente: Elaboración propia

Dentro de la directiva “DLP | Máquinas Virtuales” se ingresó al conjunto de reglas creada llamada “DLP | Regla Base” tal como puede visualizar en la Figura 28.

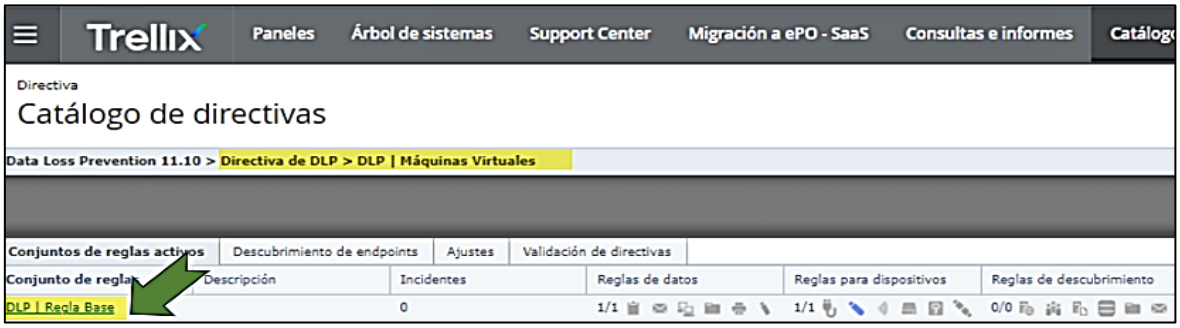


Figura 28. Conjunto de reglas para el bloqueo de correo
Fuente: Elaboración propia

Se ingreso a la sección de “Protección de datos” y desde ahí se seleccionó la pestaña de “Protección de correo electrónico” tal como lo se puede ver en la Figura 29.

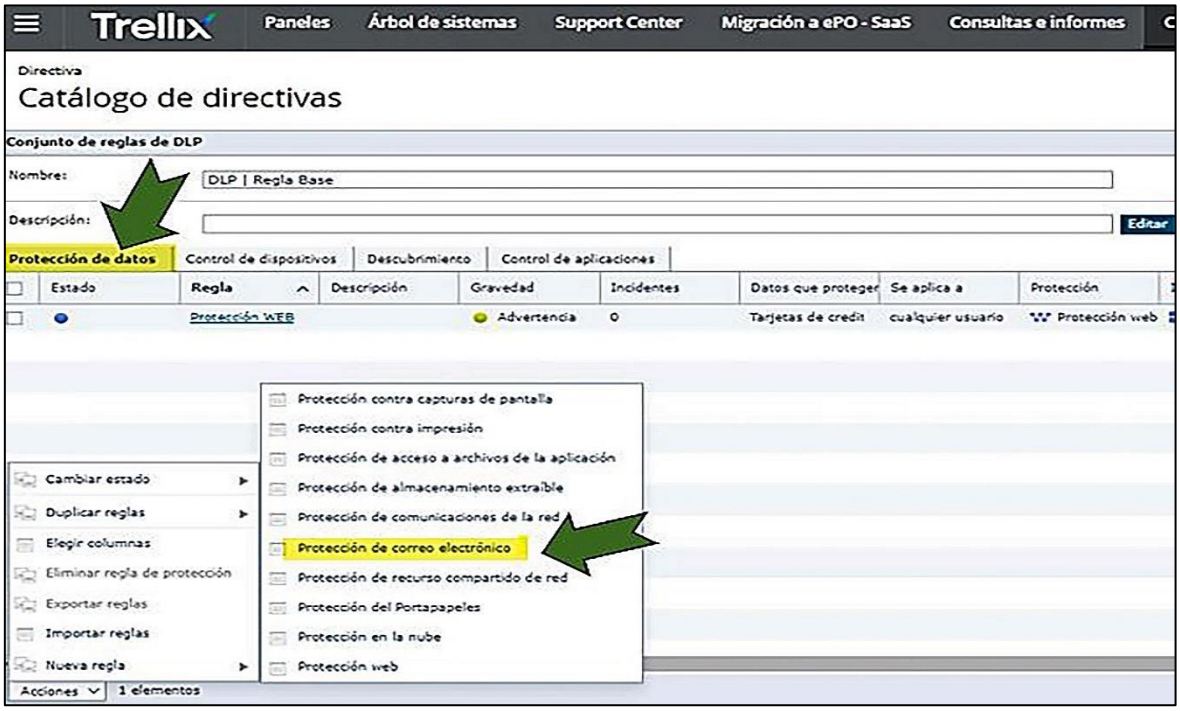


Figura 29. Regla de protección de correo electrónico
Fuente: Elaboración propia

Se creo un nombre para la regla, se colocó el estado de la regla como “Activada” y se clasifico la gravedad de los eventos como “Grave”, además la regla fue definida como implementada en “Trellix DLP Endpoint for Windows” tal como se puede visualizar en la Figura 30.

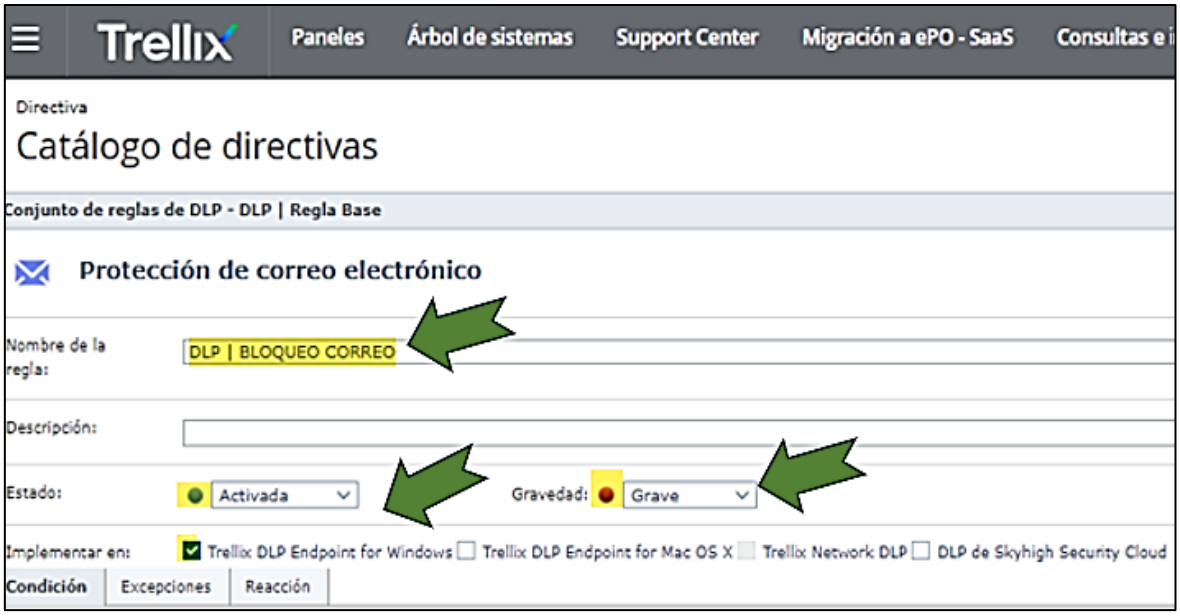


Figura 30. Configuración inicial de la regla de bloqueo de correo
Fuente: Elaboración propia

El umbral de destinatario se dejó configurado como “ninguno” y dentro de la sección de clasificación se seleccionó en “uno de los elementos del correo electrónico” según lo mostrado en la Figura 31.

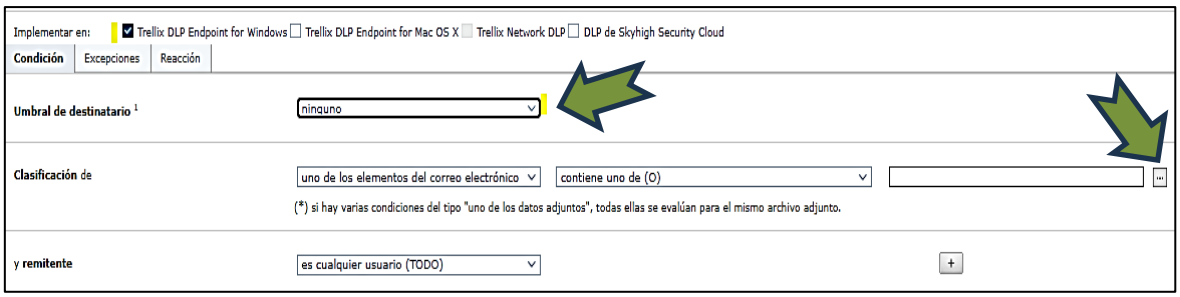


Figura 31. Configuración de bloqueo de correos, sección condiciones
Fuente: Elaboración propia

Dentro de la sección de clasificación al elegir clasificaciones, se creó una nueva opción colocándole por nombre “EMAIL PROTECTION”, luego de ser agregada esta opción apareció en la lista para poder ser seleccionada tal como se puede visualizar en las Figuras 32 y 33.

Con dicha configuración al momento que aparezca algún evento del tipo email será clasificado bajo la etiqueta de “EMAIL PROTECTION”.

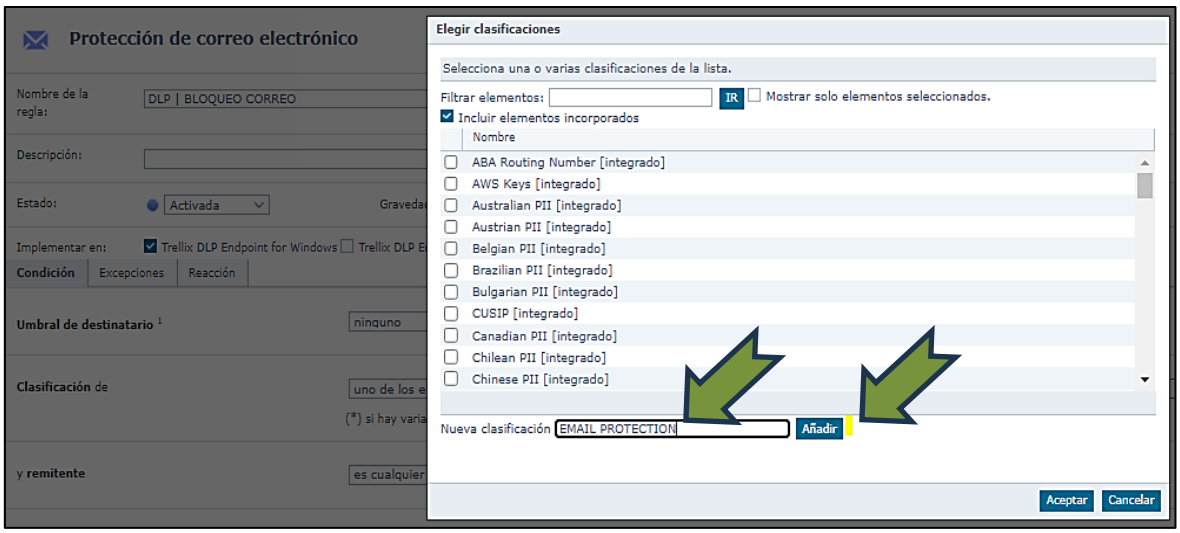


Figura 32. Definimos el tipo de clasificación
Fuente: Elaboración propia

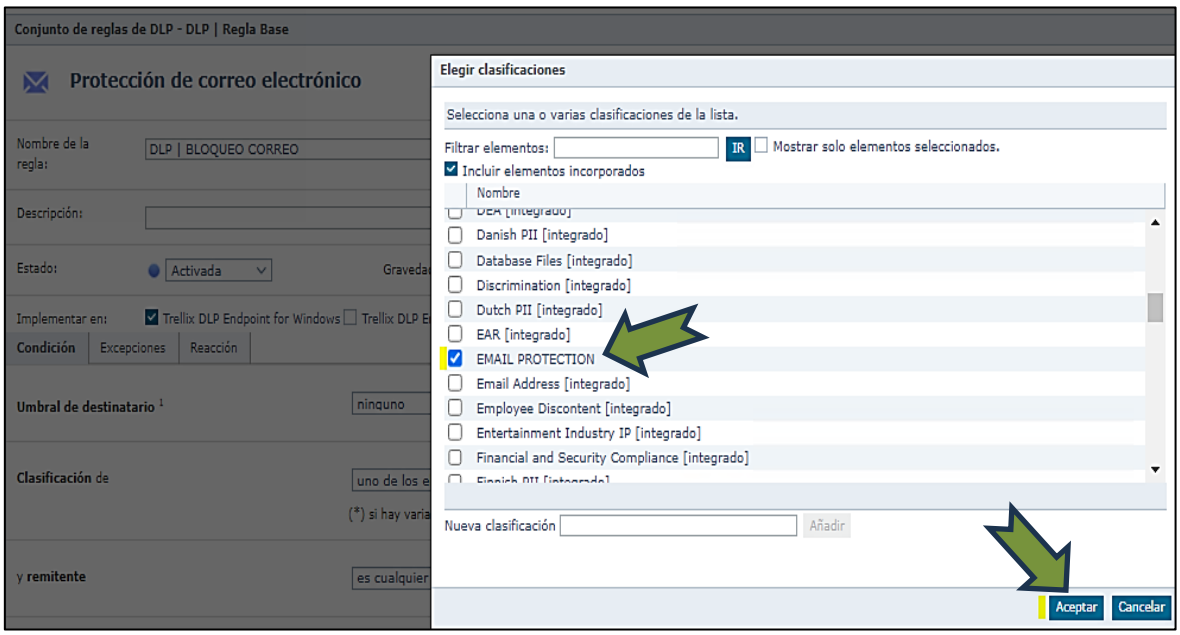


Figura 33. Selección del tipo de clasificación
Fuente: Elaboración propia

En el campo “Remitente” y “Sobre de correo electrónico” se dejó las opciones por defectos, en el campo “lista de destinatarios incluye” se seleccionó la opción “al menos un destinatario que pertenece a todas las listas de dirección de correo electrónico siguientes”.

Se procedió a seleccionar el grupo que se tomó como referencia para su lista de bloqueo, tal como se puede visualizar en la Figura 34.

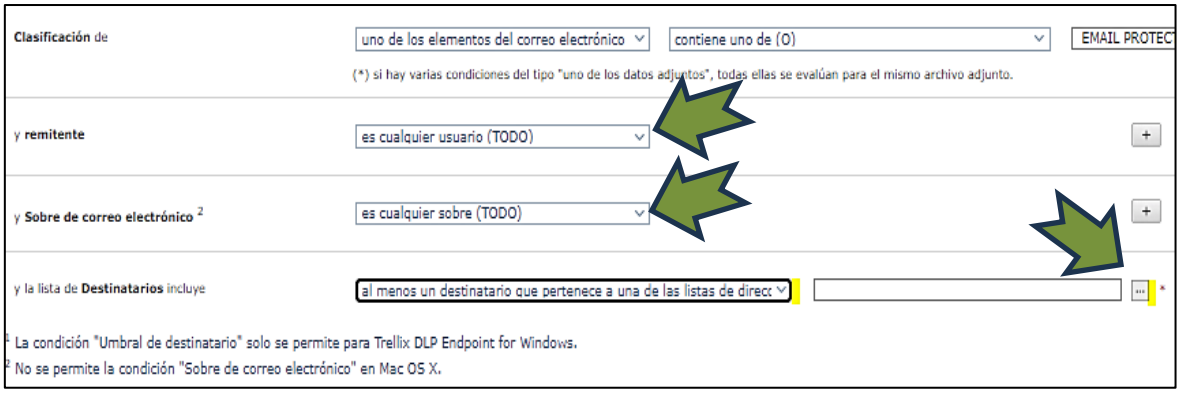


Figura 34. Configuración de la regla de bloqueo, destinatarios
Fuente: Elaboración propia

Dentro de la sección de “Destinatarios” se seleccionó “Nuevo elemento” donde se abrió una ventana para agregar los dominios de correo a bloquear, tal como se puede apreciar en la Figura 35.

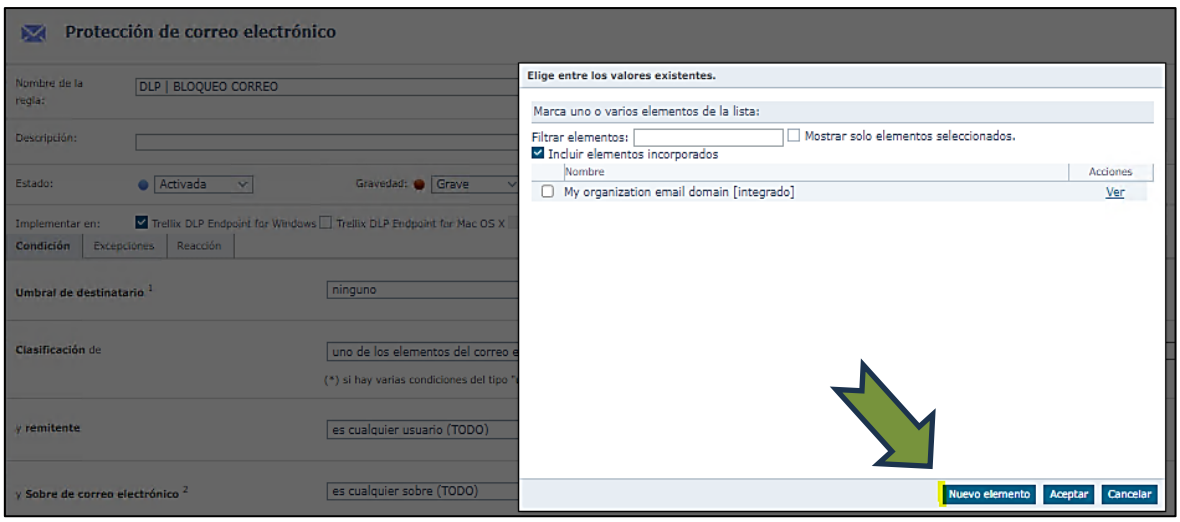


Figura 35. Generación de un nuevo grupo de dominio
Fuente: Elaboración propia

Se colocó como nombre del grupo “Dominio No Permitido” y se añadió los dominios más frecuentes de uso general que fueron considerados a ser bloqueados tal como se puede visualizar en la Figura 36.

Cabe indicar que los dominios de correo que fueron bloqueados son aquellos dominios que la empresa Securesoft deseo que no se pueda enviar correos desde los equipos de ingeniería.

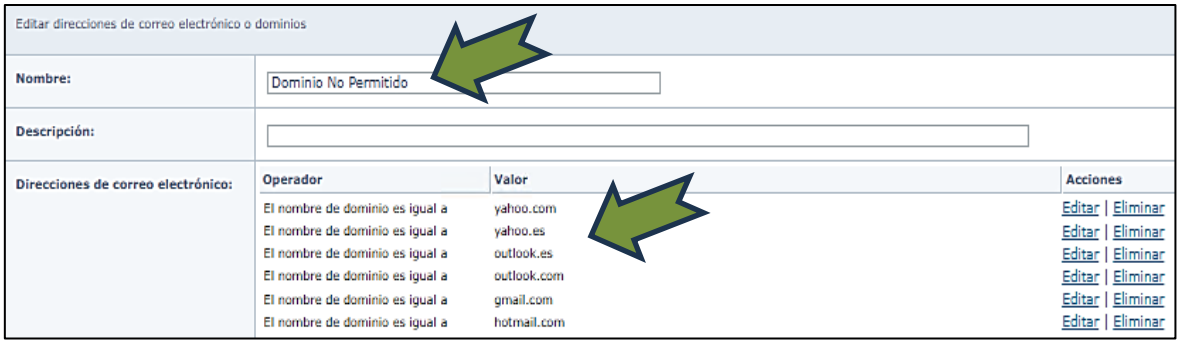


Figura 36. Agregar los dominios a la lista de bloqueo
Fuente: Elaboración propia

Una vez se terminó de configurar la sección de “Condición” para nuestro Bloqueo de Correos electrónicos, se procedió a configurar la sección de “Reacción” en donde se aplicó la acción a tomar como “bloqueo” y se eligió la Notificación que se iba a presentar cuando apareciera algún evento de bloqueo de correo electrónico saliente, tal como se puede apreciar en la Figura 37.

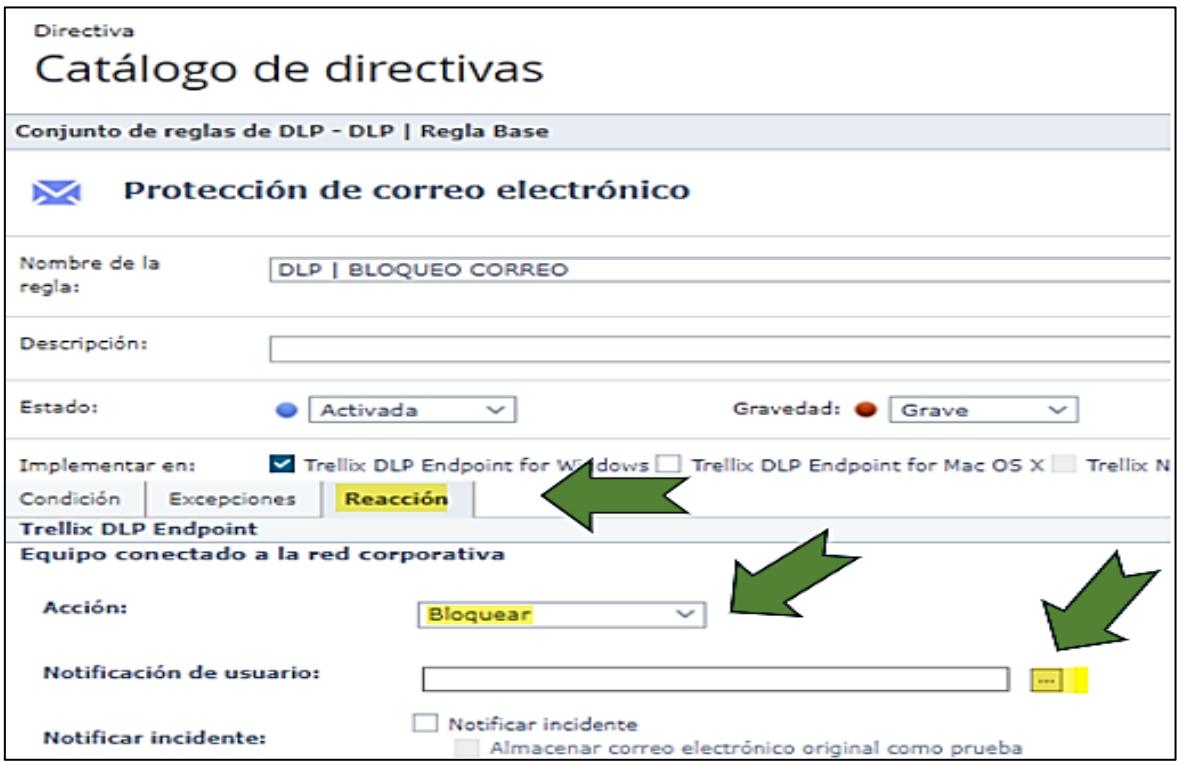


Figura 37. Configuración de la pestaña de reacción
Fuente: Elaboración propia

Dentro de las opciones de notificación de usuario se pudo ver varias opciones creados por defecto, en nuestro caso se procedió a crear un nuevo elemento tal como se puede ver en la Figura 38.

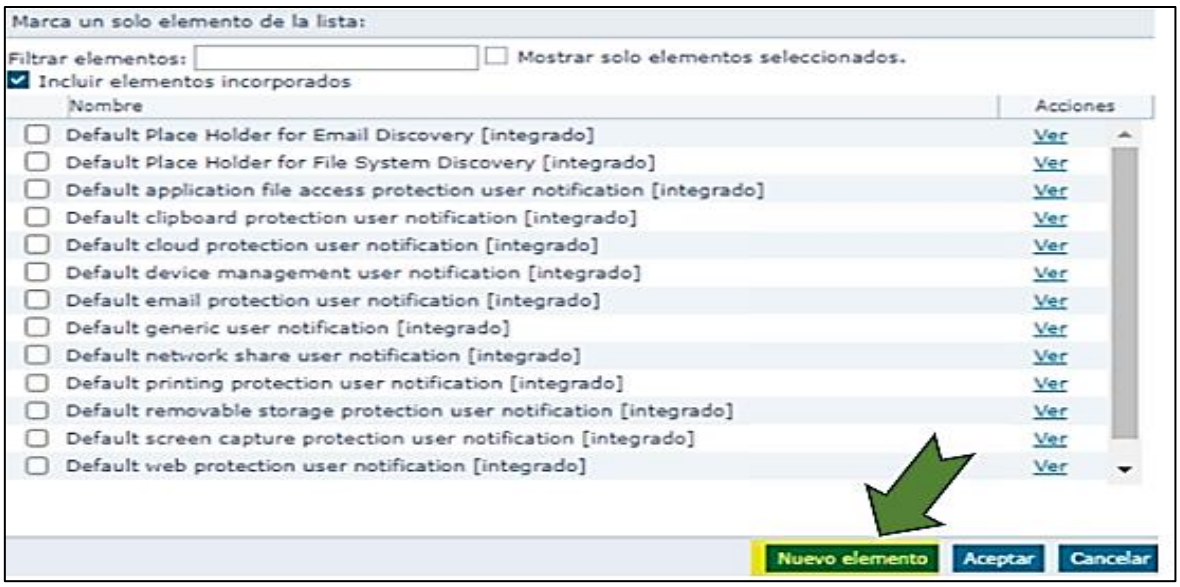


Figura 38. Creación del tipo de notificación para el bloqueo de correos
Fuente: Elaboración propia

Se procedió a darle un nombre al nuevo elemento el cual fue “BLOQUEO DE CORREO” y la posición del cuadro de diálogo fue en “Bandeja del sistema”. Adicionalmente se colocó mensaje intuitivo para el usuario el cual fue “Recipient domain not allowed SECURESOFT CORPORATION” tal como se puede visualizar en la Figura 39, con ello quedo configurado la notificación de eventos de este tipo.

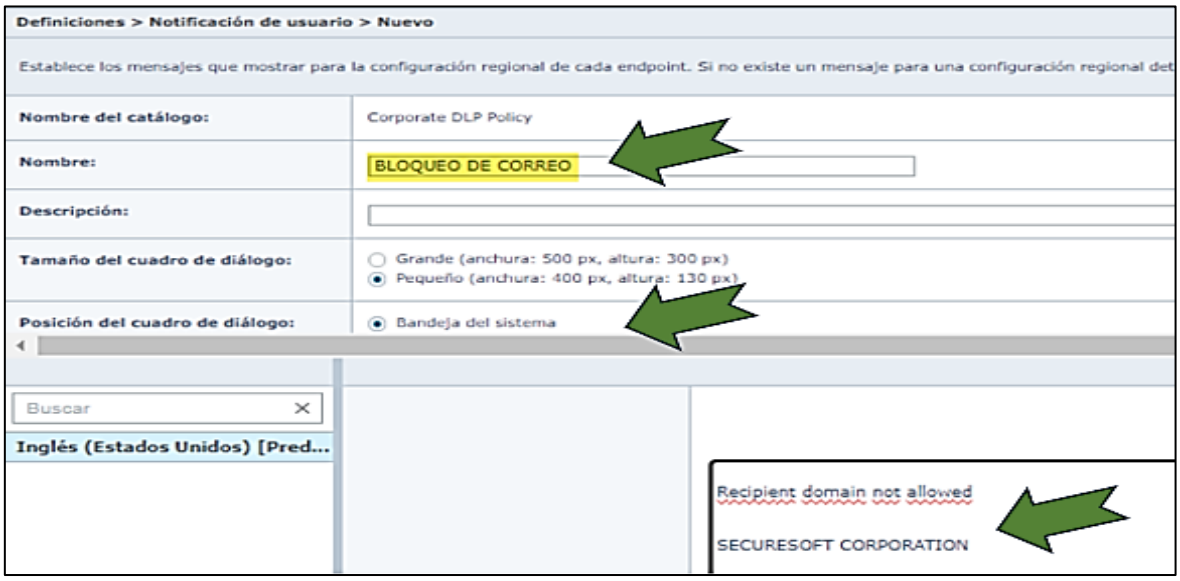


Figura 39. Configuración de la notificación para el bloqueo de correos
Fuente: Elaboración propia

Adicional a ello tal como se puede visualizar en la Figura 40 se dejó activado los checks de “Notificar incidente” y “Almacenar correo original como prueba”. El

campo Acción se dejó seleccionado en “Reaccionar de la misma manera que el sistema conectado” para que de este modo la regla se pueda activar tanto si el equipo estuviera fuera o dentro de la red de la empresa.

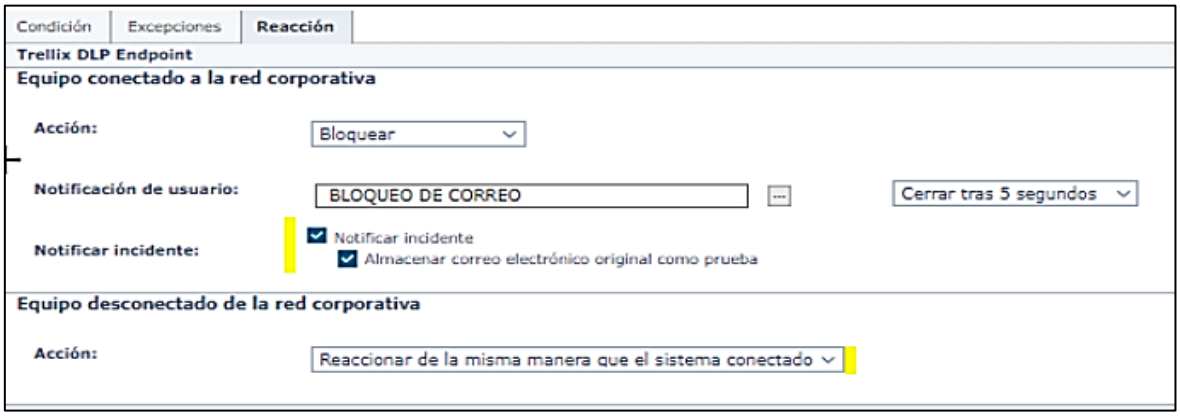


Figura 40. Configuración de la pestaña de reacción con respecto a alertas
Fuente: Elaboración propia

B) Bloqueos de Puertos USB

El bloqueo de puertos USB fue configurado para proteger los equipos y evitar que se instale software que no están permitidos dentro la empresa SecureSoft o que se extraiga información por este medio lo cual conllevaría a pérdidas monetarias a la empresa o perdida de información de los clientes a los que se brinda soporte.

Para la creación de la regla de bloqueo de los puertos USB se siguió los siguientes pasos para su adecuada configuración.

Se ingreso a la Directiva de prueba creada tal como podemos visualizar en la Figura 41.

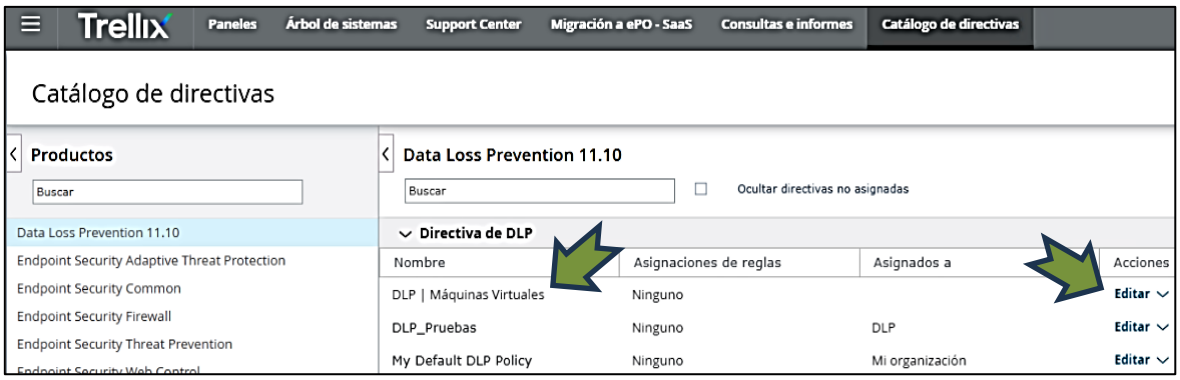


Figura 41. Configuración de la directiva de prueba para bloqueo USB
Fuente: Elaboración propia

Se ingreso al conjunto de reglas “DLP | Regla Base” tal como se puede ver en la Figura 42.

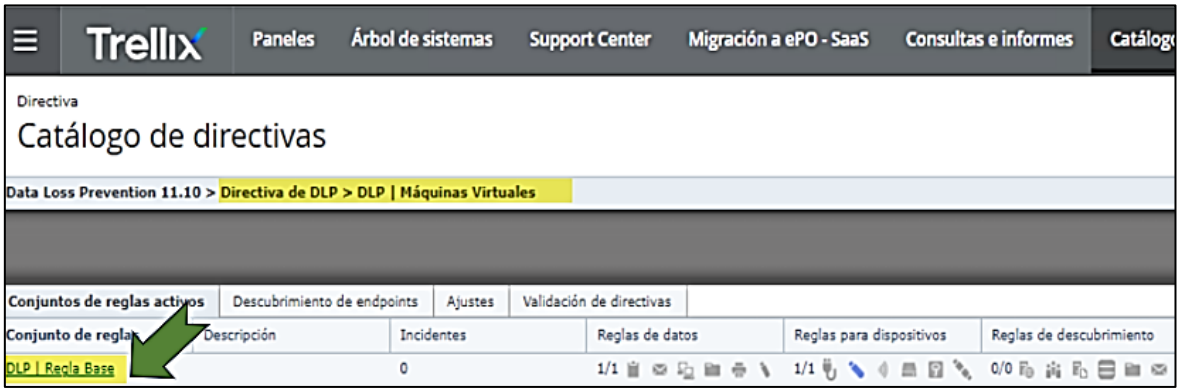


Figura 42. Conjunto de reglas para el bloqueo USB
Fuente: Elaboración propia

Se selecciono la pestaña de “Control de dispositivos” y posterior a ello se ingresó en la opción de Acciones, “Nueva regla” seguido de “Regla para dispositivos de almacenamiento extraíbles” según como se puede visualizar en la Figura 43.

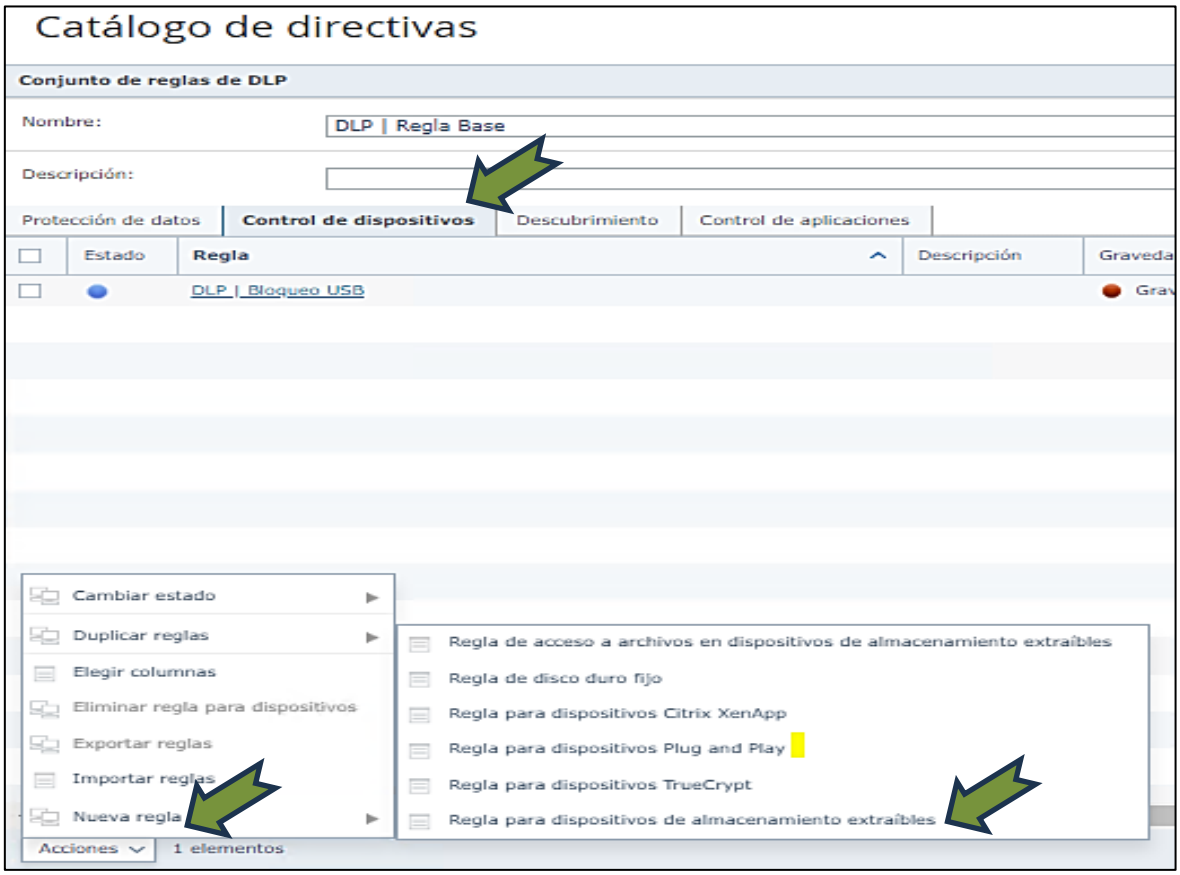


Figura 43. Regla de protección de bloqueo USB
Fuente: Elaboración propia

Una vez dentro de la nueva regla, se procedió a darle un nombre para el bloqueo de puertos USB el cual se llamó “DLP | Bloqueo USB”.

El estado que inicialmente indicaba “Desactivado”, procedimos pasarlo a “Activada”, la Gravedad que inicialmente aparecía como “Advertencia”, procedimos pasarlo a “Grave” según fue la prioridad que se le dio a este tipo de eventos.

Esta regla por defecto figuraba para ser implementada en “Trellix DLP Endpoint for Windows” y “Trellix DLP Endpoint for Mac OS X”, la cual para el caso de la empresa Securesoft solo se debió dejar seleccionado la opción de “Trellix DLP Endpoint for Windows” debido a que solo se tenía equipos Windows a los cuales aplicar la regla.

Para el campo de “Usuario final” se seleccionó la opción de “es cualquier usuario (TODO)”, con lo cual se definió que esta regla se aplique a todos los usuarios que tengas aplicada la directiva DLP creada.

Adicional a ello en el campo Almacenamiento extraíble se procedió a hacer click en los 3 puntos seguidos a fin de seleccionar la categoría de dispositivos a los cuales se iba a aplicar la regla creada.

Todo lo antes mencionada se puede visualizar en la Figura 44.

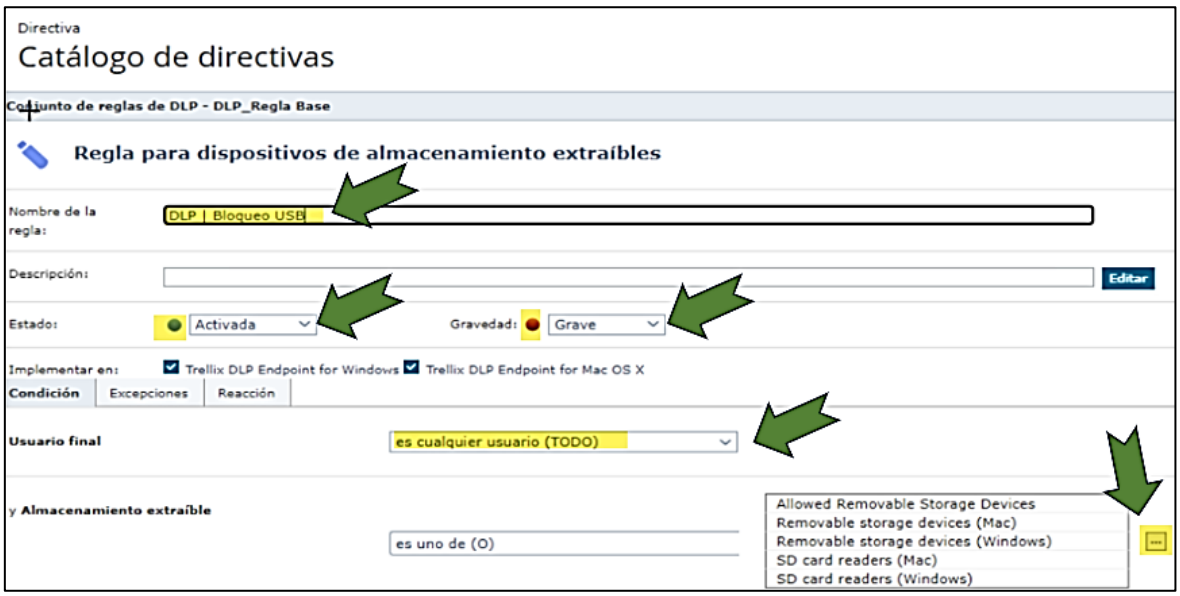


Figura 44. Configuración inicial de la regla de bloqueo de USB
Fuente: Elaboración propia

Se procedió a seleccionar los tipos de dispositivos a los cuales se aplicó la regla de bloqueo, entre los dispositivos bloqueados se encontraban dispositivos como discos duros, USB y tarjetas microSD tal como se puede ver en la Figura 45.

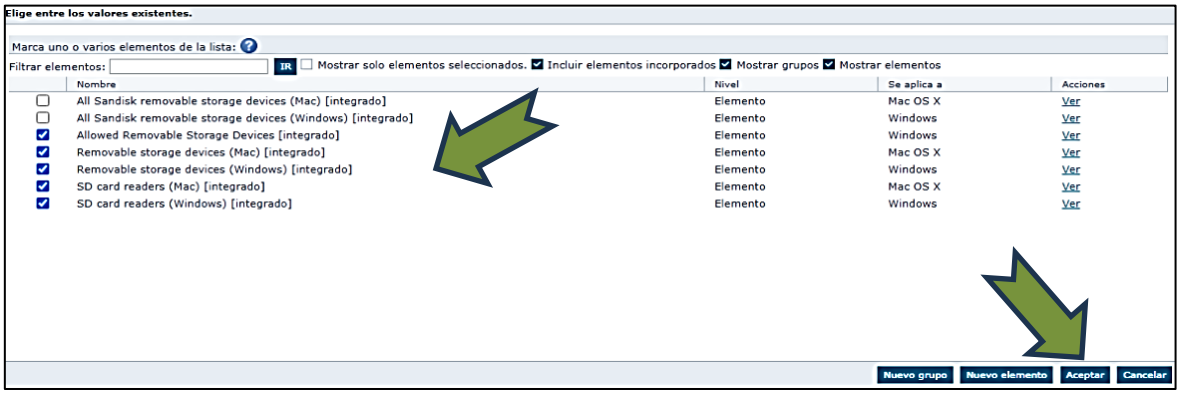


Figura 45. Elección de los valores a bloquear por USB
Fuente: Elaboración propia

Una vez se realizó la configurado las condiciones de bloqueo, se procedió a configurar la pestaña de “Reacción”.

En el campo acción se le aplico la opción de “Bloquear”, en el campo notificación de usuario se escogió la opción de “Notificación de usuario” y cerrar tras 10 segundos.

Se dejo activado el check de “Notificar incidente” para proceder a guardar los cambios realizados, con esta configuración se culminó la creación de la regla de bloqueo de acceso de dispositivos de almacenamiento. Tal como se puede visualizar en la Figura 46.

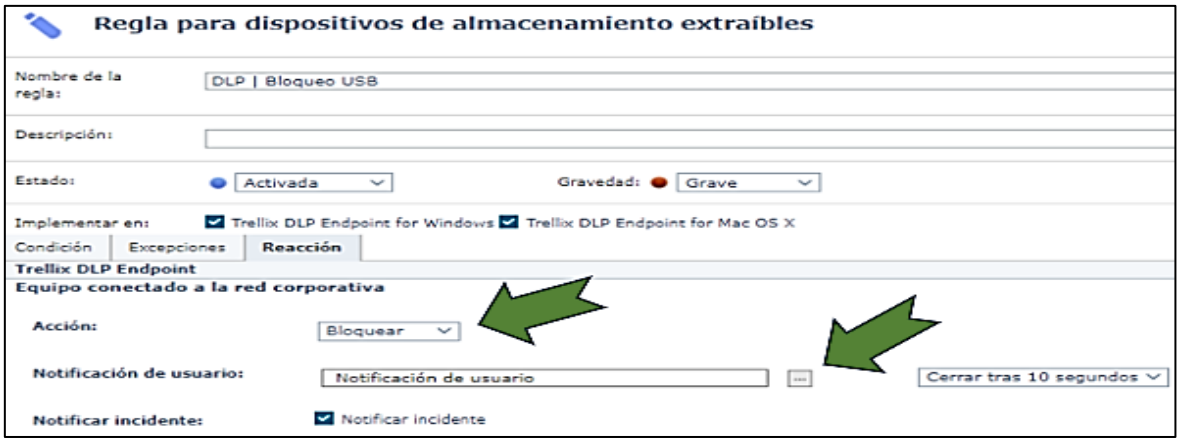


Figura 46. Configuración de la pestaña de reacción para bloqueo USB
Fuente: Elaboración propia

C) Bloqueos Bluetooth

El bloqueo de bluetooth fue configurado para proteger los equipos y evitar que se envié o reciba archivos a través de este medio y así contribuir con la seguridad en los equipos del área de ingeniería.

Durante la configuración de la regla de bloqueo bluetooth se siguió los siguientes pasos a fin de realizar la configuración de forma adecuada.

Se ingreso a la Directiva creada tal como se puede visualizar en la Figura 47.

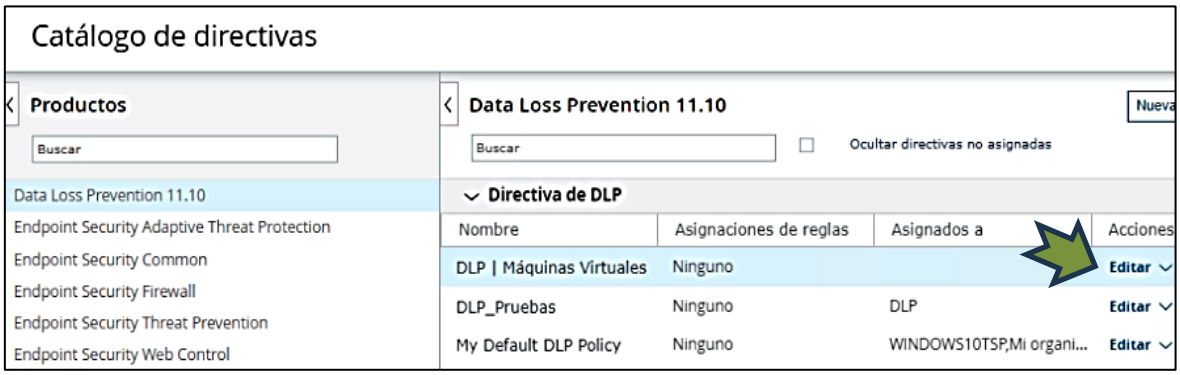


Figura 47. Configuración de la directiva de prueba para bloqueo Bluetooth
Fuente: Elaboración propia

Se selecciono el conjunto de reglas “DLP | Regla Base” tal como se puede visualizar en la Figura 48, en dicho conjunto de reglas se realizó la creación de la regla de bloqueo bluetooth.

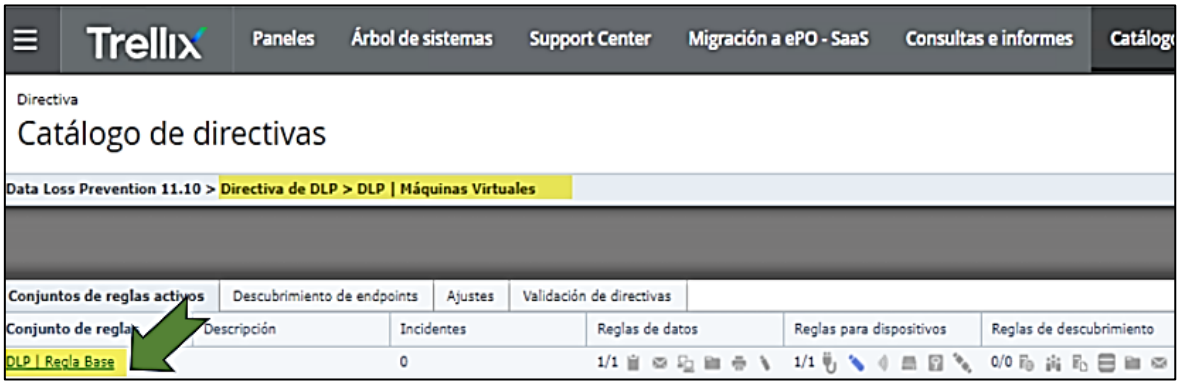


Figura 48. Conjunto de reglas para el bloqueo bluetooth
Fuente: Elaboración propia

Se selecciono la pestaña de “Control de dispositivos” y nos dirigimos a la opción de Acciones en donde se seleccionó “Regla para dispositivos Plug and Play”.

Lo antes mencionado se puede visualizar en la Figura 49.

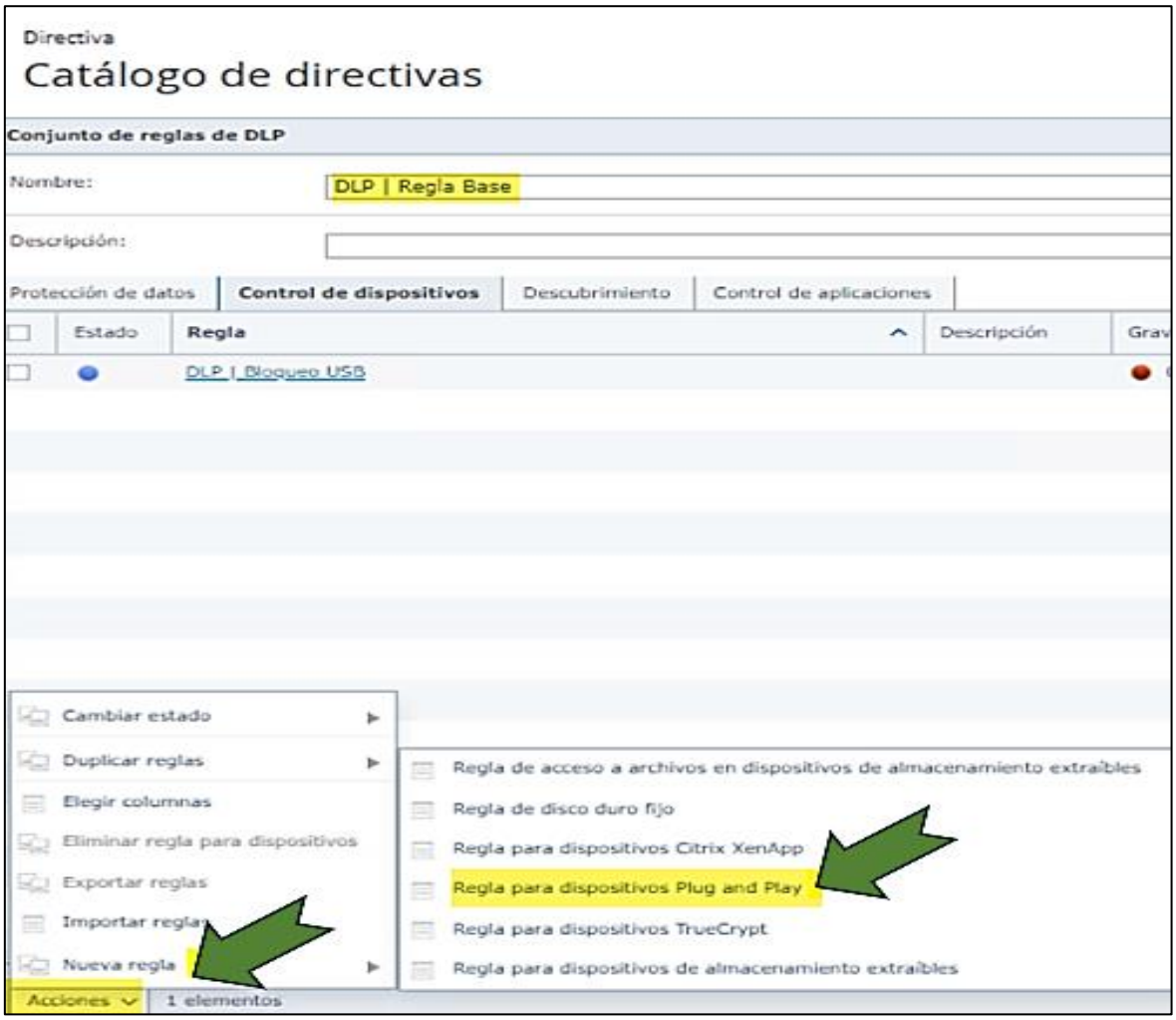


Figura 49. Regla de protección de bloqueo Bluetooth
Fuente: Elaboración propia

Se le dio un nombre a la nueva regla de bloqueo creada la cual fue “DLP | BLOQUEO BLUETOOTH”.

El estado que inicialmente se encontró como “Desactivado” se procedió a cambiar a “Activada” y la Gravedad que inicialmente figuraba como “Advertencia” se procedió a cambiar a “Grave” según fue la prioridad que se le dio a este tipo de eventos.

La regla por defecto se encontró definida a implementarse en “Trellix DLP Endpoint for Windows” y “Trellix DLP Endpoint for Mac OS X”, pero para las necesidades de la empresa Securesoft que solo cuenta con equipos Windows, solo se dejó seleccionado la opción de “Trellix DLP Endpoint for Windows”.

El campo “Usuario final” se definió en “es cualquier usuario (TODO)” con lo cual se le indico a la regla que se ejecutara a todos los usuarios que tuvieran aplicada la directiva.

Adicional a ello en el campo “Plug and Play” se procedió a hacer click en los 3 puntos seguidos a fin de seleccionar la categoría de dispositivos a los cuales se iba a aplicar la regla creada.

Todo lo antes mencionada se puede visualizar en la Figura 50.

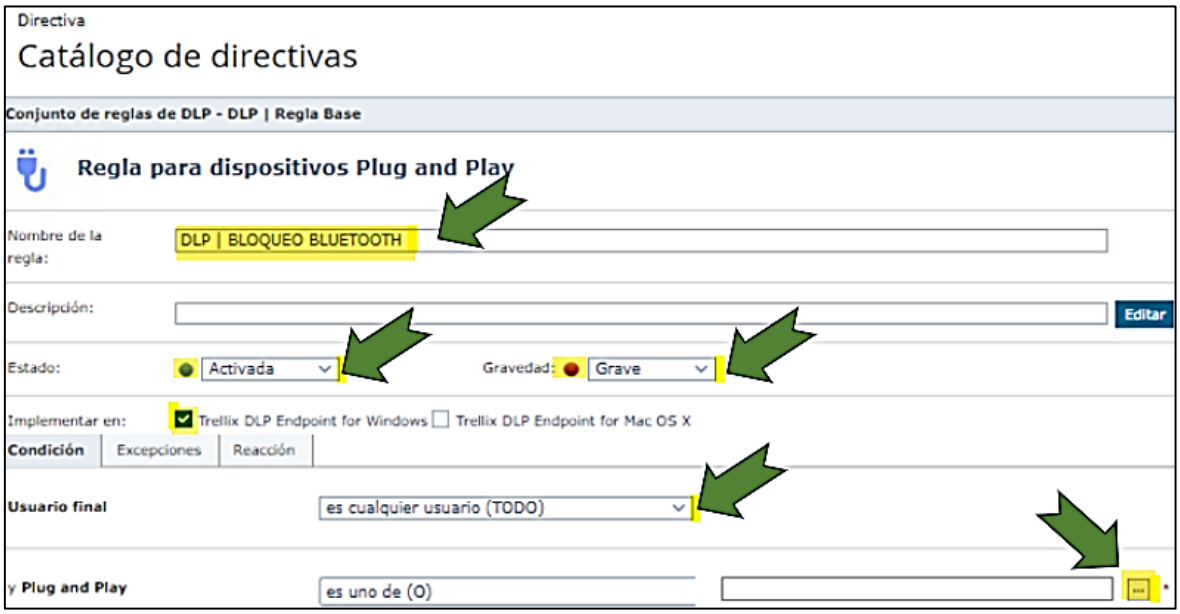


Figura 50. Configuración inicial de la regla de bloqueo bluetooth
Fuente: Elaboración propia

Estando dentro de la sección de Plug and Play se procedió a Seleccionar la opción que corresponde a los dispositivos Bluetooth, tal como se puede ver en la Figura 51.

Dentro del cuadro que se puede ver en la Figura 51 se pudo encontrar todos los dispositivos bluetooth estándares, entre ellos encontramos la transferencia de información con dispositivos móviles y la comunicación con periféricos como impresoras y monitores.

Cabe indicar que la regla de bloqueo de bluetooth que fue configurada solo afecto a los dispositivos que hacían uso de la transferencia de datos, estando excluidos de esto dispositivos como mouse y teclados.

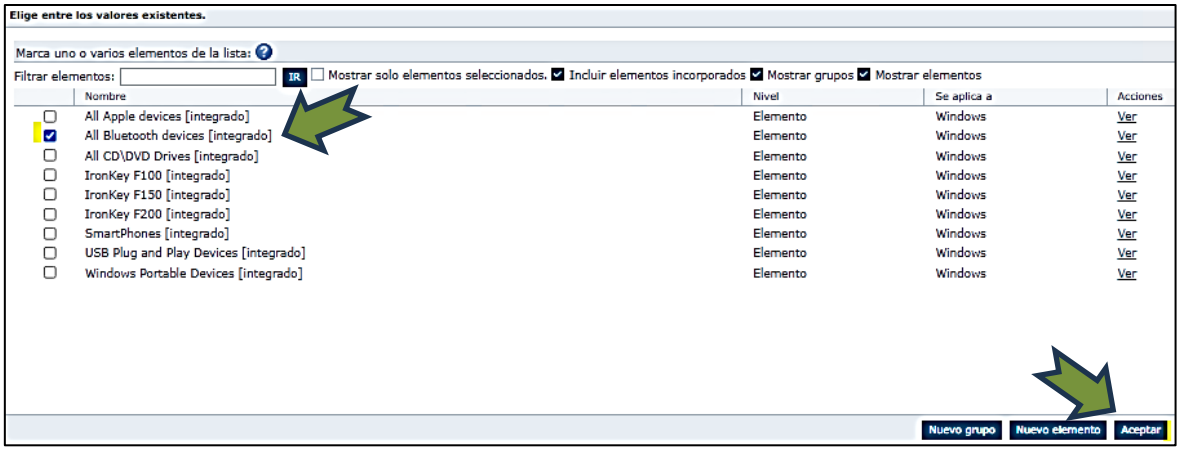


Figura 51. Elección de los valores a bloquear por Bluetooth
Fuente: Elaboración propia

En la Figura 52 se puede observar el campo Plug and Play cuando fue definido para todos los dispositivos bluetooth que hacen uso de la transferencia de datos.

Figura 52. Definición de los dispositivos bluetooth a bloquear
Fuente: Elaboración propia

Luego de haber culminado la configuración de la pestaña “Condición” se continuo con la configuración de la pestaña “Reacción”.

Dentro de la pestaña de “Reacción” la acción que se configuro para este tipo de eventos fue “Bloquear”, así mismo se seleccionó una notificación para los usuarios cuando se llegue a generar algún tipo de evento bluetooth. Dicha configuración se puede visualizar en la Figura 53.

Figura 53. Configuración de la pestaña de reacción para bloqueo Bluetooth
Fuente: Elaboración propia

Así mismo tal como se puede ver en la Figura 54, se dejó marcado la opción de "Notificar incidente" y en los campos de Acción se colocó la opción de "Reaccionar de la misma manera que el sistema conectado" para que la regla configurada se ejecute en los equipos que estén fuera o dentro de la red de la empresa.

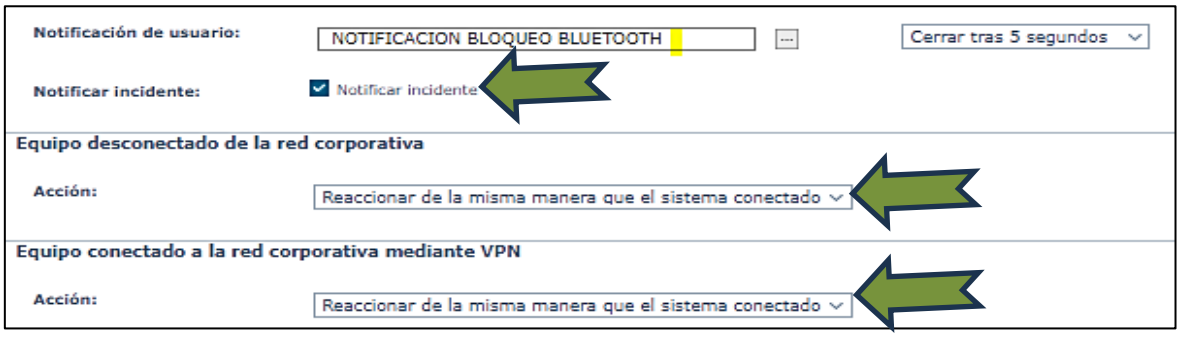


Figura 54. Configuración de las notificaciones para bloqueo de Bluetooth
Fuente: Elaboración propia

3.2.5 Aplicación de la directiva en la Máquina Virtual

En la Figura 55 se puede visualizar el equipo al cual se le aplico la directiva DLP posterior a la configuración de las reglas de bloqueo, entre las cuales se encuentra la regla de bloqueo de correos saliente, regla de bloqueo de puertos USB y regla de bloqueo bluetooth.

Figura 55. Equipo de prueba sin la directiva aplicada
Fuente: Elaboración propia

Para poder aplicar la Directiva DLP se ingresó en la configuración del equipo al cual se deseó aplicar dicha directiva y se seleccionó la opción de “Editar directivas en un solo sistema” tal como se puede visualizar en la Figura 56.

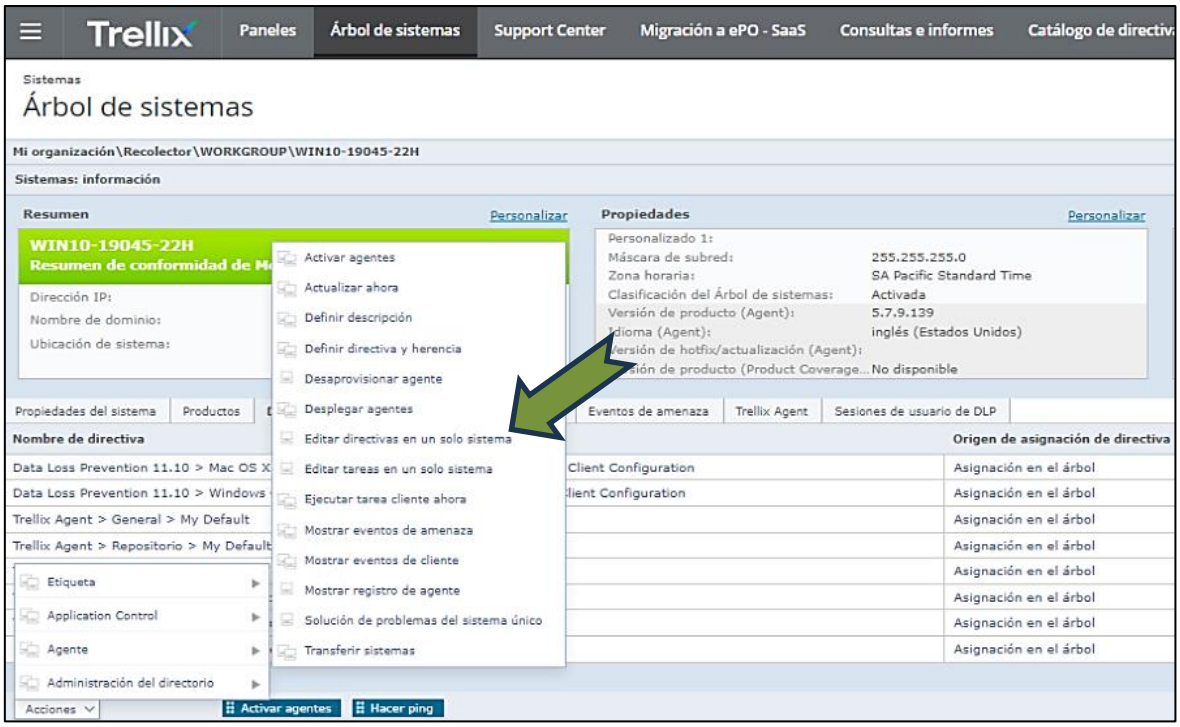


Figura 56. Aplicación de la directiva de prueba
Fuente: Elaboración propia

Se selecciono el producto “Data Loss Prevention 11.10” y se escogió editar la directiva en la cual se realizó, cuyo nombre fue “Directiva de DLP” tal como se puede visualizar en la Figura 57.

Es importante indicar que las otras dos directivas se dejaron por defecto, debido a que no se realizó ningún tipo de configuración en ellas.

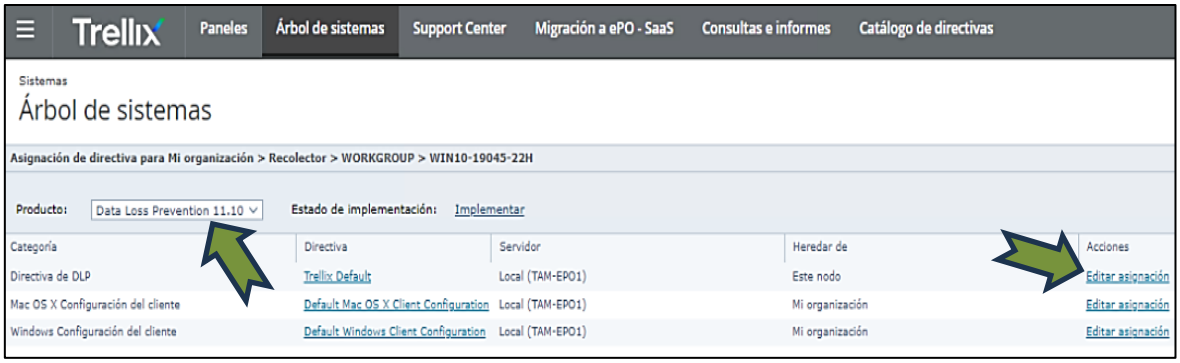


Figura 57. Edición de la directiva aplicada
Fuente: Elaboración propia

Para proceder a realizar el cambio de directiva se seleccionó la opción de "Interrumpir herencia y asignar la directiva y la configuración a partir de este punto", con lo cual se habilito la opción para poder seleccionar una directiva diferente a la que se tenía por defecto, tal como se puede visualizar en la Figura 58.

Figura 58. Interrumpir herencia de la directiva actual
Fuente: Elaboración propia

Posterior al cambio realizado se pudo validar en la configuración del equipo, en la sección de producto Data Loss Prevention que figuraba ya con el nombre de la directiva que contenía las reglas de bloqueo que fueron configuradas. Esto se puede visualizar en la Figura 59.

Este proceso de cambio de directiva que fue posible debido a la interrupción de la herencia fue fundamental, debido a que sin este paso no hubiera sido posible que se pueda aplicar las reglas de bloqueo.

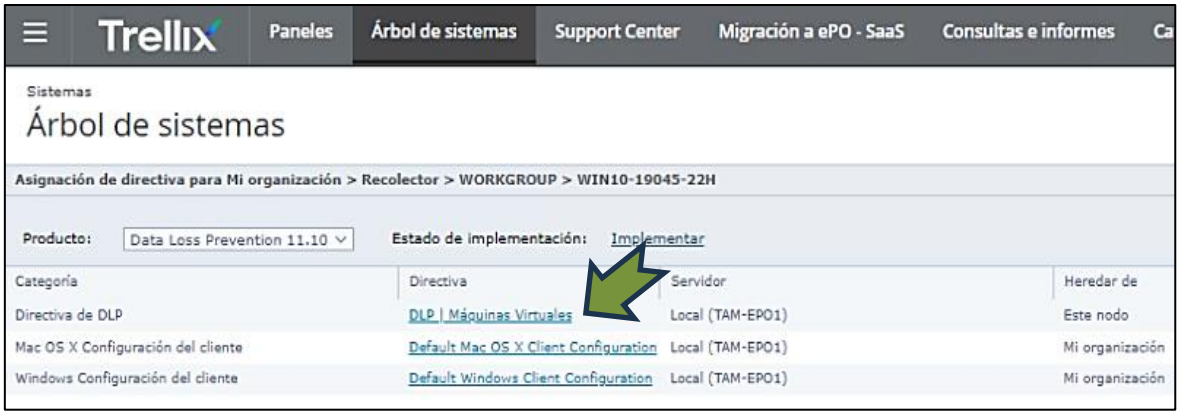


Figura 59. Validación de la aplicación de la directiva de prueba
Fuente: Elaboración propia

En la Figura 60 se muestra la Máquina Virtual WIN10-19045-22H con IP 10.0.2.15 en la cual se instaló la versión 5.7.9 del agente de Trellix, además se puede visualizar todas las directivas que poseía el equipo entre las cuales se puede observar la directiva “Data Loss Prevention 11.10 > Directiva de DLP > DLP | Máquinas Virtuales”.

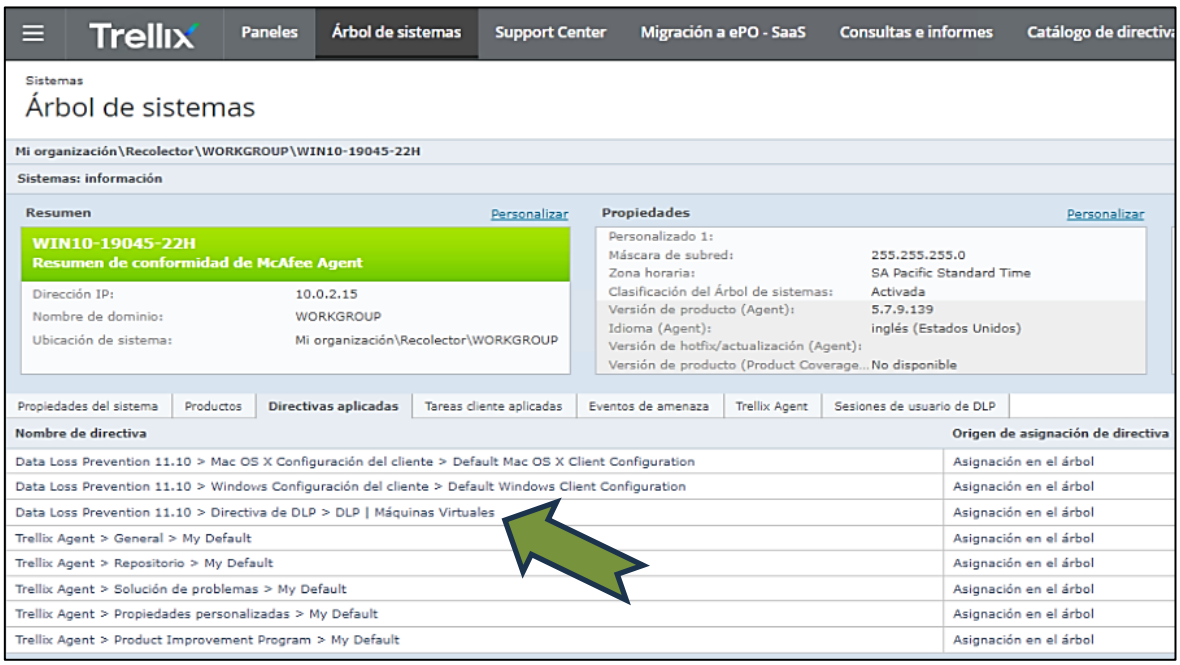


Figura 60. Total de directivas aplicadas en el equipo de prueba
Fuente: Elaboración propia

Otra forma de validar que la directiva fue correctamente aplicada es en la misma directiva, en donde se pudo observar que el equipo de prueba se encontraba bajo la directiva creada tal como se puede visualizar en la Figura 61.

Figura 61. Directiva de bloqueo DLP aplicándose al equipo de prueba
Fuente: Elaboración propia

3.2.6 Aplicación de la directiva DLP en los equipos empresariales

Luego de haberse aplicado la directiva en el equipo de prueba y observar resultados satisfactorios, se procedió a replicar dicha directiva con mínimas modificaciones de configuración en el ePO principal de la empresa SecureSoft.

Al momento de aplicar la directiva en los equipos empresariales se pudo validar que el producto de Trellix DLP Endpoint poseía una duración permanente, lo cual nos indicaba que la licencia de funcionamiento que se iba a utilizar no estaba sujeta a caducidad.

Lo antes mencionado se puede observar en la Figura 62.

Figura 62. Duración de la licencia en el DLP de Securesoft
Fuente: Elaboración propia

En la Figura 63 se puede observar los grupos en la consola ePO, entre dichos grupos se puede ver el grupo “INGENIERIA” al cual se le aplico la directiva de DLP que fue configurada.

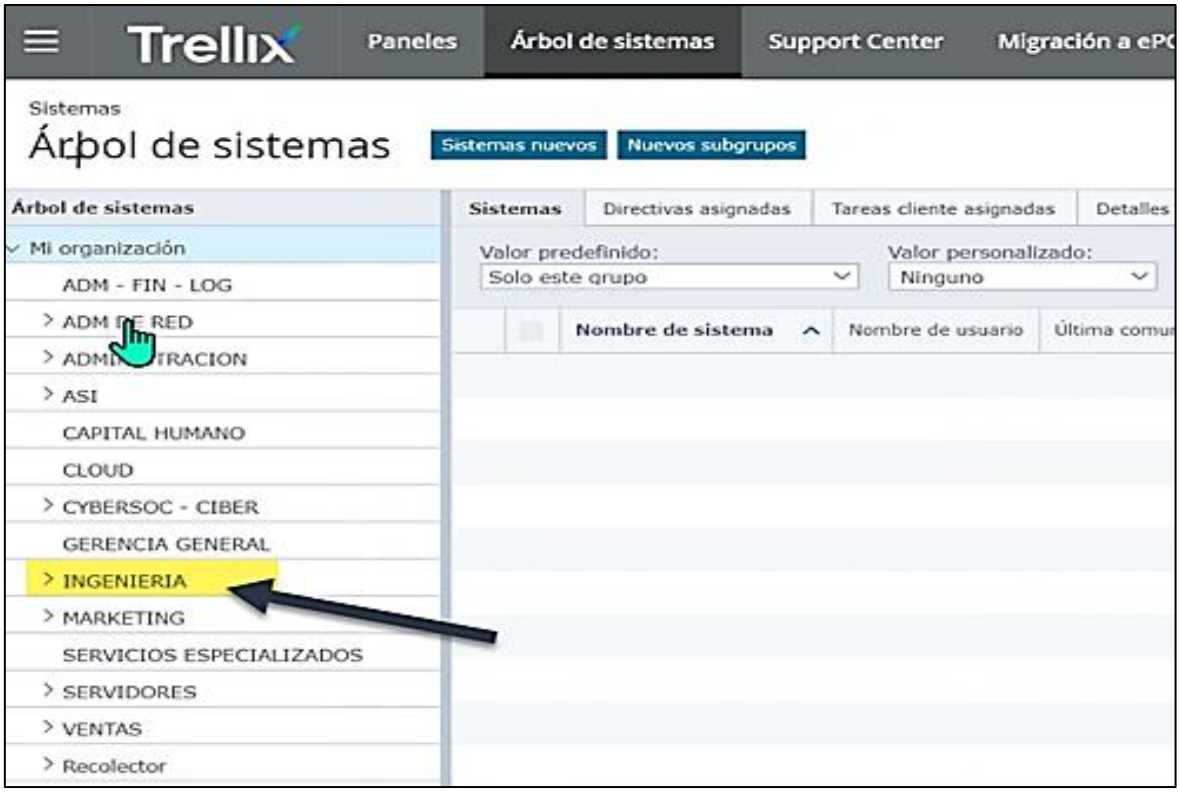


Figura 63. Grupo en el cual se aplicó el DLP y sus directivas
Fuente: Elaboración propia

Dentro del grupo INGENIERIA se encontró subgrupos los cuales contenían el registro de los equipos tal como se puede visualizar en la Figura 64.

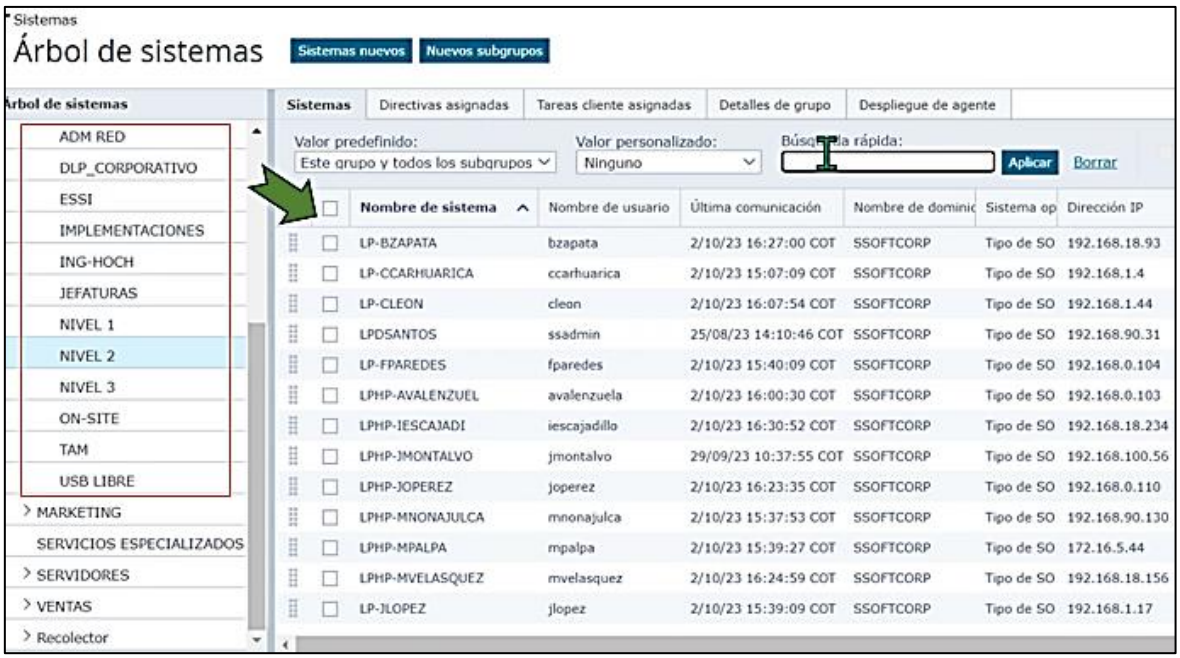


Figura 64. Subgrupos del grupo Ingeniería
Fuente: Elaboración propia

En la Figura 65 se puede observar la directiva que fue configurada previamente en la sección 3.2.4 la cual se aplicó a los equipos empresariales con el nombre de “ING-USB-BLOQUEO” además se cambió la definición de la gravedad de los eventos, la cual se les asigno una gravedad de “Crítica”.

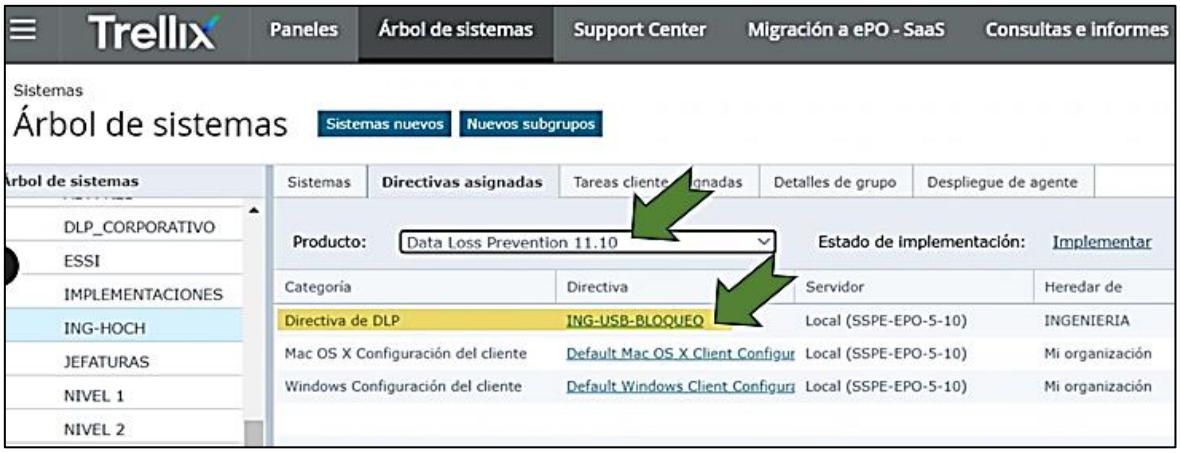


Figura 65. Directivas aplicadas a los equipos empresariales
Fuente: Elaboración propia

En la Figura 66 se puede visualizar que la directiva “ING-USB-BLOQUEO” fue aplicada a 190 equipos los cuales formaban parte de los equipos del área de ingeniería.

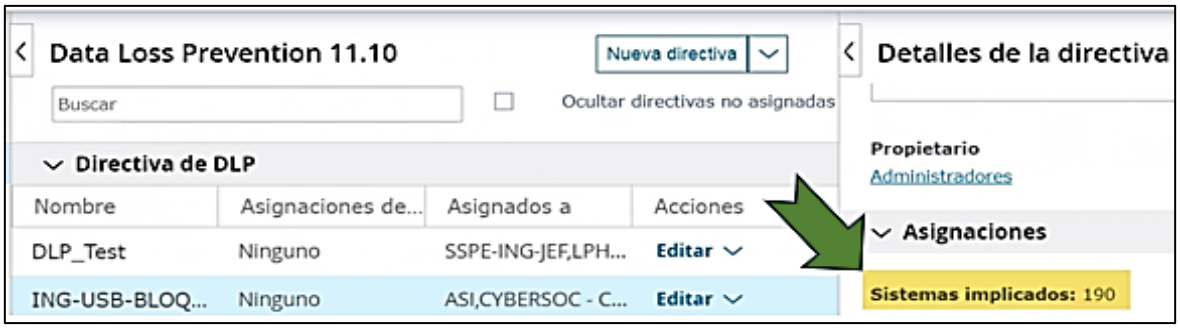


Figura 66. Equipos afectados por la directiva “ING-USB-BLOQUEO”
Fuente: Elaboración propia

En la Figura 67 se puede visualizar las reglas que fueron creadas y aplicadas a los 190 equipos, dichas reglas creadas corresponden al bloqueo de correo saliente, bloqueo de puertos USB y bloqueo de bluetooth.

Cabe rescatar que para el bloqueo de correos electrónicos saliente se crearon 2 reglas, las cuales tenían la misma configuración, pero con la diferencia que poseían diferente lista de dominios de correos a bloquear.

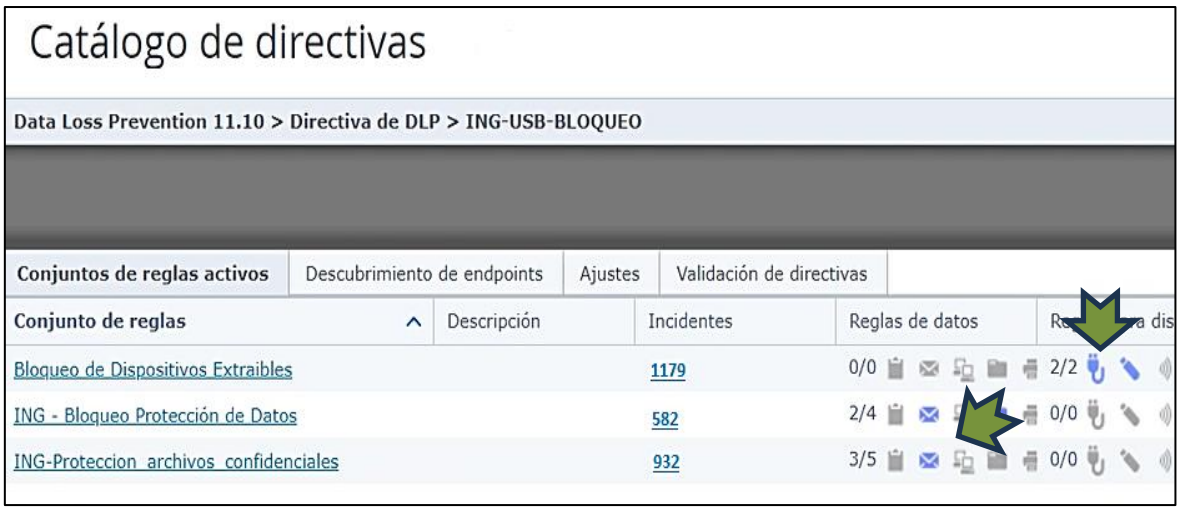


Figura 67. Conjunto de reglas que se están aplicando
Fuente: Elaboración propia

En la Figura 68 se puede visualizar dos de las 3 reglas de bloqueo que fueron creadas, las cuales corresponden al bloqueo de puertos USB y bloqueo de bluetooth.

A ambas de las reglas se les asigno una gravedad del tipo “Crítica”, dicha gravedad de los eventos se pudo hacer notoria al ver los registros en la consola que fueron presentados en la sesión de resultados del presente trabajo.

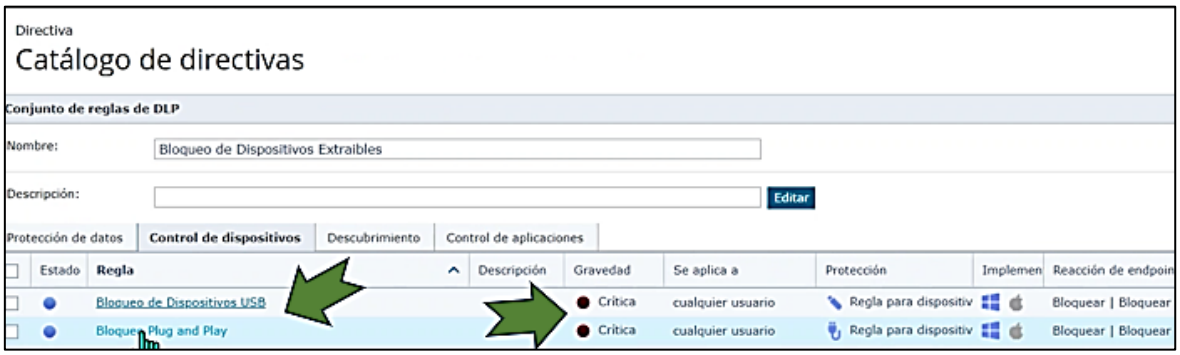


Figura 68. Reglas de bloqueo de USB y Bluetooth en equipos empresariales
Fuente: Elaboración propia

Se puede observar la configuración que se aplicó para el bloqueo de conexión Bluetooth a los equipos empresariales del grupo de INGENIERIA en la Figura 69 teniendo el estado de la regla como “Activada” y la gravedad de los eventos como “Crítica”.

Figura 69. Referencia de configuración de la regla de bloqueo bluetooth
Fuente: Elaboración propia

Se puede observar la configuración que se aplicó para el bloqueo de puertos USB a los equipos empresariales del grupo de INGENIERIA en la Figura 70 teniendo el estado de la regla como “Activada” y la gravedad de los eventos como “Crítica”.

Figura 70. Referencia de configuración de la regla de bloqueo USB
Fuente: Elaboración propia

Se puede observar la configuración que se aplicó para el bloqueo de correos salientes a los equipos empresariales del grupo de INGENIERIA en la Figura 71

teniendo el estado de la regla como “Activada” y la gravedad de los eventos como “Crítica”.

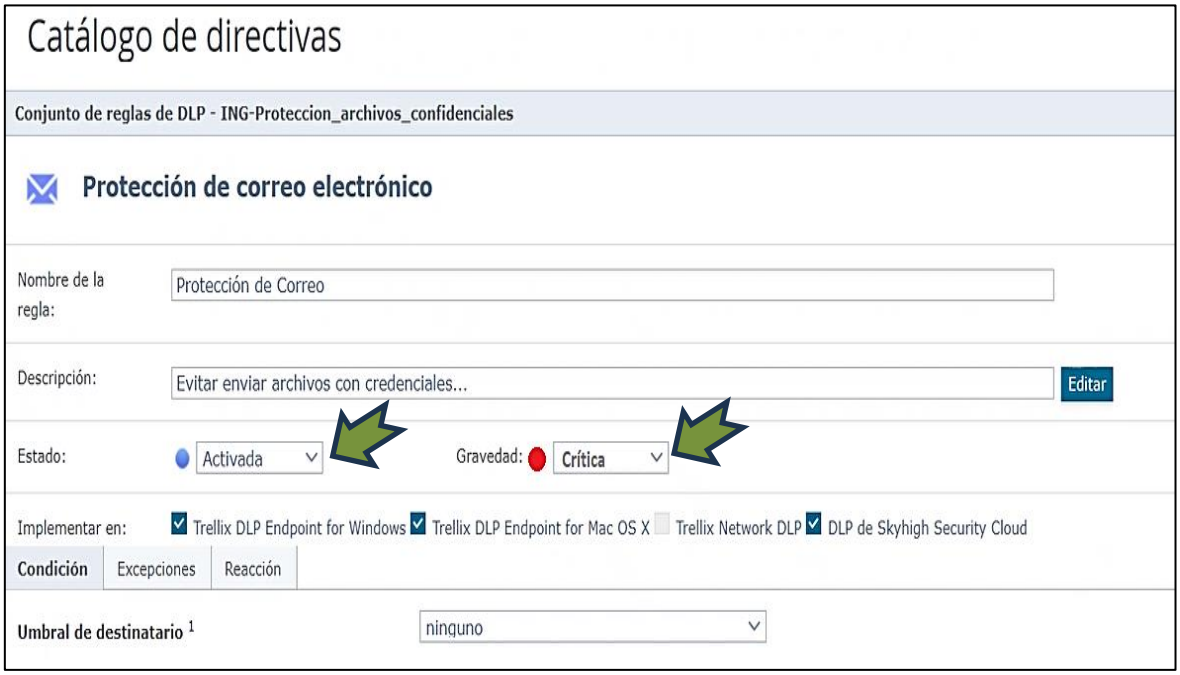


Figura 71. Configuración de la regla de bloqueo de correo saliente
Fuente: Elaboración propia

3.3 Resultados

3.3.1 Resultado de la conexión de la Máquina virtual a la consola ePO

En la Figura 72 se puede observar el registro de instalación del agente Trellix de forma satisfactoria, lo cual fue reflejado en la consola de administración ePO.

La consola ePO registro todos los equipos que lograron vincularse estando dentro de la red empresarial o estando conectados a través de una VPN.

En la captura también se puede apreciar que se desplego satisfactoriamente el producto DLP en el equipo de prueba lo cual se puede confirmar en la casilla de Versión de producto.

Cabe recordar que antes de proceder con la instalación en la máquina virtual de prueba, se realizó la validación de compatibilidad entre el agente y el sistema operativo tal como se indica en la Tabla 4, con lo cual al comprobar que eran compatibles recién se procedió con la instalación del agente y del producto en la máquina virtual.

Figura 72. Máquina virtual de prueba instalada y registrada en consola
Fuente: Elaboración propia

3.3.2 Resultados de las validaciones realizadas en el equipo de prueba

Luego de realizar la configuración y aplicación de las reglas DLP de bloqueo propuestas, se procedió a realizar las validaciones de funcionamiento de dichas reglas.

Se pudo corroborar su correcta aplicación y respuesta. Así mismo con dicho laboratorio realizado se pudo contemplar posibles mejoras a futuro para ser implementadas.

A) Resultados de la aplicación de la regla de bloqueo USB

Tal como se puede apreciar en la Figura 73, se procedió a conectar un dispositivo USB a fin de poder transferir un archivo desde la máquina virtual de pruebas a ese dispositivo, pero luego de realizar la conexión con la laptop se bloqueó el acceso del USB y nos generó el mensaje de alerta correspondiente.

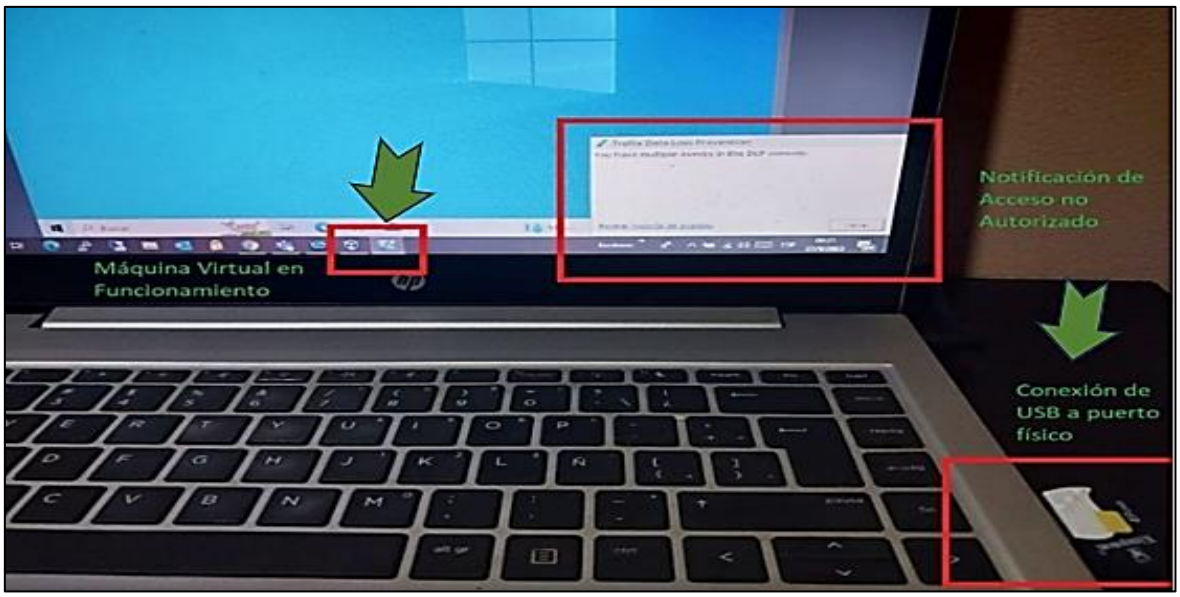


Figura 73. Bloqueo de dispositivos extraíbles en el equipo de prueba
Fuente: Elaboración propia

B) Resultados de la aplicación de la regla de bloqueo de correo

Tal como se puede observar en las Figuras 74 y 75, se generó un correo electrónico desde la máquina virtual de pruebas dirigido al dominio “gmail.com” el cual se encontraba agregado en la lista de dominios a bloquear, por esta razón al intentar enviar el correo de prueba se nos impidió el envío y se generó el mensaje de alerta.

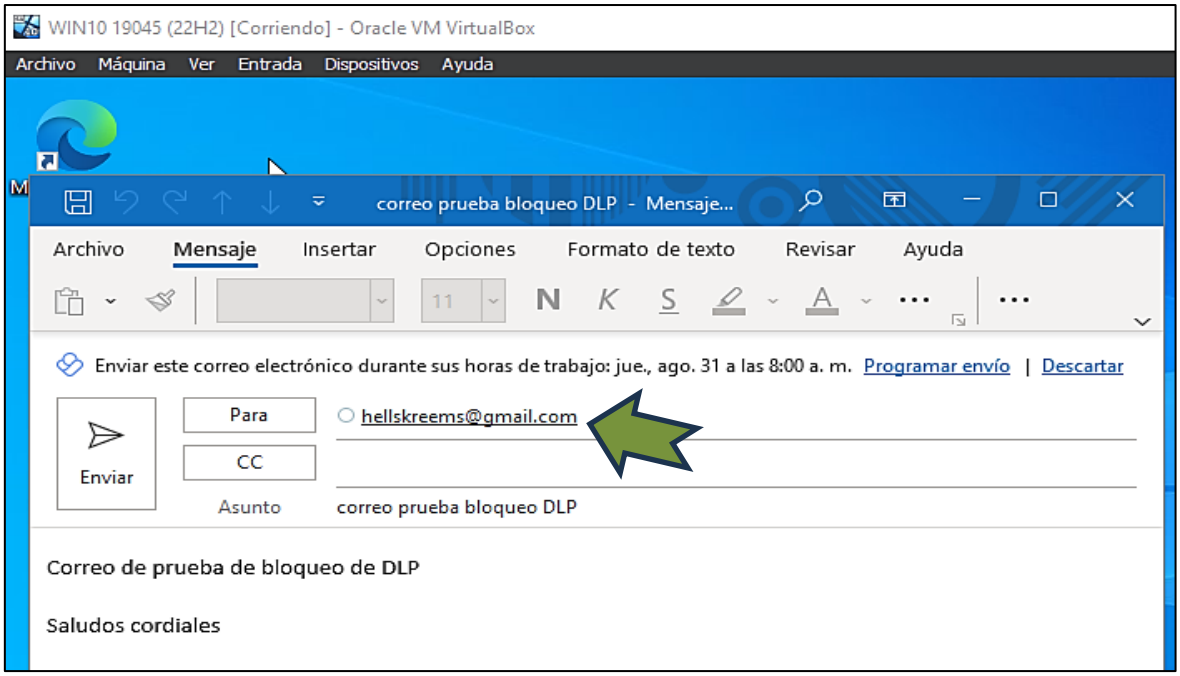


Figura 74. Correo de prueba generado en la máquina virtual
Fuente: Elaboración propia

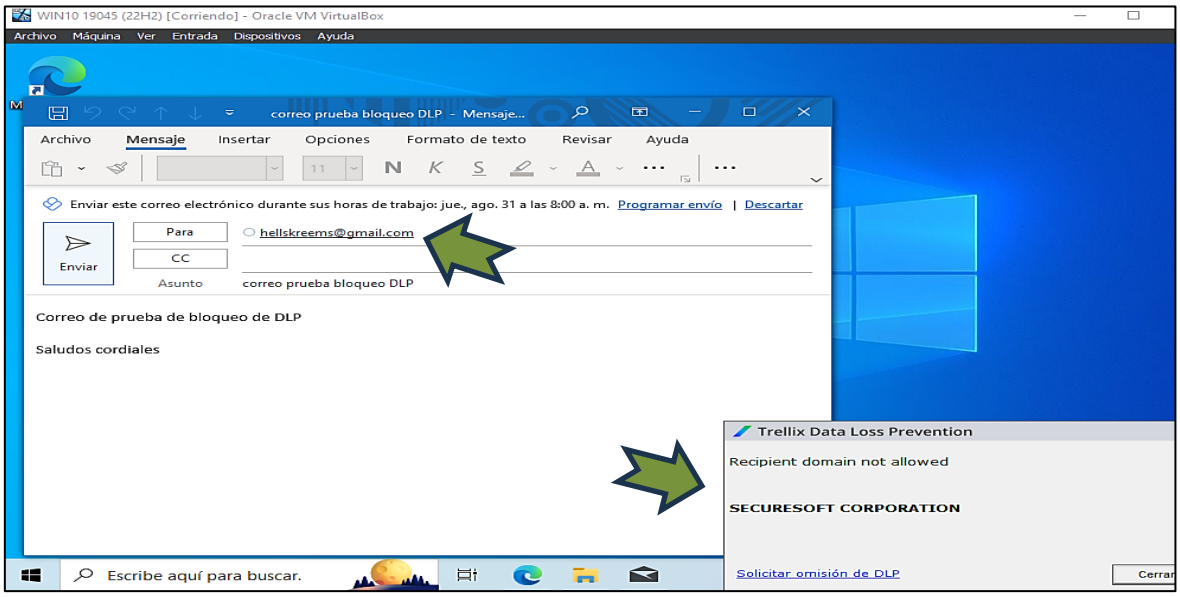


Figura 75. Mensaje de alerta al enviar el correo a dominio no permitido
Fuente: Elaboración propia

C) Resultados de la aplicación de la regla de bloqueo de Bluetooth

Luego de haber realizado la configuración de la regla de bloqueo Bluetooth y aplicar la directiva, se procedió a realizar pruebas de envío de información desde el celular hacia el equipo de prueba y viceversa, generándonos un mensaje de error al momento de realizar la transferencia tal como se puede observar en la Figura 76.

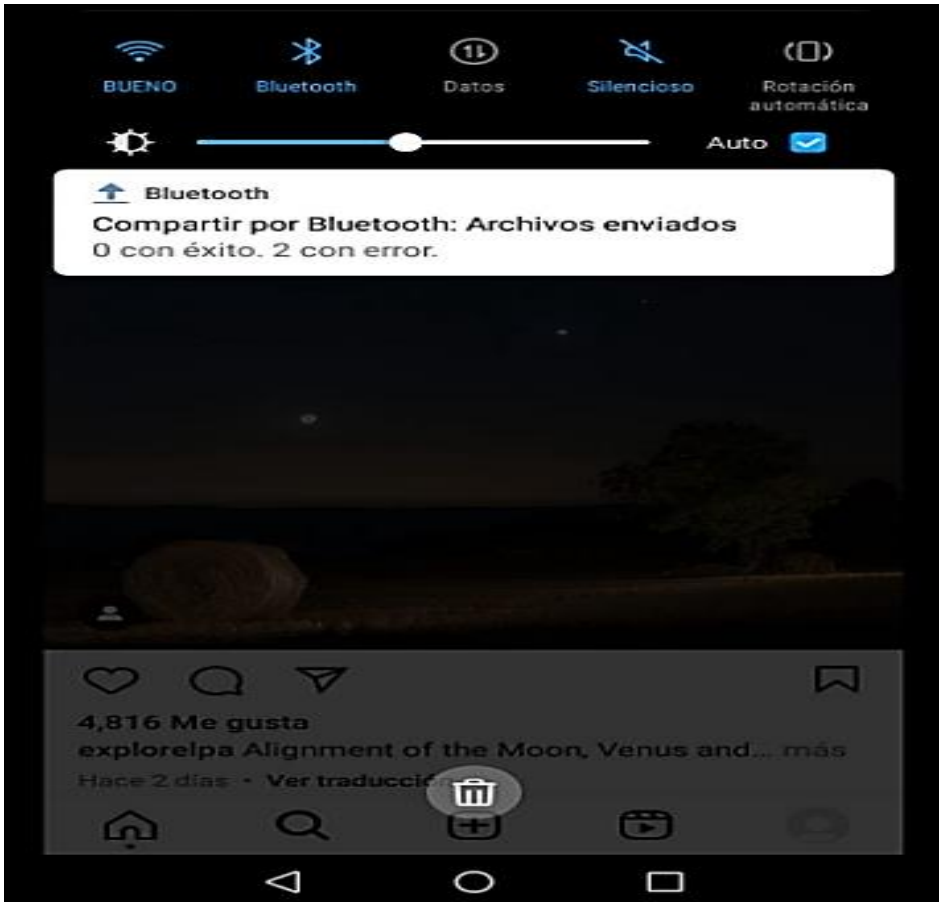


Figura 76. Mensaje de error al transferir archivos por Bluetooth
Fuente: Elaboración propia

3.3.3 Resultados de las reglas en los equipos empresariales

Existen 2 tipos de validaciones que se realizaron en los equipos empresariales:

- Validaciones en equipos que se encontraron fuera de la red de la empresa conectándose a través de una VPN.
- Validaciones en equipos que se encontraron conectados directamente a la red de las oficinas de Securesoft.

Cabe mencionar que las validaciones realizadas fueron exitosas, adicional a ello la implementación realizada a todo el parque de 190 equipos se culminó dentro del

plazo establecido mejorando la seguridad y cubriendo las posibles vulnerabilidades internas.

A) Validaciones en equipos fuera de la red de la empresa

Estas validaciones se realizaron directamente en mi propia laptop empresarial con nombre “JSUSANIBAR”, con ella se realizó las validaciones del funcionamiento de las reglas de bloqueo.

Tal como se puede visualizar en la Figura 77, se conectó un dispositivo de almacenamiento a la laptop por uno de sus puertos y como consecuencia la regla de bloqueo de puertos USB aplicada a todas las laptops del grupo de INGENIERIA genero el bloqueo de dicho dispositivo y nos notificó el intento de infracción.

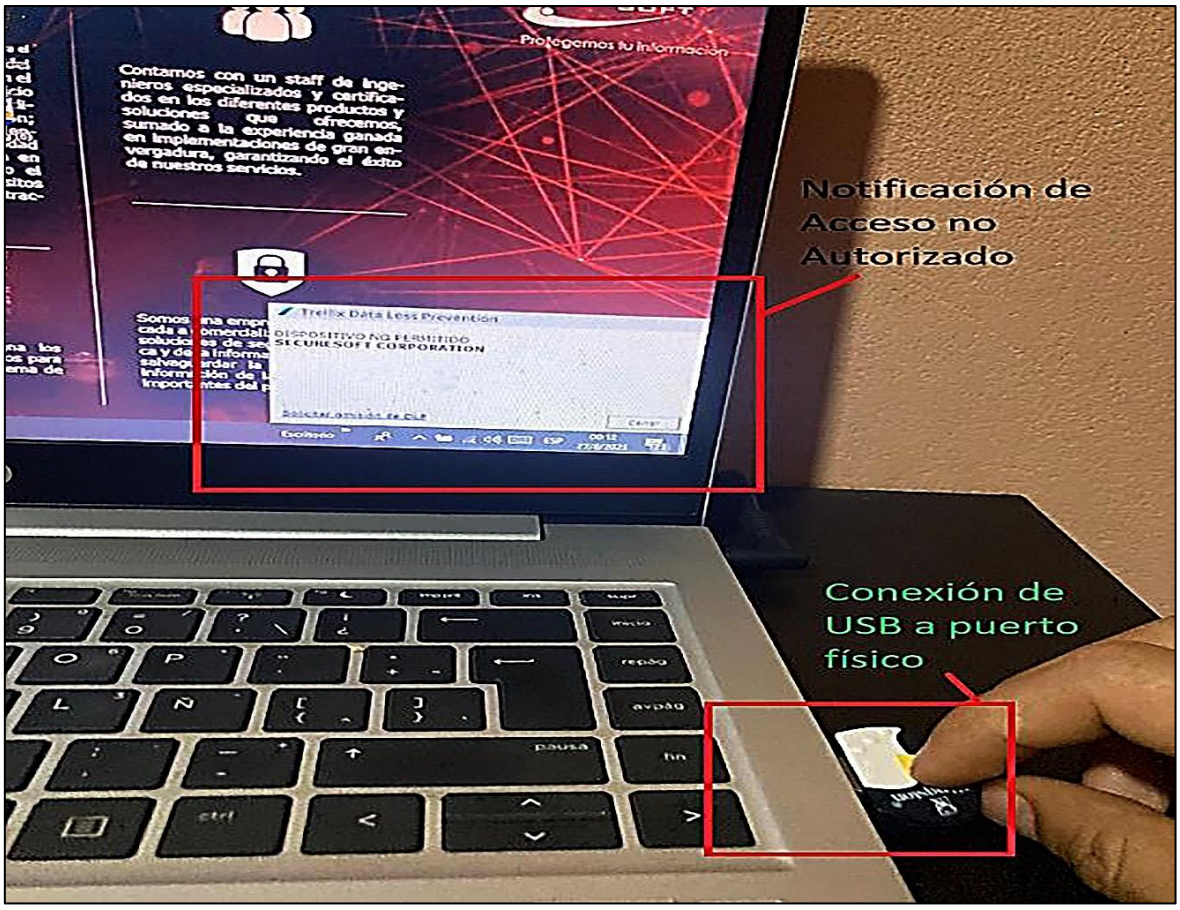


Figura 77. Resultado del bloqueo USB en equipos empresariales
Fuente: Elaboración propia

En la Figura 78 se puede visualizar que debido al bloqueo de acceso USB, el dispositivo de almacenamiento no fue reconocido por la laptop como una unidad extraíble conectada al equipo.

Cabe mencionar que el bloqueo de dispositivos extraíbles USB se aplica para cualquier modelo o marca de USB.

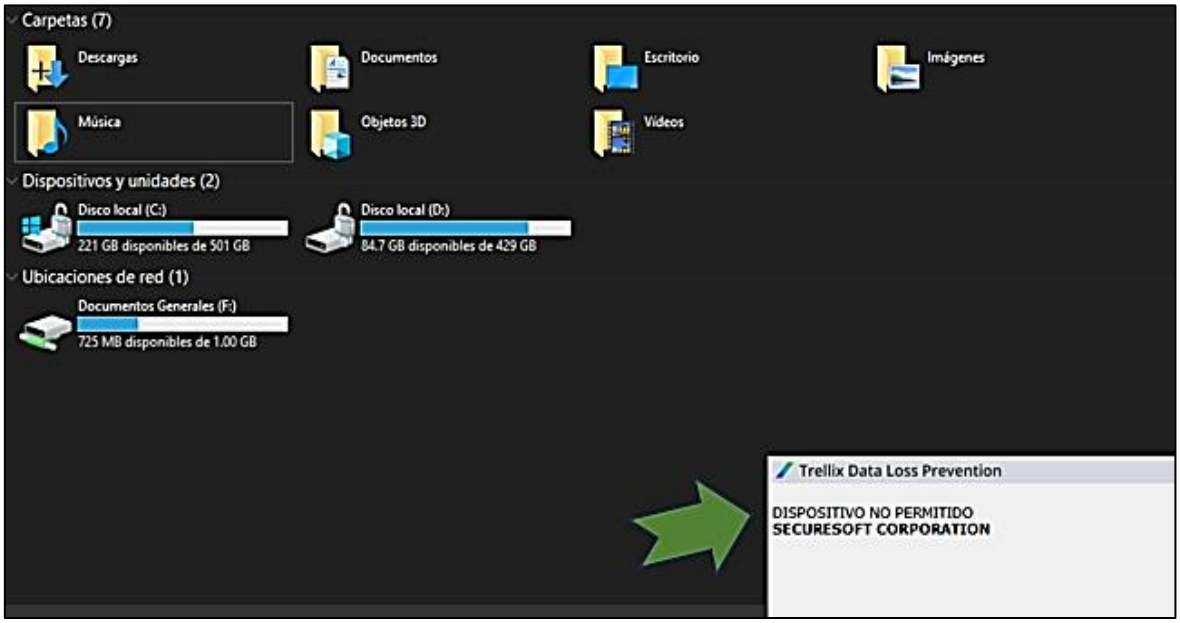


Figura 78. Dispositivo USB no registrado
Fuente: Elaboración propia

En las Figuras 79 y 80 se puede apreciar el correcto funcionamiento de la regla de bloqueo de correos salientes, se obstruyo el envío de un correo generado desde la laptop empresarial hacia un dominio no permitido y se generó una notificación de alerta ante dicha infracción.

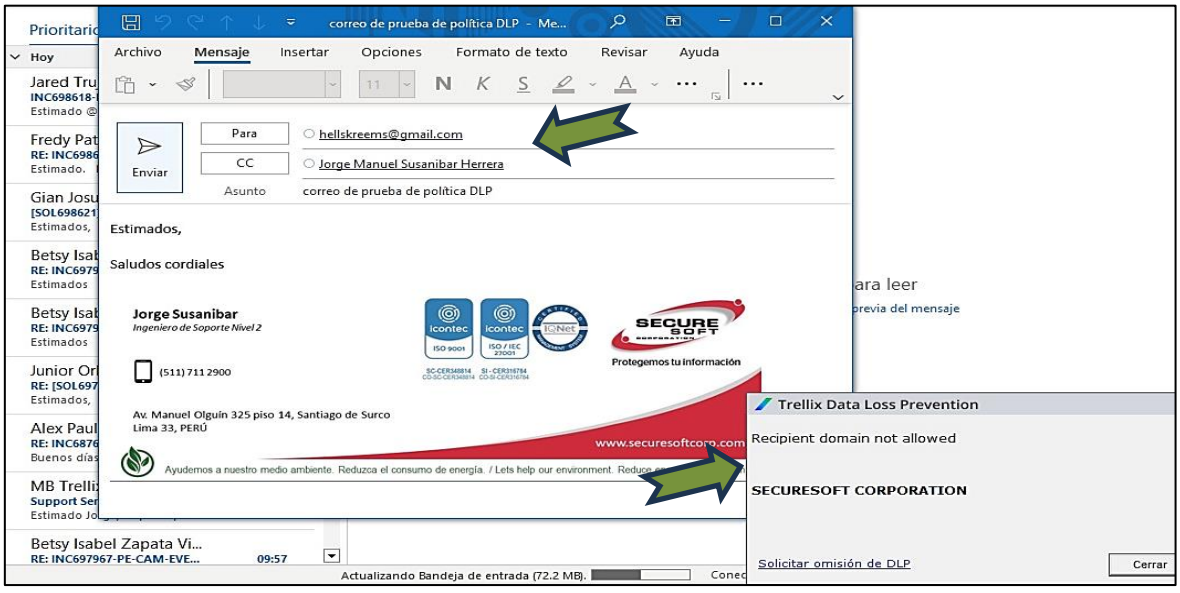


Figura 79. Resultado del bloqueo de correo en equipos empresariales
Fuente: Elaboración propia

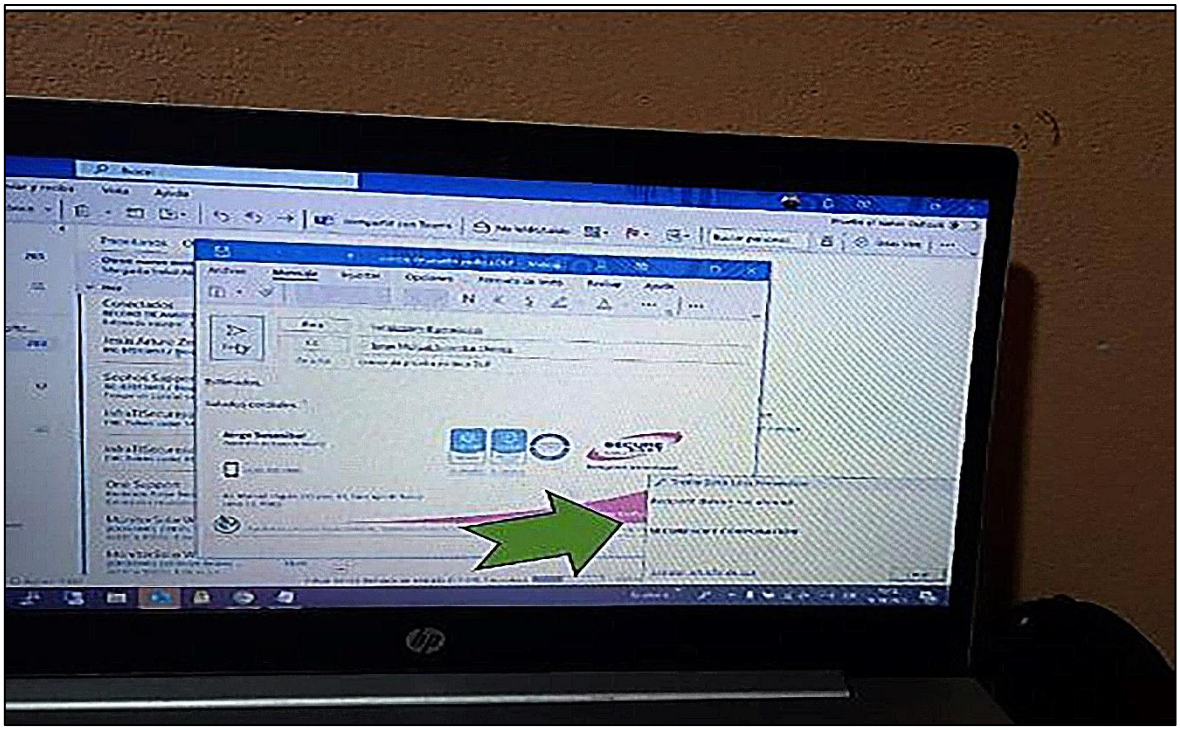


Figura 80. Bloqueo de correo en equipos empresariales, imagen sin ampliar
Fuente: Elaboración propia

B) Validaciones en equipos dentro de la red empresarial

Estas validaciones se realizaron directamente en las oficinas de la empresa Securesoft.

En la Figura 81 se puede visualizar una sección correspondiente al área de ingeniería.

Figura 81. Imagen del área de ingeniería
Fuente: Elaboración propia

En las Figuras 82, 83 y 84 se puede visualizar el momento en el cual se procedió a realizar las pruebas del bloqueo de dispositivos extraíbles (USB) en diferentes laptops pertenecientes al grupo de INGENIERIA, para ello se solicitó el apoyo de 2 ingenieros que se encontraron presentes.

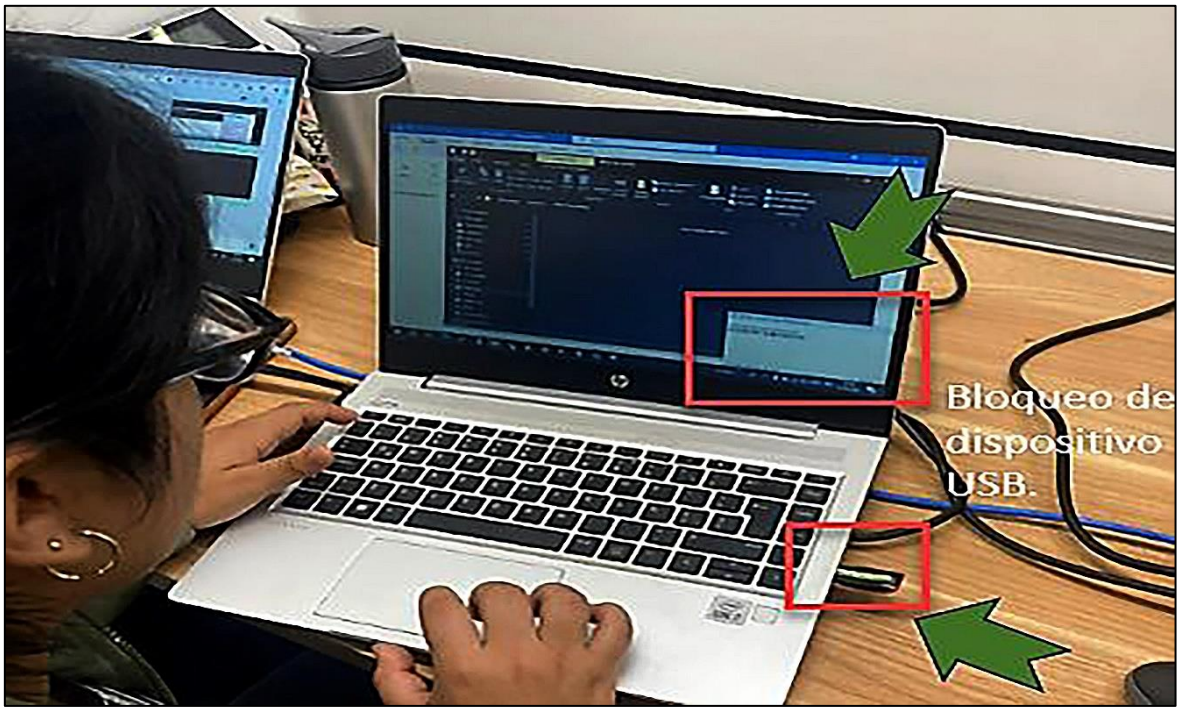


Figura 82. Bloqueo de USB en laptop 1 de la oficina
Fuente: Elaboración propia

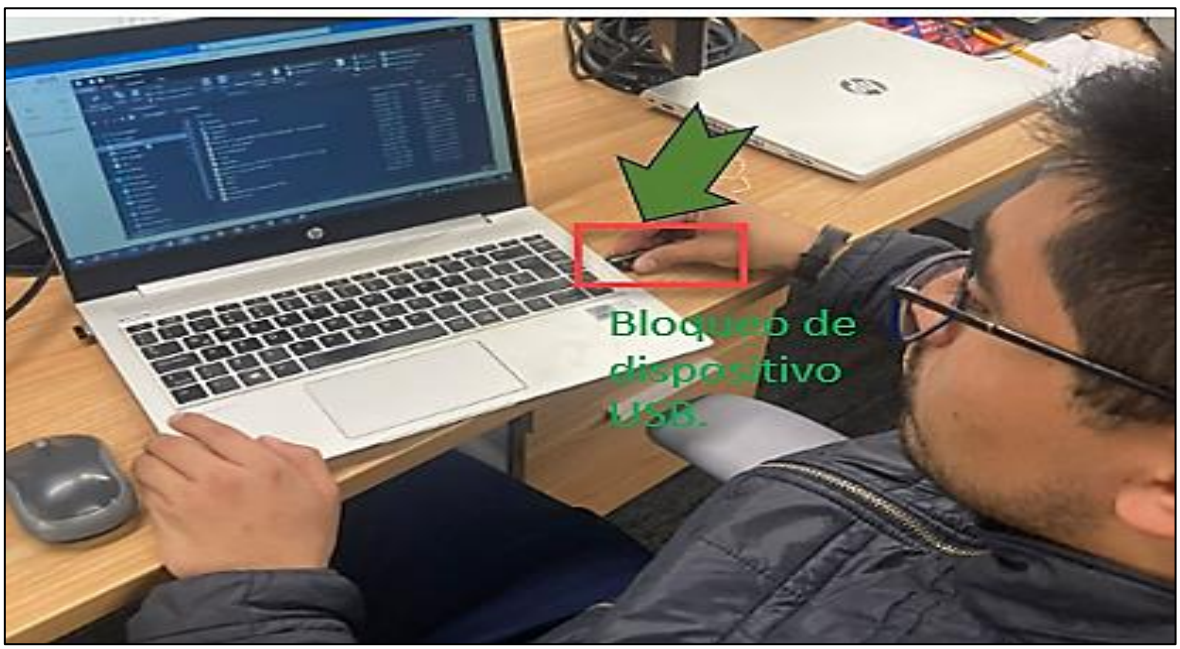


Figura 83. Bloqueo de USB en laptop 2 de la oficina
Fuente: Elaboración propia

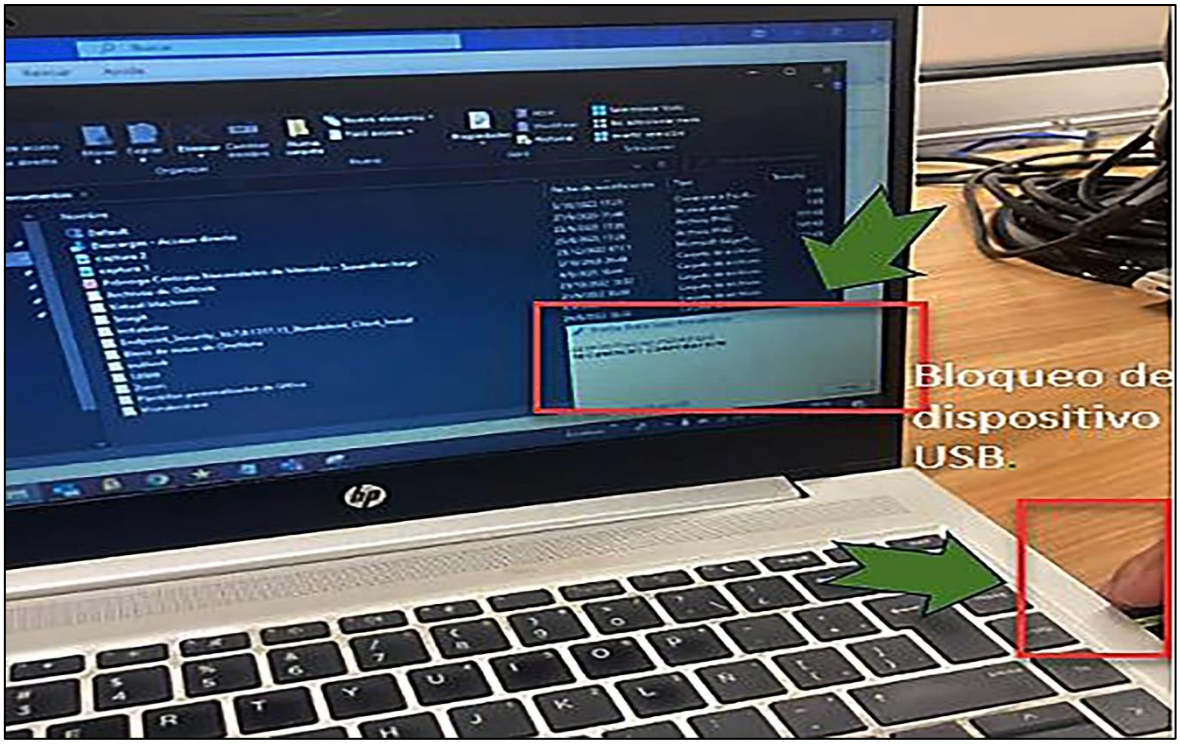


Figura 84. Bloqueo de USB en laptop 2 de la oficina, segunda captura
Fuente: Elaboración propia

En las Figuras 85, 86 y 87 se puede visualizar el momento en el cual se procedió a enviar un correo a un dominio no permitido en la regla de bloqueo, para dicha validación se solicitó ayuda de 3 ingenieros diferentes y sus respectivas laptops.

Figura 85. Bloqueo de correo en laptop 1 de la oficina
Fuente: Elaboración propia

Figura 86. Bloqueo de correo en laptop 2 de la oficina
Fuente: Elaboración propia

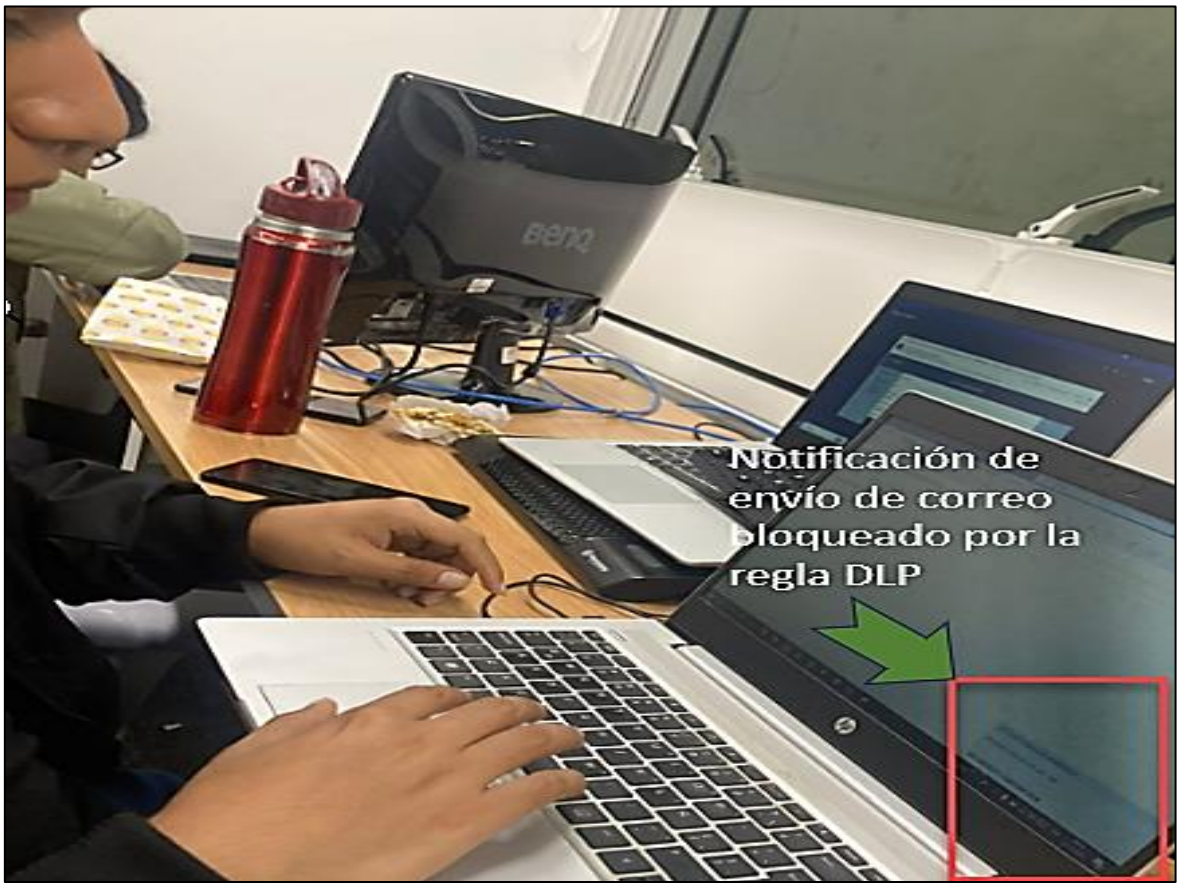


Figura 87. Bloqueo de correo en laptop 3 de la oficina
Fuente: Elaboración propia

En las Figuras 88, 89 y 90 se puede visualizar el momento en el cual se intentó transferir archivos desde el celular a la laptop sin éxito debido al bloqueo realizado por la regla DLP para el bloqueo bluetooth.

Para ello se solicitó ayuda de un ingeniero y su respectiva laptop y celular a fin de realizar la validación.

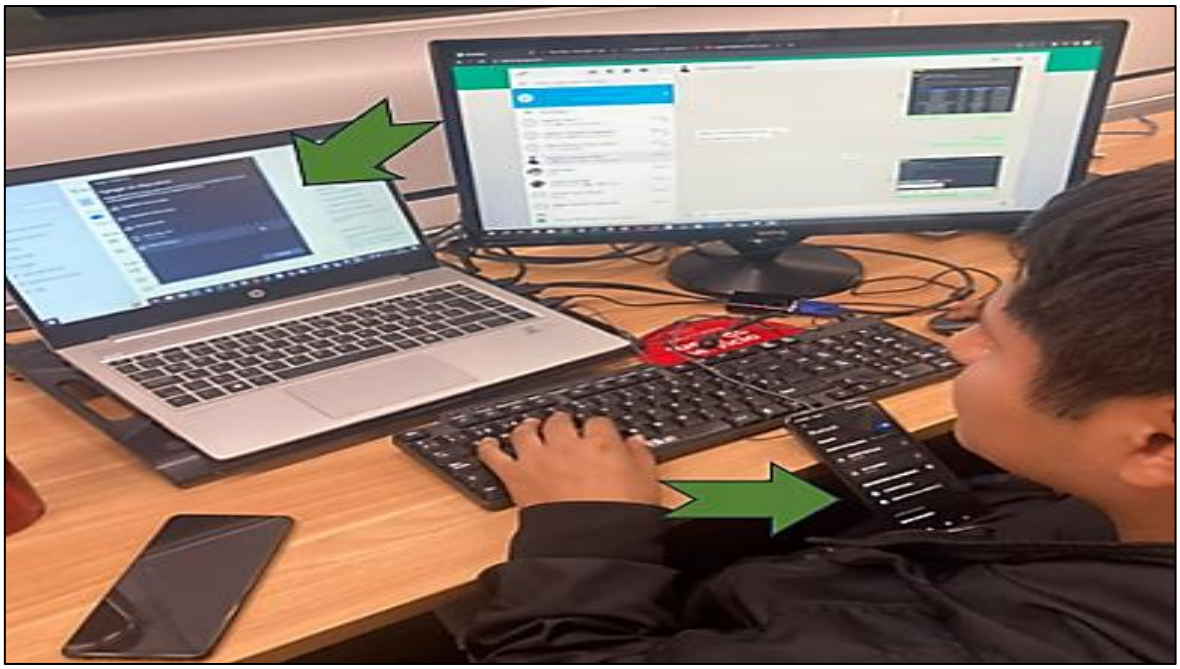


Figura 88. Vinculación de celular con la laptop por bluetooth
Fuente: Elaboración propia

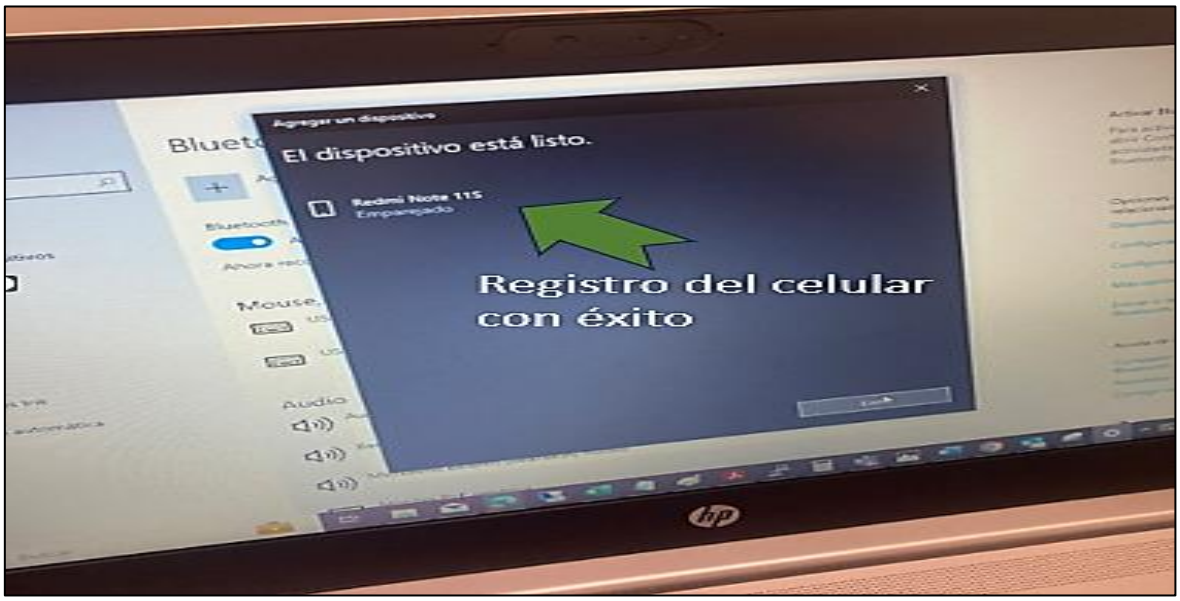


Figura 89. Vinculación de celular con laptop exitoso
Fuente: Elaboración propia

Figura 90. Envío de archivos de celular a laptop fallido
Fuente: Elaboración propia

Luego de realizar la implementación en los equipos empresariales se procedió a mantener un monitoreo de incidentes que se generaría en las laptops de todo el departamento de ingeniería luego de aplicarles las reglas de DLP.

Se registró al mes de octubre del presente Año, 2693 eventos de DLP que fueron notificados y solucionados según la configuración de las reglas realizadas.

Con lo cual podemos corroborar que al mes de octubre desde la culminación de la implementación de la directiva DLP, se pudo evitar 2693 posibles eventos de fuga de información y con ello se validó la eficiencia y la utilidad del trabajo propuesto.

En las Figuras 91 y 92 se puede visualizar el panel de administración de incidentes DLP en el cual se puede aprecias los incidentes detonados en los equipos

empresariales desde mediados del mes de Julio hasta finales del mes de octubre, así mismo se puede apreciar la gravedad del evento y la acción tomada por el DLP.

Podemos visualizar algunos eventos adicionales en el Anexo 3 y Anexo 4.

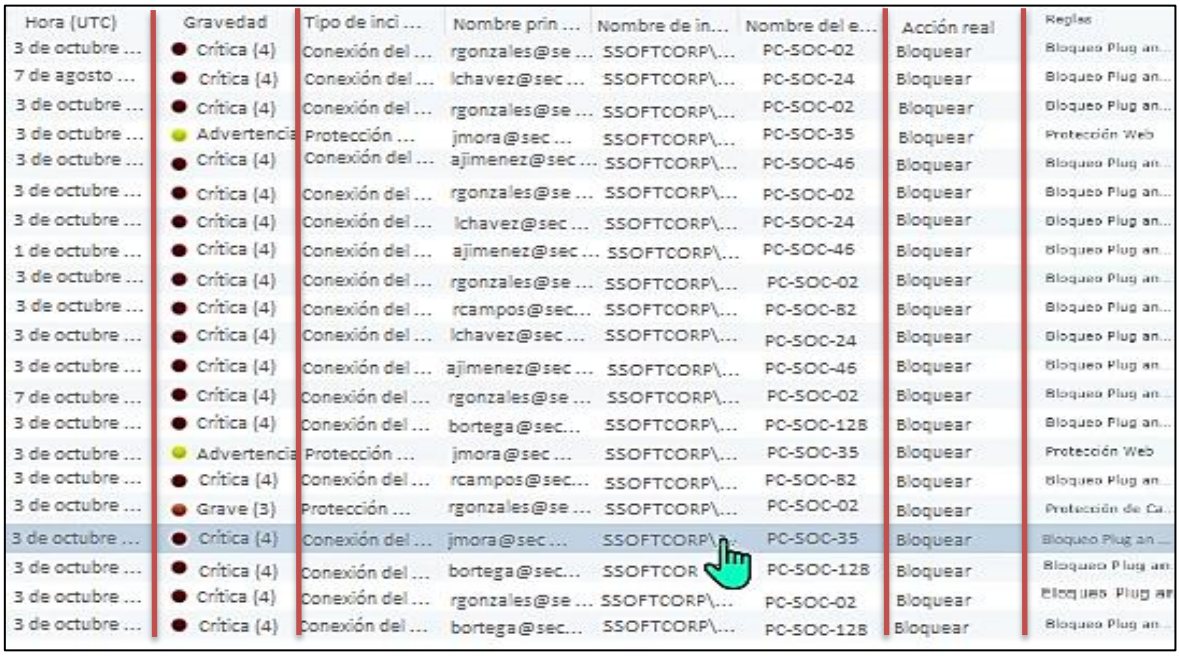


Figura 91. Ventana 1 de eventos registrados en la consola
Fuente: Elaboración propia

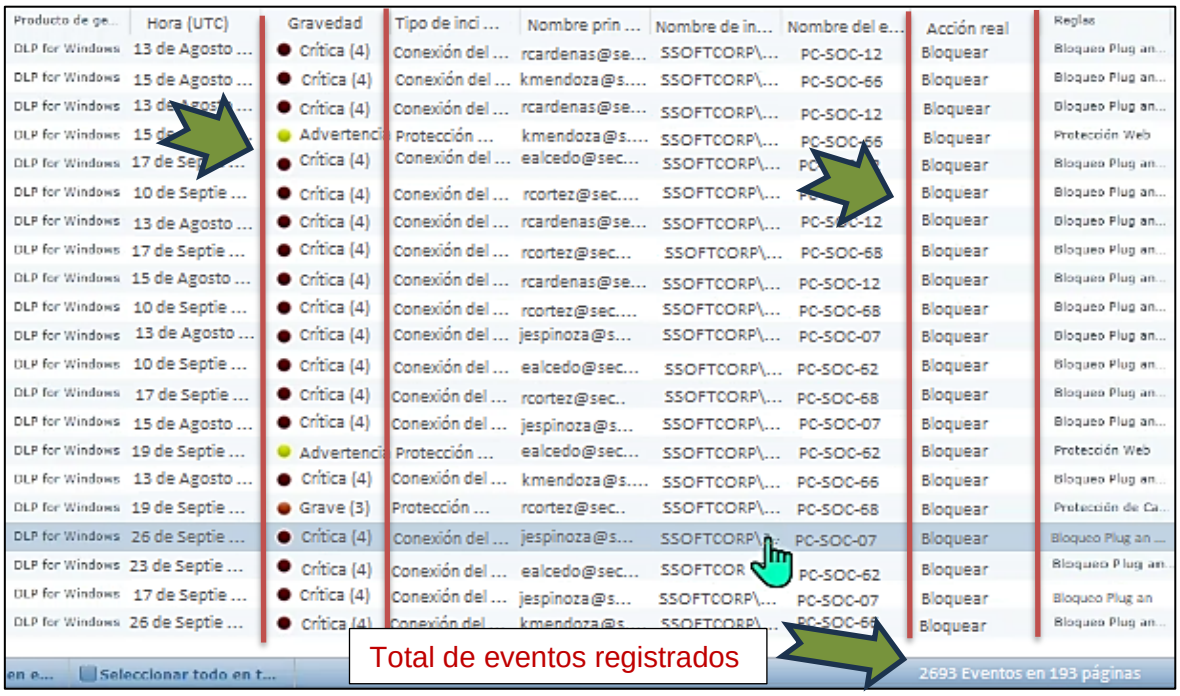


Figura 92. Ventana 2 de eventos registrados en la consola
Fuente: Elaboración propia

Del total de alertas podemos observar que se generó 1514 eventos correspondientes al bloqueo de correos electrónicos salientes, siendo este el tipo de alerta más generado. Adicional a ello se generaron alertas de bloqueo de dispositivos de almacenamiento extraíble con una cantidad de 828 eventos y alertas de bloqueo bluetooth con una cantidad de 351 eventos.

En las Figuras 93 y 94 podemos apreciar una representación de dichos valores.

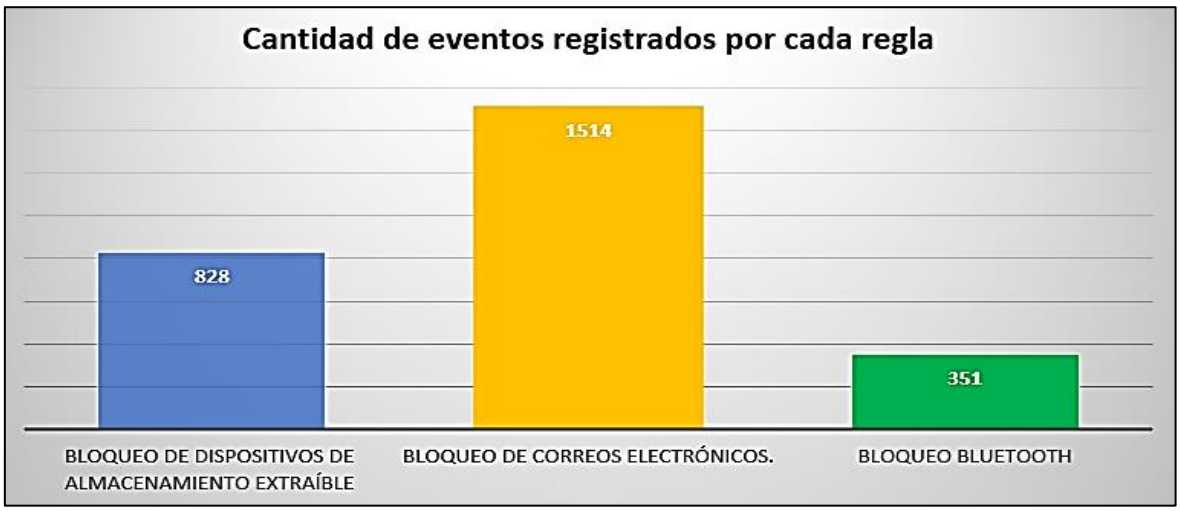


Figura 93. Eventos correspondientes a cada regla
Fuente: Elaboración propia

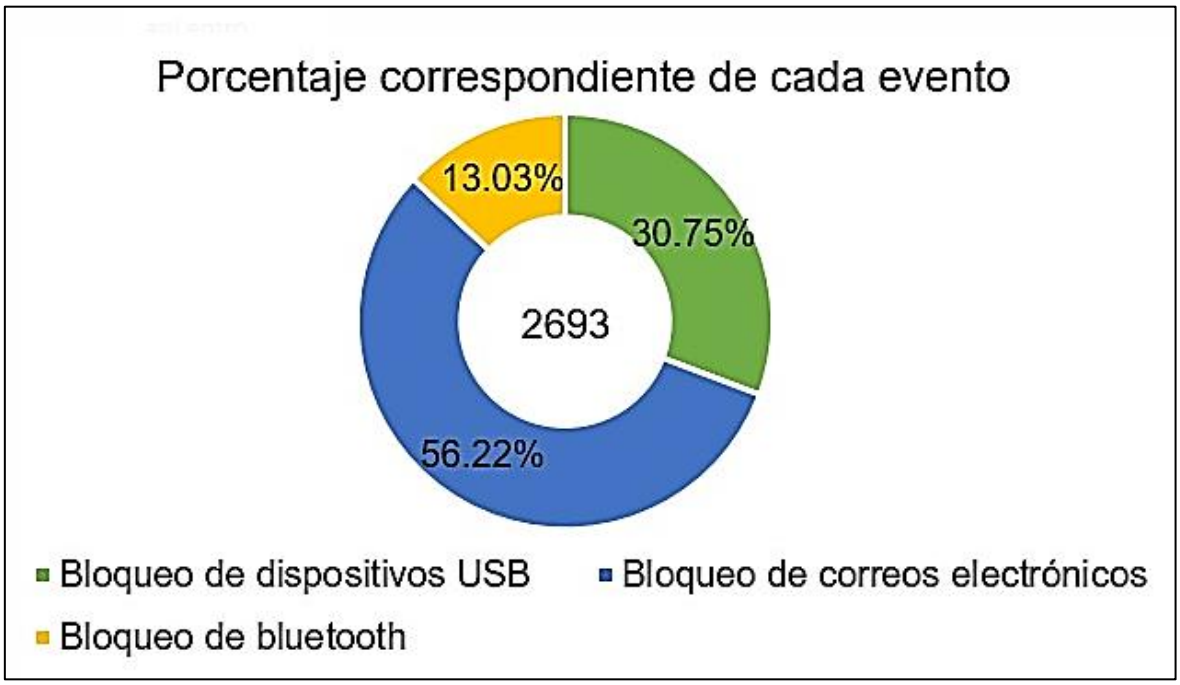


Figura 94. Porcentaje correspondiente a cada tipo de evento
Fuente: Elaboración propia

Previo a la aplicación de las reglas DLP, se evidenció 642 registros de posibles fugas de información captados en la consola de administración ePO, tal como se puede visualizar en la Figura 95.

Dichos eventos corresponden a un periodo de 8 días, realizando una proyección se pudo estimar que sin la presencia del DLP para los 45 días en los cuales se aplicó el monitoreo se tendría un registro de 3611 eventos.

Cabe indicar que luego de culminado la implementación, durante el monitoreo se evidenció 2693 eventos durante el periodo de 45 días tal como se pudo apreciar en la Figura 92, con lo cual se vio una reducción del 25.42% del total de ataques de seguridad proyectados gracias a la presencia de las reglas DLP. Cabe indicar que los incidentes registrados durante el periodo de monitoreo fueron bloqueados.

Hora (UT...	G...	Tipo de ...	Nombre princi...	N...	Nombre...
6 de Abril del 202...	..	Conexión ...	jsalazar@secure...	SSO...	PC-SOC-01
6 de Abril del 202...	..	Conexión ...	adiaz@securesof...	SSO...	PC-SOC-02
7 de Abril del 202...	..	Conexión ...	pgonzales@secu...	SSO...	PC-SOC-24
7 de Abril del 202...	..	Conexión ...	jsaturio@secure...	SSO...	PC-SOC-35
8 de Abril del 202...	..	Conexión ...	yelias@secureso...	SSO...	PC-SOC-58
9 de Abril del 202...	..	Conexión ...	jsaturio@secure...	SSO...	PC-SOC-35
10 de Abril del 202.	..	Conexión ...	pgonzales@secu...	SSO...	PC-SOC-24
11 de Abril del 202.	..	Conexión ...	yelias@secureso...	SSO...	PC-SOC-58
12 de Abril del 202.	..	Conexión ...	jsalazar@secure...	SSO...	PC-SOC-01
12 de Abril del 202.	..	Conexión ...	adiaz@securesof...	SSO...	PC-SOC-02
13 de Abril del 202	..	Conexión ...	jsaturio@secure...	SSO...	PC-SOC-35

Seleccionar todo en t... 642 Eventos

Figura 95. Eventos previos a la culminación de la implementación
Fuente: Elaboración propia

Respecto al costo de la implementación del proyecto, se aplicó un valor de 50 dólares por hora invertida para realizar la configuración, despliegue y validación de las políticas DLP, así mismo el costo de la licencia del módulo para 600 equipos (licencia estándar) tuvo un valor de 2000 dólares dándonos un total de 4900 dólares el valor del proyecto.

El costo a detalle del proyecto lo podemos visualizar en la Tabla 5.

Tabla 5
Costo de la implementación

Costos de la implementación				
Ítems	Horas invertidas	Precio por hora	Costo en dólares	Proyección en soles
Configuración del módulo	3	$ 50.00	$ 150.00	S/ 559.50
Configuración de reglas	35	$ 50.00	$ 1,750.00	S/ 6,527.50
Validación y afinaciones	20	$ 50.00	$ 1,000.00	S/ 3,730.00
Licencia del módulo DLP			S/ 2,000.00	S/ 7,460.00
Total			S/ 4,900.00	S/ 18,277.00

Fuente: Elaboración propia

CONCLUSIONES

- Luego de realizar el análisis de la topología de la red de la empresa se pudo determinar las áreas en las cuales se iba a implementar las reglas DLP, con lo cual se pudo realizar el diseño y configuración de las reglas necesarias para los puntos finales a implementar.
- Se pudo realizar la implementación de las reglas de bloqueo DLP en los equipos virtuales según las especificaciones deseadas para el área de ingeniería.
- Durante el periodo de implementación en los equipos empresariales, se pudo validar que se contó con una licencia permanente para el módulo DLP, lo cual represento una gran ventaja debido a que no será necesario una renovación semestral o anual al igual que otras plataformas DLP que se encuentran en el mercado.
- Después de culminar con éxito la fase de prueba en las máquinas virtuales, se procedió con la implementación de las reglas en los equipos empresariales del grupo de Ingeniería compuestos por equipos que se encuentran en la oficina y equipos que se encuentran fuera de oficina trabajando al remoto.
- Se corroboró el correcto funcionamiento de las reglas implementadas en los 190 equipos correspondientes al área de ingeniería, así mismo durante el monitoreo posterior a la implementación se pudo confirmar el registro de las incidencias por parte de los puntos finales en la consola ePO Trellix.
- Se pudo observar que durante el monitoreo que se realizó entre los meses de julio a octubre se registró un total de 2693 alertas de los cuales 1514 fueron por bloqueo de correos electrónicos y 1179 por bloqueo de puertos extraíbles (USB) y bluetooth. De acuerdo con estos resultados, se puede concluir que las reglas de DLP desplegadas a los puntos finales funcionan correctamente bloqueando cualquier tipo de fuga de información.
- Como toda empresa está compuesta de diferentes áreas y tienen funciones distintas se concluye que las reglas de DLP no se pueden aplicar de forma uniforme a todas las áreas sin tener en claro cuáles son las necesidades que requieren para cumplir con sus funciones diarias.

RECOMENDACIONES

- De acuerdo con lo visto durante el proceso de implementación de Trellix a los equipos de Ingeniería, se recomienda usar el Sistema Trellix ePO Cloud ya que facilitaría la conexión de los equipos de los usuarios a la consola debido a que solo tendrían que tener acceso a internet hacia la URL de la consola.
- Se recomienda migrar a ePO Cloud debido a que el procedo de descarga del agente en ese tipo de solución es automática y mediante una tarea programada, se podría mantener actualizado el sistema de prevención de fuga de datos DLP sin intervención de una persona que lo realice.
- Monitorear de forma constante la consola de Trellix ya que es allí donde se registran los eventos de seguridad y de esta forma podemos brindar una respuesta rápida ante algún incidente que necesite de revisión inmediata.
- Se recomienda siempre mantener actualizado el agente Trellix en la consola ePO ya que de este modo se pueda desplegar el agente a los usuarios finales sin inconveniente.
- Mantener actualizado el DLP que se encuentra desplegado en los usuarios finales a fin de tener las ultimas actualizaciones por parte de marca.
- Se recomienda tener sesiones de concientización con el personal de las diferentes áreas a fin de generar una cultura de prevención frente a posibles ataques internos y externos de Data Loss Prevention (DLP) y de este modo reducir paulatinamente la cantidad de incidentes reportados en la consola ePO correspondiente al módulo DLP.
- Antes de realizar cualquier tipo de instalación del agente Trellix se recomienda verificar la compatibilidad con el Sistema Operativo de acuerdo con la página Oficial de Trellix Supports a fin de evitar futuros inconvenientes de comunicación entre agente y servidor o incidentes de alto consumo de recursos.
- Se recomienda revisar el cuadrante mágico de Gartner que sirve como referencia a tomar al momento de escoger el sofware DLP que más se ajusta a las necesidades del cliente.
- Se recomienda implementar reglas DLP de forma personalizada para los diferentes grupos de la empresa teniendo en cuenta sus necesidades.

REFERENCIAS BIBLIOGRÁFICAS

Asurza Cáceres, J. D. (2022). Diseño de una arquitectura de seguridad informática para incrementar la seguridad de información en la empresa Bafing S.A.C. en 2021 [Tesis de Grado, Universidad Científica del Sur]. Repositorio Académico -Universidad Científica del Sur. https://repositorio.cientifica.edu.pe/handle/20.500.12805/2414

Azurín, A. (2023, septiembre 7). Datos personales: Nuevo proyecto de reglamento sobre uso de información de clientes. Gestión. https://gestion.pe/economia/datos-personales-nuevo-proyecto-de-reglamento-sobre-uso-de-informacion-de-clientes-minjus-noticia/

Baca Urbina, G. (2016). Introducción a la seguridad informática. Grupo editorial Patria. https://www.academia.edu/40572652/Introduccion_a_la_seguridad_informatica_LIBRO

Cano Mora, J. (2013). Inseguridad de la información, una visión estratégica. Alfaomega.

Clementelli, C. (2023). Modern Data Loss Prevention (DLP). dummies. https://www.netskope.com/resources/ebooks/modern-data-loss-prevention-dlp-for-dummies

Diogenes, Y., & Ozkaya, E. (2018). Cybersecurity-attack and defense strategies. Packt.https://digtvbg.com/files/books-for-hacking/Cybersecurity%20%E2%80%93%20Attack%20and%20Defense%20Strategies%20-%20Infrastructure%20security%20with%20Red%20Team%20and%20Blue%20Team%20Tactics%20by%20Erdal%20Ozkaya%20and%20Yuri%20Diogenes.pdf

eBIZ Latin America. (2022, abril 4). Perú está entre los países con más incidentes de seguridad del continente. eBIZ Noticias. https://noticias.ebiz.pe/peru-esta-entre-los-paises-con-mas-incidentes-de-seguridad-del-continente/

Gartner. (s/f). Data loss prevention reviews and ratings. Gartner. Recuperado el 30 de septiembre de 2023, de https://www.gartner.com/market/data-loss-prevention

Gestión. (2020). Ciberseguridad en el Perú: ¿Qué tan preparados estamos para enfrentar la ciberdelincuencia?[Imagen]. NOTICIAS GESTIÓN. https://gestion.pe/publirreportaje/ciberseguridad-en-el-peru-que-tan-preparados-estamos-para-enfrentar-la-ciberdelincuencia-noticia/

Gestión. (2017, noviembre 7). Ciberespías tienen en la mira a países de América Latina, como Perú y Asia. Gestión; NOTICIAS GESTIÓN. https://gestion.pe/tendencias/ciberespias-mira-paises-america-latina-peru-asia-1-149899-noticia/

Godínez Chávez, A. D., & Olvera Espinoza, I. (2017). Implementación de un sistema de seguridad DLP (Data Loss Prevention) [Tesis de Grado, Universidad Nacional Autónoma de Mexico]. Repositorio Institucional de la UNAM. https://ru.dgb.unam.mx/handle/20.500.14330/TES01000756317

Instituto Nacional de Ciberseguridad. (2020, mayo 28). Evitando Fuga Informacion Sci. https://www.incibe.es/incibe-cert/blog/evitando-fuga-informacion-sci

ISO. (s/f). Estándares. ISO. Recuperado el 28 de septiembre de 2023, de https://www.iso.org/standards.html

Kaspersky. (s/f). Ciberamenaza Mapa en tiempo real. Ciberamenaza Mapa en tiempo real. Recuperado el 22 de septiembre de 2023, de https://cybermap.kaspersky.com/es/stats

Kiser, Q. (2020). Ciberseguridad: Una Simple Guía para Principiantes sobre Ciberseguridad, Redes Informáticas y Cómo Protegerse del Hacking en Forma de Phishing, Malware, Ransomware e Ingeniería Social. Independently published.

Lagua Gavilanes, A. S. (2021). Herramientas data loss prevention (dlp) opensource, para la seguridad de la información [Tesis de Maestria, Pontificia Universidad Católica del Ecuador]. Repositorio PUCESA. https://repositorio.pucesa.edu.ec/handle/123456789/3121

Ley N.° 30171. Ley de delitos informáticos, (2014, marzo 10). https://www.leyes.congreso.gob.pe/Documentos/Leyes/30171.pdf

Medrano Marin, H. (2022, mayo 20). Fuga de información en entidades públicas: Filtran y ofertan por Internet los datos personales de peruanos. El Comercio. https://elcomercio.pe/lima/sucesos/fuga-de-informacion-en-entidades-publicas-filtran-y-ofertan-por-internet-los-datos-personales-de-peruanos-asbanc-reniec-sunarp-noticia/?ref=ecr

Organización Internacional de Normalización [ISO]. (2018). Tecnología de la información—Técnicas de seguridad—Sistemas de gestión de seguridad de la información—Descripción general y vocabulario (ISO 27000). https://www.iso.org/standard/73906.html

Organización Internacional de Normalización [ISO]. (2022a). Seguridad de la información, ciberseguridad y protección de la privacidad: Controles de seguridad de la información (27002). https://www.iso.org/standard/75652.html

Organización Internacional de Normalización [ISO]. (2022b). Seguridad de la información, ciberseguridad y protección de la privacidad. Sistemas de gestión de seguridad de la información. Requisitos (ISO 27001). https://www.iso.org/standard/27001

Romero Castro, M. I., Figueroa Morán, G. L., Vera Navarrete, D. S., Álava Cruzatty, J. E., Parrales Anzúles, G. R., Álava Mero, C. J., Murillo Quimiz, Á. L., & Castillo Merino, M. A. (2018). Introducción a la seguridad informática y el análisis de vulnerabilidades. 3Ciencias.

Salinas Tomapasca, A. P. (2020). Modelo de ciberseguridad para cajas municipales en tiempo de transformacion digital—Un nuevo enfoque [Tesis de Maestria, Universidad Privada del Norte]. Repositorio Institucional UPN. https://repositorio.upn.edu.pe/handle/11537/29733

Samaniego Mena, E., & Ponce Ordóñez, J. (2021). Libro Fundamentos de seguridad informática. Compás. https://www.researchgate.net/publication/354054517_Libro_Fundamentos_de_seguridad_informatica

Trellix. (2017, diciembre 12). Cómo funciona McAfee Agent. Trellix. https://docs.trellix.com/es-ES/bundle/agent-5.5.0-product-guide-epolicy-orchestrator-cloud/page/GUID-BC52A070-B597-45A7-A004-A166ACE740CE.html

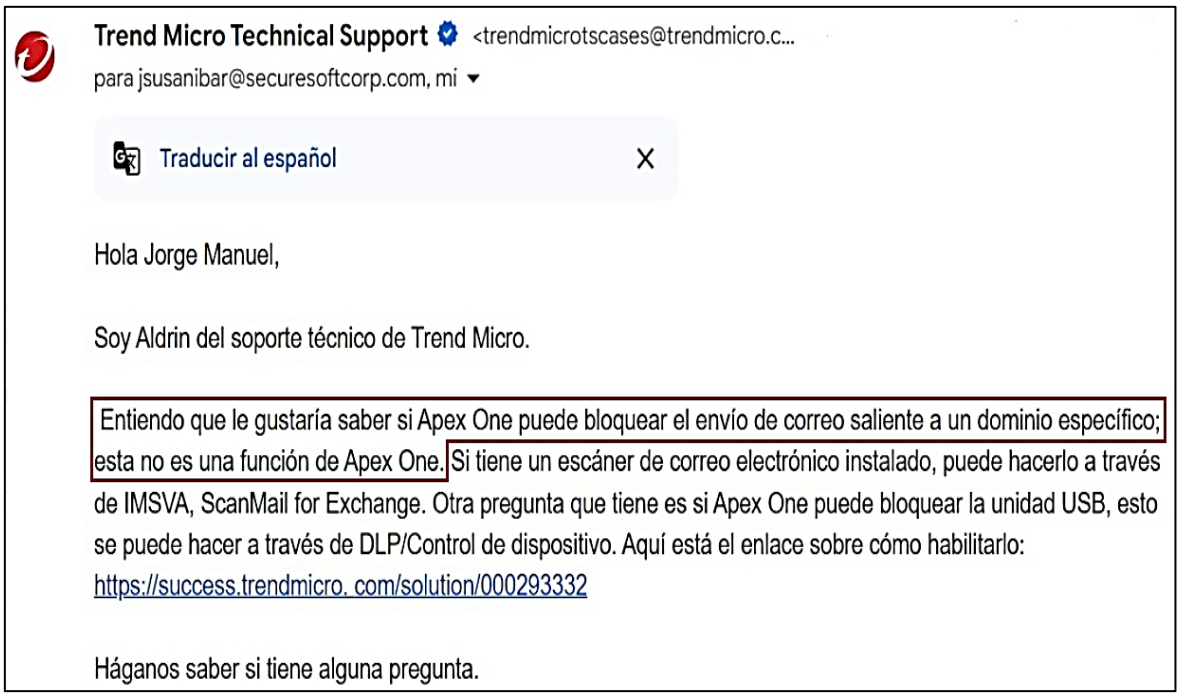
Trellix. (2022, noviembre 28). Cómo funcionan los controladores de agentes. Trellix. https://docs.trellix.com/es-ES/bundle/trellix-epolicy-orchestrator-on-prem-5.10.0-product-guide/page/GUID-7D32F2F1-1DF7-4A17-B57A-6F77F5BDE443.html

Vaca Escobar, P. N. (2019). Modelo de Gestión de seguridad lógica de la información en la protección de los datos sensibles de los distritos de

educación del Ecuador. [Tesis de Maestria, Universidad Técnica de Ambato]. Repositorio Universidad Técnica de Ambato. https://repositorio.uta.edu.ec/handle/123456789/30565

ANEXOS

Anexo 1. Consulta de funcionalidad de Trend Micro



Trend Micro Technical Support <trendmicrotscases@trendmicro.c...
para jsusanibar@securesoftcorp.com, mi

Traducir al español

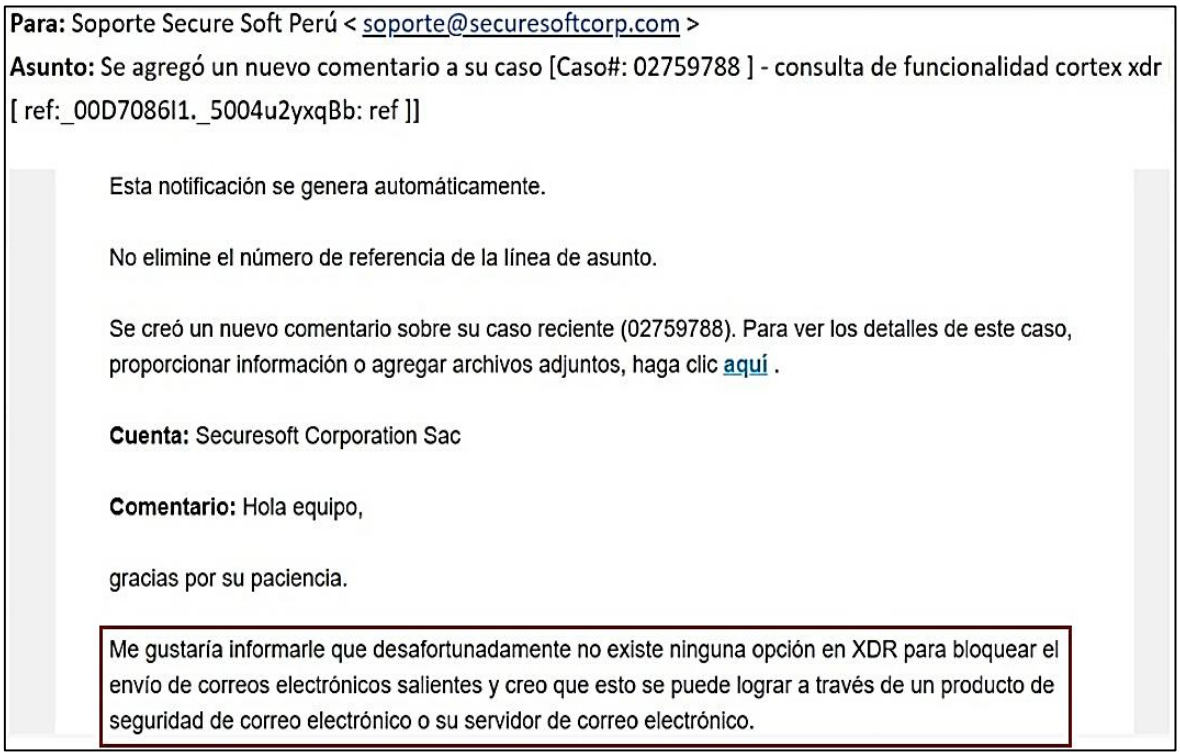
Hola Jorge Manuel,

Soy Aldrin del soporte técnico de Trend Micro.

Entiendo que le gustaría saber si Apex One puede bloquear el envío de correo saliente a un dominio específico; esta no es una función de Apex One. Si tiene un escáner de correo electrónico instalado, puede hacerlo a través de IMSVA, ScanMail for Exchange. Otra pregunta que tiene es si Apex One puede bloquear la unidad USB, esto se puede hacer a través de DLP/Control de dispositivo. Aquí está el enlace sobre cómo habilitarlo: https://success.trendmicro. com/solution/000293332

Háganos saber si tiene alguna pregunta.

Anexo 2. Consulta de funcionalidad de Cortex XDR



Para: Soporte Secure Soft Perú < soporte@securesoftcorp.com >
Asunto: Se agregó un nuevo comentario a su caso [Caso#: 02759788] - consulta de funcionalidad cortex xdr [ref:_00D7086I1._5004u2yxqBb: ref]]

Esta notificación se genera automáticamente.

No elimine el número de referencia de la línea de asunto.

Se creó un nuevo comentario sobre su caso reciente (02759788). Para ver los detalles de este caso, proporcionar información o agregar archivos adjuntos, haga clic aquí .

Cuenta: Securesoft Corporation Sac

Comentario: Hola equipo,

gracias por su paciencia.

Me gustaría informarle que desafortunadamente no existe ninguna opción en XDR para bloquear el envío de correos electrónicos salientes y creo que esto se puede lograr a través de un producto de seguridad de correo electrónico o su servidor de correo electrónico.

Anexo 3. Eventos críticos de bloqueo USB y bluetooth

Gravedad	Tipo de inci ...	Nombre prin ...	Nombre de in...	Nombre del e...	Acción real	Reglas
Crítica (4)	Conexión del ...	kzambrano@s...	SSOFTCORP\...	PC-SOC-73	Bloquear	Bloqueo Plug an...
Crítica (4)	Conexión del ...	rrios@secur...	SSOFTCORP\...	PC-SOC-78	Bloquear	Bloqueo Plug an...
Crítica (4)	Conexión del ...	kzambrano@s..	SSOFTCORP\...	PC-SOC-73	Bloquear	Bloqueo Plug an...
Advertencia	Protección ...	rrios@secur..	SSOFTCORP\...	PC-SOC-78	Bloquear	Protección Web
Crítica (4)	Conexión del ...	aquispe@s...	SSOFTCORP\...	PC-SOC-82	Bloquear	Bloqueo Plug an...
Crítica (4)	Conexión del ...	rrios@secur...	SSOFTCORP\...	PC-SOC-78	Bloquear	Bloqueo Plug an...
Crítica (4)	Conexión del ...	kzambrano@s..	SSOFTCORP\...	PC-SOC-73	Bloquear	Bloqueo Plug an...
Crítica (4)	Conexión del ...	aquispe@s...	SSOFTCORP\...	PC-SOC-82	Bloquear	Bloqueo Plug an...
Crítica (4)	Conexión del ...	rcondori@s..	SSOFTCORP\...	PC-SOC-85	Bloquear	Bloqueo Plug an...
Crítica (4)	Conexión del ...	mberrocal@s...	SSOFTCORP\...	PC-SOC-38	Bloquear	Bloqueo Plug an...
Crítica (4)	Conexión del ...	rcondori@s..	SSOFTCORP\...	PC-SOC-85	Bloquear	Bloqueo Plug an...
Crítica (4)	Conexión del ...	mberrocal@s...	SSOFTCORP\...	PC-SOC-38	Bloquear	Bloqueo Plug an...
Crítica (4)	Conexión del ..	rcondori@s..	SSOFTCORP\...	PC-SOC-85	Bloquear	Bloqueo Plug an...

Anexo 4. Eventos críticos del bloqueo de correos

Gravedad	Tipo de inci ...	Nombre prin ...	Nombre de in...	Nombre del e...	Acción real	Reglas
Crítica (4)	Conexión del ...	jperez@sec...	SSOFTCORP\...	PC-SOC-92	Bloquear	Bloqueo Plug an...
Crítica (4)	Protección de ..	tlopez@sec...	SSOFTCORP\...	PC-SOC-95	Bloquear	Bloqueo de c...
Crítica (4)	Conexión del ...	jperez@sec...	SSOFTCORP\...	PC-SOC-92	Bloquear	Bloqueo Plug an...
Advertencia	Protección ...	jsurita@sec	SSOFTCORP\...	PC-SOC-98	Bloquear	Protección Web
Crítica (4)	Conexión del ...	tlopez@sec...	SSOFTCORP\...	PC-SOC-95	Bloquear	Bloqueo Plug an...
Crítica (4)	Protección de ..	dsilva@sec...	SSOFTCORP\...	PC-SOC-134	Bloquear	Bloqueo de c...
Crítica (4)	Protección de ..	jperez@sec...	SSOFTCORP\...	PC-SOC-92	Bloquear	Bloqueo de c...
Crítica (4)	Protección de ..	jsurita@sec	SSOFTCORP\...	PC-SOC-98	Bloquear	Bloqueo de c...
Crítica (4)	Conexión del ...	tlopez@sec...	SSOFTCORP\...	PC-SOC-95	Bloquear	Bloqueo Plug an...
Crítica (4)	Protección de ..	dsilva@sec...	SSOFTCORP\...	PC-SOC-134	Bloquear	Bloqueo de c...
Crítica (4)	Conexión del ...	tlopez@sec...	SSOFTCORP\...	PC-SOC-95	Bloquear	Bloqueo Plug an...
Crítica (4)	Conexión del ...	dsilva@sec...	SSOFTCORP\...	PC-SOC-134	Bloquear	Bloqueo Plug an...
Crítica (4)	Conexión del ..	jsurita@sec.	SSOFTCORP\...	PC-SOC-98	Bloquear	Bloqueo Plug an...