Implementación de políticas de seguridad de la información mediante una solución de Prevención de Perdida de Datos (DLP) para el ESPE-CERT

Quiroga Siza, Kevin Alexander

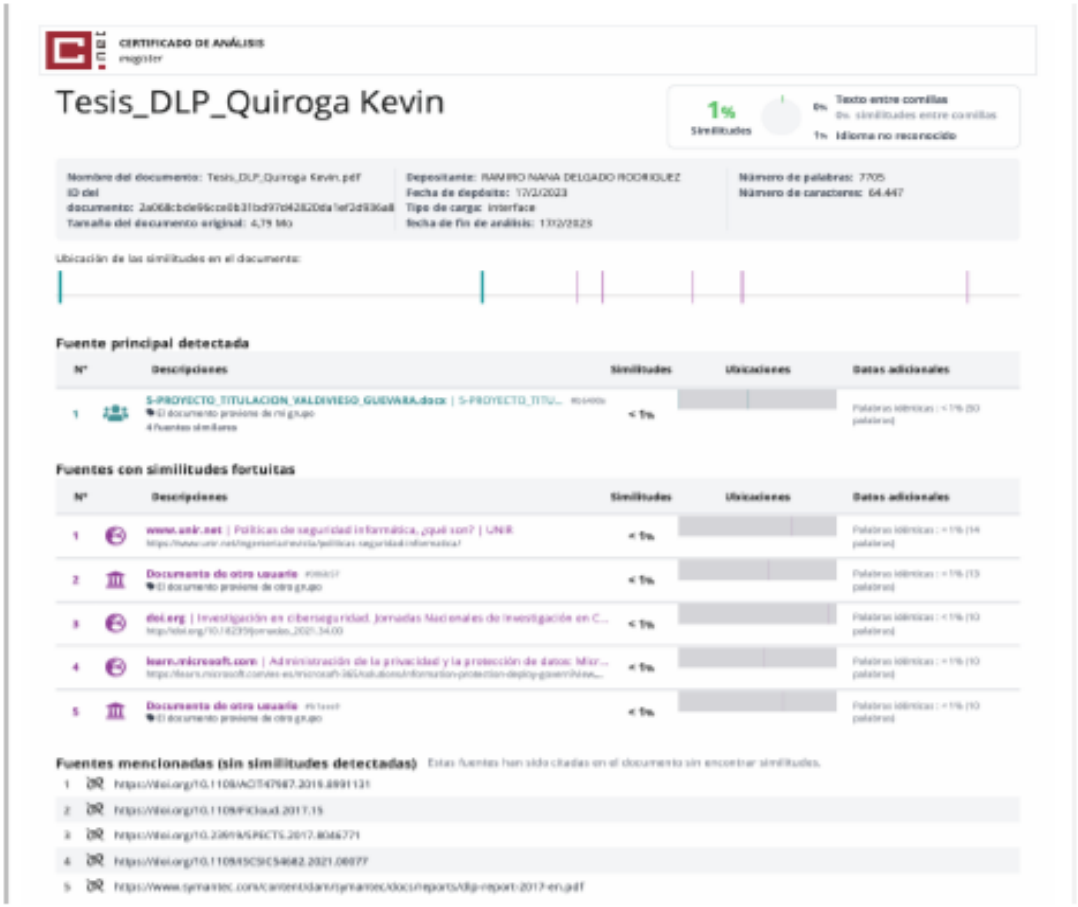
Departamento de Ciencias de la Computación

Carrera de Ingeniería de Sistemas e Informática

Trabajo de titulación, previo a la obtención del título de Ingeniero en Sistemas e Informática

Ing. Fuertes Díaz, Walter Marcelo, PHD

22 de febrero del 2023



CERTIFICADO DE ANÁLISIS
Tesis_DLP_Quiroga Kevin

1% Similitudes
0% Texto entre comillas
0% Idioma no reconocido

Nombre del documento: Tesis_DLP_Quiroga Kevin.pdf
ID del documento: 2a068cbcbde95cce8b31bd97d4282bda1ef2d936a8
Tamaño del documento original: 4,79 Mb

Depositante: RAMIRO NANA DELGADO RODRIGUEZ
Fecha de depósito: 17/2/2023
Tipo de carga: interface
Fecha de fin de análisis: 17/2/2023

Número de palabras: 7705
Número de caracteres: 64.447

Ubicación de las similitudes en el documento:

Fuente principal detectada

Nº	Descripciones	Similitudes	Ubicaciones	Datos adicionales
1	S-PROYECTO_TITULACION_VALDIVIESO_GUEVARA.docx | S-PROYECTO_TITU... El documento proviene de mi grupo. 4 fuentes similares	< 1%		

Fuentes con similitudes fortuitas

Nº	Descripciones	Similitudes	Ubicaciones	Datos adicionales
1	www.unir.net | Políticas de seguridad informática, ¿qué son? | UNIR	< 1%		
2	Documento de otro usuario El documento proviene de otro grupo	< 1%		
3	doi.org | Investigación en ciberseguridad. Jornadas Nacionales de Investigación en C...	< 1%		
4	learn.microsoft.com | Administración de la privacidad y la protección de datos: Micr...	< 1%		
5	Documento de otro usuario El documento proviene de otro grupo	< 1%		

Fuentes mencionadas (sin similitudes detectadas) Estas fuentes han sido citadas en el documento sin encontrar similitudes.

1 https://doi.org/10.1109/ACT47987.2019.8991131
2 https://doi.org/10.1109/PICloud.2017.15
3 https://doi.org/10.2991/ASPECTS.2017.8046721
4 https://doi.org/10.1109/ISCSIC54682.2021.00077
5 https://www.symantec.com/content/dam/symantec/docs/reports/dlp-report-2017-en.pdf

Firma:

WALTER MARCELO FUERTES DIAZ

Ing. Fuertes Díaz, Walter Marcelo, PHD

Director

Departamento de Ciencias de la Computación

Carrera de Ingeniería de Sistemas e Informática

Certificación

Certifico que el trabajo de titulación: "**Implementación de políticas de seguridad de la información mediante una solución de Prevención de Perdida de Datos (DLP) para el ESPE-CERT**" fue realizado por el señor **Quiroga Siza, Kevin Alexander;** el mismo que cumple con los requisitos legales, teóricos, científicos, técnicos y metodológicos establecidos por la Universidad de las Fuerzas Armadas ESPE, además fue revisado y analizado en su totalidad por la herramienta de prevención y/o verificación de similitud de contenidos; razón por la cual me permito acreditar y autorizar para que se lo sustente públicamente.

Sangolquí, 09 de mayo del 2023

Firma:

.....

Ing. Fuertes Díaz, Walter Marcelo, PHD

C. C. 1707017701

Departamento de Ciencias de la Computación
Carrera de Ingeniería de Sistemas e Informática

Responsabilidad de Autoría

Yo, **Quiroga Siza, Kevin Alexander**, con cédula de ciudadanía n°1726152661, declaro que el contenido, ideas y criterios del trabajo de titulación**: Implementación de políticas de seguridad de la información mediante una solución de Prevención de Perdida de Datos (DLP) para el ESPE-CERT** es de mi autoría y responsabilidad, cumpliendo con los requisitos legales, teóricos, científicos, técnicos, y metodológicos establecidos por la Universidad de las Fuerzas Armadas ESPE, respetando los derechos intelectuales de terceros y referenciando las citas bibliográficas.

Sangolquí, 09 de mayo del 2023

Firma

.....

Quiroga Siza, Kevin Alexander

C.C.: 1726152661

Departamento de Ciencias de la Computación

Carrera de Ingeniería de Sistemas e Informática

Autorización de Publicación

Yo **Quiroga Siza, Kevin Alexander**, con cédula de ciudadanía n° 1726152661, autorizo a la Universidad de las Fuerzas Armadas ESPE publicar el trabajo de titulación: **Implementación de políticas de seguridad de la información mediante una solución de Prevención de Perdida de Datos (DLP) para el ESPE-CERT** en el Repositorio Institucional, cuyo contenido, ideas y criterios son de mi responsabilidad.

Sangolquí, 09 de mayo del 2023

Firma

.....

Quiroga Siza, Kevin Alexander

C.C.: 1726152661

Dedicatoria

El presente trabajo de titulación lo dedico a mis padres que con su esfuerzo lograron proveer lo necesario para poder cumplir esta meta, su cariño y perseverancia me mostraron que cuando algo se hace con amor siempre tendrá su recompensa.

En este apartado especial quiero mencionar a la mejor persona que pude tener como Abuelito el señor Suboficial de la Fuerza Aérea Ecuatoriana Luis Siza, a pesar de que se encuentra disfrutando de la eternidad y presencia de Dios siempre estuvo presente en cada paso de mi vida, demostrándome con su ejemplo lo que es ser una verdadera persona en todos los ámbitos y sobre todo el servicio a los demás por medio del amor de Dios.

A mi hermana Karen, que ha estado presente desde el inicio de esta etapa de mi vida, y que a través de este logro pueda entender que todo el conocimiento viene de Dios, pero también debemos esforzarnos.

Kevin Quiroga

Agradecimiento

Mas sean dadas gracias a Dios, 1 Corintios 15:57 a, tomando a consideración el versículo mencionado, quiero comenzar agradeciendo a Dios, quien fue el que me permitió vivir esta etapa y sobre todo la sabiduría para poder afrontar cada momento, reconociéndolo como el único señor y salvador en el cual descansa mi vida.

A mi familia paterna que a pesar de la distancia siempre estuvieron pendientes de los avances que tenía en mi vida universitaria, siempre estuvo presente su respaldo con palabras de aliento y cariño.

A mi familia materna que fueron el apoyo más grande no solo en lo académico si no en toda mi vida, cada uno aporto con sus enseñanzas, consejos, palabras de alegría y lo más importante una palabra de bendición por parte de Dios.

A mis padres y mi hermana, son la razón por la cual nunca me di por vencido cada paso en mi vida ha sido para buscar su bienestar y que puedan tener en mi un apoyo.

Finalmente Agradecer a todos los docentes de la Universidad de las Fuerzas Armadas ESPE, por la dedicación y conocimientos impartidos. De manera muy especial al Dr. Walter Fuertes y al Ing. Mario Ron quienes me brindaron toda su ayuda, tiempo y conocimiento en este proceso de elaboración del proyecto de tesis.

Kevin Quiroga

Contenido

Índice de Tablas

Índice de Figuras

Resumen

En este trabajo se muestra la contribución realizada al Cert Académico ESPE con el objetivo que se presente como servicio una solución para la prevención de perdida de datos (DLP). El trabajo desarrollado muestra la implementación de una herramienta para la aplicación de políticas de seguridad y la gestión de la fuga de información. La herramienta contiene 2 entornos de despliegue en los cuales se encuentran en ambientes de nube y local. El entorno de administración en donde se encuentra la consola de administración mediante el cual se realizan la gestión y manejo general de la herramienta. En la consola de administración se encuentran los apartados de configuración las políticas de seguridad que van a ser desplegadas, manejo de usuarios y de dispositivos finales además de los reportes de uso, mediante el agente en el entorno de usuario final, en lo cual es necesario la instalación del agente de comunicación mediante el cual se realiza la comunicación con la consola de administración que se encuentra en la nube con la maquina final que se encuentra de manera local. El agente es el encargado de recopilar el comportamiento del usuario en el dispositivo y envía la información a la consola, también ejecuta las acciones que se generan con las políticas de seguridad con el control del sistema operativo que lo hospeda. Para el desarrollo se utilizó la metodología Design Science, Scrum, y la herramienta Teramind DLP como software de implementación.

Palabras clave: prevención de perdida de datos, políticas, prevención, seguridad de la información

Abstract

This work shows the contribution made to the Cert Academic ESPE with the aim of presenting as a service a solution for the prevention of data loss (DLP). The work developed shows the implementation of a tool for the application of security policies and the management of information leakage. The tool contains 2 deployment environments in which they are in cloud and on-premises environments. The administration environment where the administration console is located, through which the management and general handling of the tool is carried out. In the administration console are the sections of configuration security policies to be deployed, user management and end devices in addition to the reports of use, through the agent in the end user environment, which requires the installation of the communication agent through which communication with the management console that is in the cloud with the final machine that is locally. The agent is responsible for collecting the user's behavior on the device and sends the information to the console, and executes the actions generated with the security policies with the control of the operating system that hosts it. For the development we used the Design Science methodology, Scrum, and the Teramind DLP tool as implementation software.

Keywords: data loss prevention, policies, prevention, information security

Capítulo I
Introducción

Antecedentes

La protección de la información sensible es una preocupación importante para muchas empresas y organizaciones, con el incremento de la digitalización aumenta la dependencia con relación a las tecnologías, de modo que es necesario resguardar los activos que intervienen, para ello la seguridad informática se orienta a la protección de la infraestructura computacional y todo lo relacionado con ésta (incluye la información contenida), por medio de normas, protocolos, métodos, reglas, herramientas y leyes concebidas para minimizar los posibles riesgos a la infraestructura o a la información (Al-Kilani, 2019)

Por lo general, la información puede clasificarse en información “Sensible”, que es utilizada por personas privilegiadas dentro de la organización, e información “Registrada” que es utilizada por usuarios con permisos para manipularla (Al-Kilani, 2019).

En la actualidad, la protección de la información sensible es una preocupación importante para muchas empresas y organizaciones. Algunos de los desafíos más comunes al proteger la información sensible incluyen:

- Identificar qué información es sensible y necesita protección adicional
- Establecer políticas y procedimientos para proteger la información sensible
- Proporcionar una formación adecuada a los empleados sobre el uso

seguro de la información sensible

- Monitorear y evaluar de manera continua la efectividad de las políticas y los procedimientos de protección de la información sensible
- Enfrentar desafíos técnicos y de integración al implementar soluciones de protección de la información sensible en un entorno existente.

Planteamiento del Problema

La fuga de información privilegiada en el Ecuador es un hecho que se ha evidenciado desde años atrás. Como ejemplo de esta situación, se puede mencionar a uno de los casos más recientes que fue de conocimiento general: la filtración de datos de todos y cada uno de los ecuatorianos, los cuales se encontraban bajo la custodia del Registro Civil del Ecuador; en sus sistemas de información (Valladares, 2017).

La pérdida de información confidencial es uno de los problemas más críticos que enfrenta toda institución, dichos datos son considerados como un activo muy valioso, el cual está propenso a ser filtrados por medio de correos electrónicos, mensajería instantánea, impresión o copia en dispositivos de almacenamiento (Al-Kilani, 2019).

En cuanto al Cert Académico ESPE al ser un centro de respuesta a incidentes de seguridad se evidencia la necesidad de administrar, monitorear y proveer un servicio que proteja la fuga de información.

La solución que se propone es la implementación de una herramienta para la Prevención de fuga de datos (Data Loss Prevention), que tiene como objetivo que el Cert Académico ESPE provea el servicio de DLP con el fin de que evitar la fuga de

información mediante monitoreo, gestión y aplicación de políticas de seguridad de la información.

Justificación

La pérdida de datos es un problema grave que afecta a empresas y organizaciones de todo tipo. Puede ser causada por una variedad de factores, como fallos técnicos, ataques cibernéticos, errores humanos o desastres naturales.

Los ataques cibernéticos han aumentado en severidad y complejidad. Eso requiere que el CERT/CSIRT investigue y desarrolle nuevas herramientas de seguridad. Por ello la información digital es uno de los activos más importantes a proteger en una organización (Al-Kilani, 2019). El crecimiento y evolución de amenazas, vulnerabilidades y ciberataques incrementan los incidentes de seguridad y generan impactos negativos en las organizaciones (Valladares, 2017). Todas las organizaciones, ya sean educativas, financieras o gubernamentales, no pueden funcionar sin él (Al-Kilani, 2019). La seguridad de la información es un tema que cobra cada día más relevancia en todo el mundo. Las amenazas, tanto externas como internas, están en constante aumento, diversificación de sus formas y frecuencias de ataque, lo que lleva a una mayor tasa de fuga de información (Valladares, 2017).

Hoy en día, a pesar de las inversiones en sistemas de protección de hardware y software para reducir los riesgos de TI de una organización, se ha destacado a través de informes (CSIRT), un aumento de los ataques en línea y más contra la información digital que toda organización tiene. Las nuevas tecnologías de transferencia de datos

han facilitado la comunicación dentro de las empresas, sin embargo, esto aumenta los riesgos para la seguridad de la información confidencial (Miloslavskaya, 2017).

La implementación de una solución de Prevención de pérdidas de datos (DLP, por sus siglas en inglés) puede ser crucial para garantizar la seguridad y la confidencialidad de los datos de una organización.

DLP

La prevención de pérdidas de datos (DLP) es el conjunto de medidas y técnicas utilizadas para proteger los datos de la pérdida o el acceso no autorizado.

El principio fundamental de esta serie de técnicas se basa en una herramienta más que conocida en el mundo de la seguridad informática: el antivirus; sólo que, en lugar de buscar todas las formas reconocibles de una pieza de malware, este sistema busca patrones y firmas de la información que nosotros consideremos sensible.

Además, otras herramientas DLP se distribuyen por toda la infraestructura de TI (principalmente equipos de escritorio y dispositivos de red) para cubrir todos los estados de información y puntos de exposición (Miloslavskaya, 2017).

El dueño de la información puede definir si algún archivo, base de datos o algún tipo de dato en particular (como el número de una tarjeta de crédito) debe ser analizado y, en su caso, bloqueado si es transmitido por algún medio. Estas herramientas pueden ser configuradas desde la forma más sencilla y ágil de clasificación (pública o privada) hasta el esquema más complejo.

Una de las funcionalidades más interesante es la del monitoreo y bloqueo de transferencia no autorizada de los datos en resguardo. Funciona con la misma tecnología que un firewall para evitar este tipo de ataques, pero en este caso se evita que la información sensible se filtre sin permiso (Alsuwaie, 2021).

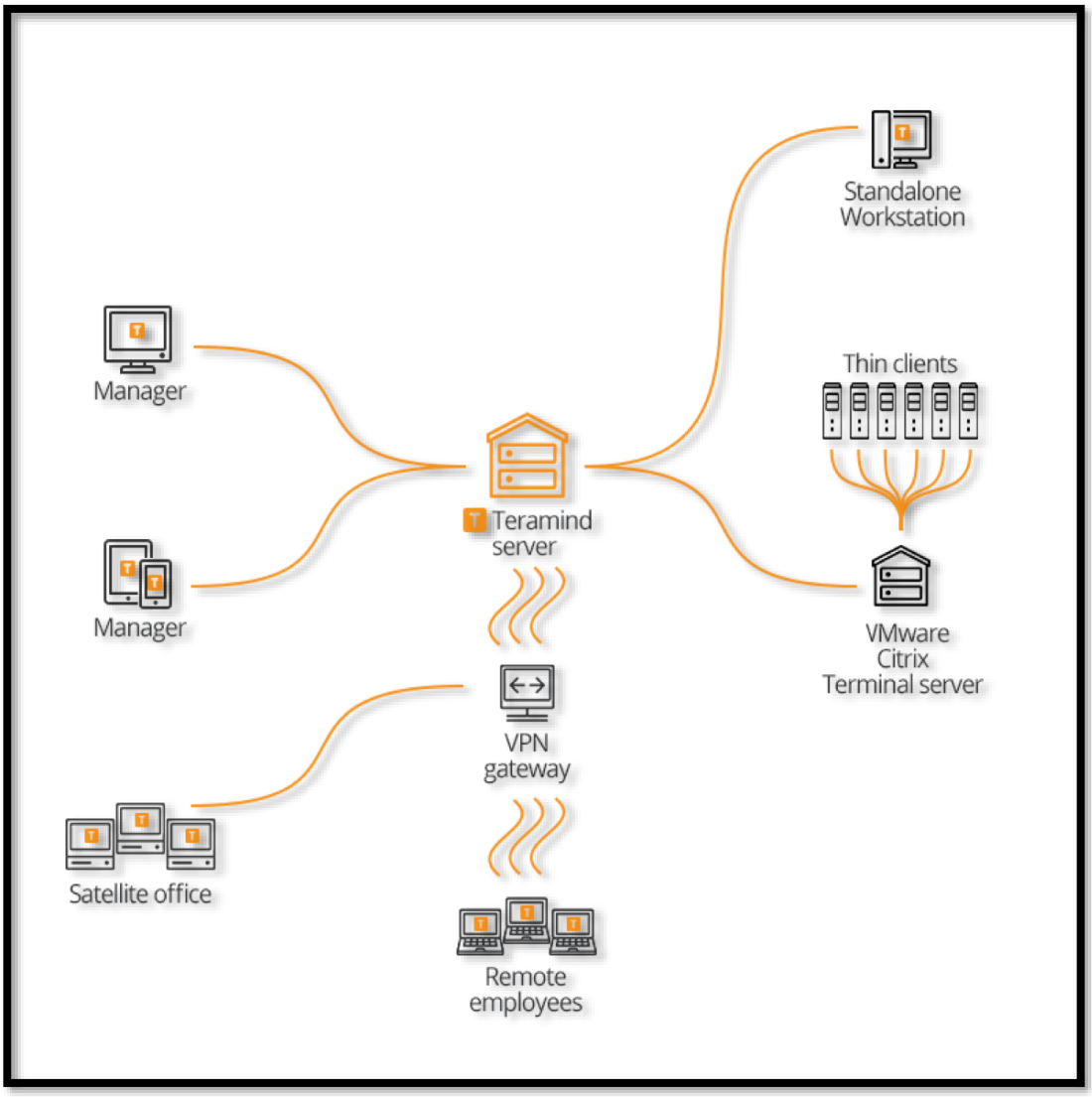
5 tipos de prevención de pérdida de datos

1. **Identificación de datos:** Se trata del proceso que emplean las organizaciones para identificar la información confidencial dentro de su entorno digital.
2. **Identificación de fugas de datos:** Se refiere a un proceso automatizado para detectar e identificar datos usados de manera incorrecta ya sea por perdida o filtración.
3. **DLP para datos en movimiento:** Cuando los datos son transferidos entre ubicaciones, DLP utiliza varias medidas de seguridad para garantizar que los datos lleguen sin manipulación a su destino.
4. **DLP para datos en reposo:** Este tipo de protección incluye datos que no se transmiten y normalmente se almacenan en alguna base de datos o sistema de intercambio de archivos.
5. **DLP para datos en uso:** DLP provee seguridad para los datos que están siendo utilizados de interacciones potencialmente dañinas, como manipulación, captura de pantalla, corte, copia, pegado, impresión o movimiento de información.

En la Figura 1 se muestra una arquitectura de ejemplo para el despliegue de la herramienta Teramind

Figura 1

Arquitectura de ejemplo Teramind



Nota. El gráfico representa la Arquitectura planteada por Teramind para el despliegue

La aplicación de herramientas DLP resuelve tres objetivos que son, son el cumplimiento, la protección de la propiedad intelectual (PI) y la visibilidad de los datos. De manera ampliada se tiene:

- **Cumplimiento de la normativa:** Cuando una empresa u organización recopila y almacena información estará sujeta a las normativas de cumplimiento vigentes en la región en la que opera. Con la utilización de una herramienta DLP es posible identificar, clasificar y etiquetar todos los datos sensibles, supervisar las actividades y los eventos relacionados con esos datos; además disponer de todos los detalles necesarios gracias a los informes generados.
- **Protección de la propiedad intelectual:** En los casos en los que se disponga de propiedad intelectual, secretos comerciales o de estado hay que ser muy cuidadosos. Cualquier pérdida o robo de estos datos podría poner en riesgo. Una solución DLP le permite clasificar la propiedad intelectual y protegerla de exposiciones no deseadas.
- **Visibilidad de los datos:** La mayor parte de las veces es muy recomendable tener visibilidad plena sobre los movimientos de los datos dentro de la organización. Las soluciones DLP son perfectas para ver y rastrear los datos en los puntos finales, las redes y la nube.

Partiendo de estas premisas, el presente trabajo pretende llevar a cabo la implementación de políticas de seguridad mediante una herramienta DLP con la finalidad de que el Cert Académico ESPE provea como servicio, para la aplicación de medidas y seguimiento a la información con esto mitigar y prevenir la fuga de información, brindado una estructura conforme a los estándares actuales de seguridad

Objetivos

Objetivo General

Implementar una solución DLP como un modelo de seguridad, prevención, protección y gobernanza de la información dirigido al Cert Académico de la ESPE para su uso y administración como servicio.

Objetivos Específicos

- Determinar las políticas de seguridad de la información que sean necesarias para que el Cert Académico ESPE brinde el servicio mediante un estudio de las tecnologías que ayude a la prevención de fuga de información.
- Comparar las diversas herramientas de DLP aplicadas a la protección de pérdida de información para la implementación como servicio en el Cert Académico ESPE.
- Supervisar los activos de información sensible que pueden ser protegidos teniendo en cuenta el comportamiento del usuario.
- Implementar el artefacto de software DLP, para la administración y funcionamiento en el Cert Académico ESPE.
- Elaborar una prueba de concepto, en donde se evidencie la implementación de políticas de seguridad.
- Realizar validaciones que permitan identificar conectividad y aplicación de políticas de seguridad, mediante el registro en la consola de administración.

Alcance

Esta investigación comprende la implementación y planteamiento de políticas de seguridad mediante DLP para aplicar la investigación reproducible a proyectos de

ingeniería de software. Como estudio de caso se utilizará el proyecto ESPE-CERT académico en la Universidad de las Fuerzas Armadas ESPE, el cual consiste en un centro de operaciones de seguridad Informática.

Para delinear de forma adecuada el alcance de la investigación planteada, se proponen varias preguntas de investigación asociadas a los objetivos específicos, tal como se muestra en la Tabla1

Tabla 1

Preguntas de Investigación

Objetivo Específico	**Pregunta de Investigación**
OE1. Determinar las políticas de seguridad de la información que sean necesarias para que el Cert Académico ESPE brinde el servicio mediante un estudio de las tecnologías que ayude a la prevención de fuga de información.	**RQ1:** ¿Con qué frecuencia se intercambia información sin catalogar?
OE2. Comparar las diversas herramientas de DLP aplicadas a la protección de pérdida de información para la implementación en el Cert Académico ESPE	**RQ3:** ¿Cuáles son los principales proveedores de DLP en la actualidad? **RQ4:** ¿Qué técnicas son utilizadas para evaluar la vulnerabilidad y el impacto en el manejo de información sensible?

Objetivo Específico	Pregunta de Investigación
OE3. Supervisar los activos de información sensible que pueden ser protegidos teniendo en cuenta el comportamiento del usuario	**RQ5:** ¿Cuáles son los riesgos más comunes de seguridad en torno a la información?
OE4. Implementar el artefacto de software DLP, para la administración y funcionamiento en el Cert Académico ESPE	**RQ6:** ¿En qué escenarios se puede implementar una herramienta de DLP?
OE5. Elaborar una prueba de concepto, en donde se evidencie la implementación de políticas de seguridad.	**RQ7:** ¿Cuál es el resultado de aplicar DLP a la información?

Nota: Esta tabla muestra el desarrollo de las preguntas de investigación y la relación con los objetivos

Hipótesis

La aplicación de políticas de seguridad mediante una herramienta DLP permitirá implementar como servicio y mejorar el nivel de seguridad de la información que ofrece el Cert Académico ESPE

Capítulo II

Marco Metodológico

La metodología que se aplicará para el desarrollo del presente proyecto será Design Science, que posee diferentes fases dentro de las cuales se aplicarán varias metodologías que apoyen y faciliten la investigación además del desarrollo ágil Scrum.

Metodología Design Science

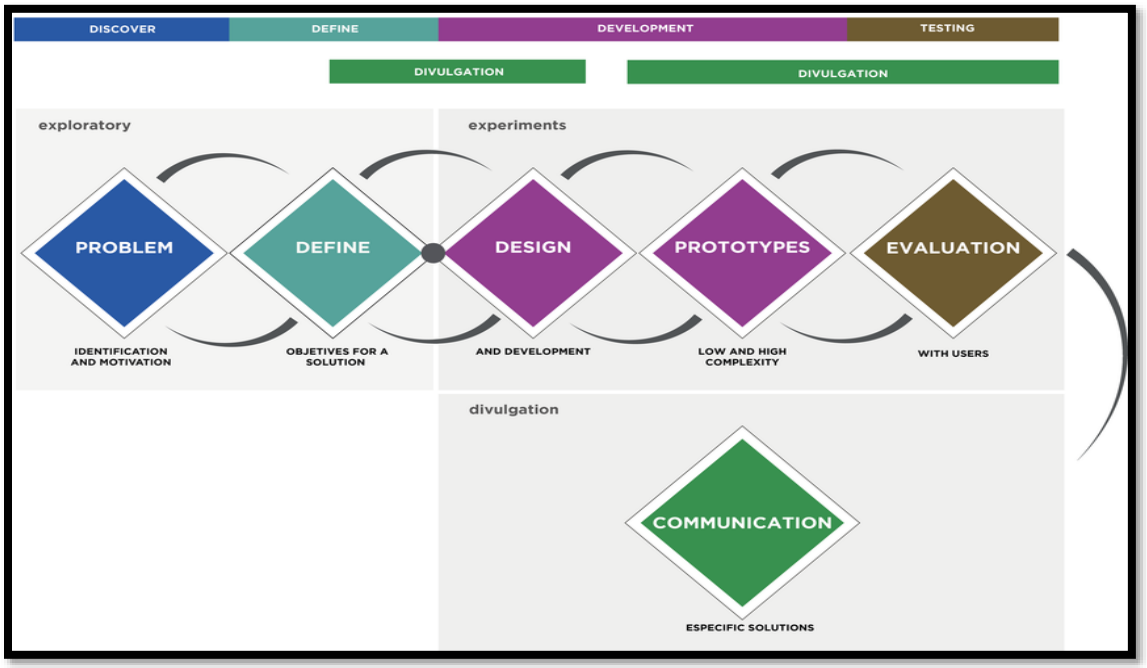
Design science es una metodología aplicada comúnmente a investigaciones en el área de Ciencias de la Computación, y consiste en el diseño y la investigación de artefactos que pertenezcan al contexto. Los artefactos pueden ser de cuatro tipos: constructos (vocabulario y símbolos), modelos (abstracciones y representaciones), métodos (algoritmos y prácticas) o instanciaciones (sistemas prototipos e implementados). Dichos artefactos están diseñados para interactuar con un contexto problemático a fin de mejorar o solucionar algo en ese contexto. Esta metodología es de naturaleza iterativa y consta de las siguientes fases: diseño del artefacto, construcción del artefacto y evaluación del artefacto.

El objetivo de Design Science es desarrollar conocimiento, de modo que el profesional de una disciplina específica lo pueda utilizar para diseñar soluciones en su campo de estudio. Este conocimiento se alcanza mediante la construcción y aplicación de un artefacto diseñado para el dominio de la problemática tratada.

La metodología Design Science se estructura de acuerdo con dos grandes ciclos de resolución de problemas: el ciclo de diseño y el ciclo empírico. El primero contiene el ciclo de ingeniería que es un proceso racional de resolución de problemas. El segundo, es una forma racional de contestar a las preguntas del conocimiento científico y está estructurado como una lista de verificación (Hevner, 2007).

Figura 2

Metodología design science propuesta por Hevner



Nota: Este gráfico muestra el flujo de la metodología Design science

Aplicación de la metodología

- **Entorno:** Lugar y herramienta donde se va a desplegar la solución DLP
- **La base de conocimiento:** Se construyó el desarrollo científico de las variables dependientes e independientes
- **Identificación del problema:** Se identifica y define el problema de pérdida de datos que se desea resolver con el sistema DLP y ofrecerlo como servicio.
- **Investigación:** Se investigan y analizan las características y funcionalidades del sistema DLP.
- **Diseño:** Se diseña la arquitectura de despliegue de la herramienta, teniendo en cuenta las necesidades y prácticas de seguridad de la información.

- **Implementación:** Se lleva a cabo la implementación del sistema DLP de en el entorno de la organización.
- **Configuración:** Se configura y se ajusta el sistema DLP para adaptarse a las necesidades.
- **Evaluación:** Se realiza una evaluación del rendimiento del sistema DLP y se realizan ajustes y mejoras necesarias para garantizar la detección y prevención de la pérdida de datos.
- **Monitoreo:** Se monitorea constantemente el rendimiento del sistema DLP.

Metodología SCRUM

Scrum es un marco de trabajo ágil utilizado en el desarrollo de software y otros proyectos. Fue desarrollado por Ken Schwaber y Jeff Sutherland en la década de 1990 como una forma de mejorar la productividad y la eficiencia en los equipos de desarrollo (Schwaber, 2020).

Scrum se basa en tres pilares: transparencia, inspección y adaptación. La transparencia implica que todos los aspectos del proceso deben ser visibles y entendidos por todos los miembros del equipo. La inspección implica que el equipo debe revisar regularmente su trabajo para detectar problemas y oportunidades de mejora. La adaptación implica que el equipo debe ajustar su trabajo en función de los resultados de la inspección (Schwaber, 2020).

Scrum utiliza una serie de roles, eventos y artefactos para facilitar el proceso de desarrollo. Los roles incluyen el propietario del producto, el equipo de desarrollo y el facilitador del proceso (Scrum Master). Los eventos incluyen la reunión diaria de Scrum,

la revisión del sprint y la retrospectiva del sprint. Los artefactos incluyen el backlog del producto, el backlog del sprint y el incremento (Schwaber, 2020).

Scrum ha demostrado ser efectivo en la mejora de la productividad, la eficiencia y la calidad en el desarrollo de software y otros proyectos. Además, el enfoque ágil de Scrum permite a los equipos adaptarse rápidamente a los cambios y requisitos cambiantes del proyecto (Schwaber, 2020).

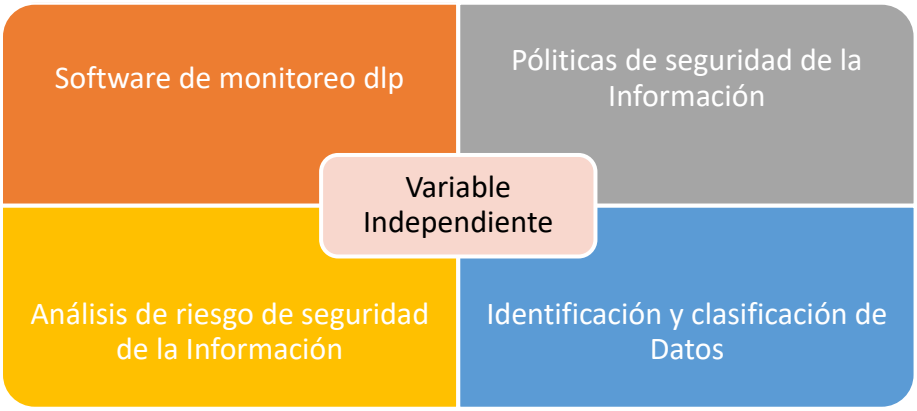
Señalamiento de variables

- **Variables Independientes:** Herramientas y políticas basados en prevención de fuga de información.
- **Variables Dependientes:** Clasificación e identificación de riesgo sobre activos de información.

Con la finalidad de tener un sustento en la sección teórica, se procedió a conformar una red de categorías que se muestran en las figuras 3 y 4.

Figura 3

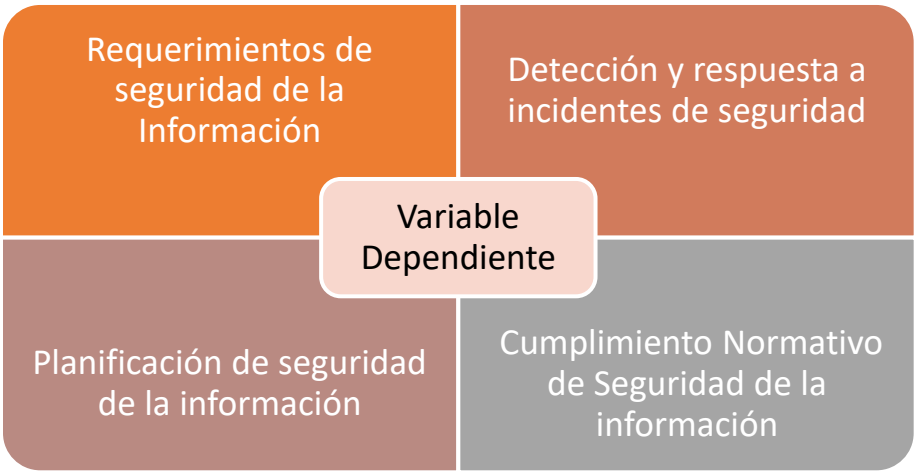
Red de categorías variable independiente



Nota. El gráfico representa la relación de las variables independientes

Figura 4

Red de categorías variable dependiente



Nota. El gráfico representa la relación de las variables independientes

Fundamentación Científica de la variable independiente

Software de monitoreo DLP

El software de monitoreo DLP (Data Loss Prevention) son herramientas informáticas que ayudan a las organizaciones a detectar y prevenir la pérdida accidental o intencional de datos sensibles. Estos programas utilizan una variedad de técnicas, como la monitorización de redes, el análisis de contenido y la detección de patrones, para detectar y bloquear el tráfico de datos sospechoso (Abrams, 2018).

Gartner destaca que DLP es una tecnología madura, que consta de herramientas centradas en casos de uso de la nube y de gestión de riesgos internos, es necesario que las organizaciones implementen soluciones de prevención de pérdida de

datos (DLP) para proteger el manejo cotidiano de datos confidenciales, especialmente en entornos de nube (Gartner, 2019).

El software de monitoreo DLP también pueden ayudar a cumplir con regulaciones y estándares de seguridad de la información aplicables, como el Reglamento general de protección de datos (RGPD) de la Unión Europea, la ISO27001 (Symantec, 2017).

Además de las técnicas mencionadas anteriormente, el software de monitoreo DLP también utilizan diferentes métodos para detectar y prevenir la pérdida de datos, tales como:

- **Control de acceso:** Establecer políticas de acceso a los datos sensibles y restringir el acceso solo a usuarios autorizados.
- **Cifrado:** Proteger los datos sensibles mediante el cifrado para evitar que los datos sean accedidos o modificados por usuarios no autorizados.
- **Detección de comportamiento:** Monitorear el comportamiento de los usuarios y detectar patrones sospechosos para identificar posibles intentos de pérdida de datos.
- **Análisis de contenido:** Revisar y analizar el contenido de los datos para detectar información confidencial o sensible.
- **Monitorización de dispositivos:** Monitorear y supervisar el uso de dispositivos de almacenamiento externos, como discos duros USB, para detectar la copia no autorizada de datos.
- **Integración con otros sistemas:** Integrar el software DLP con otros sistemas

de seguridad, como sistemas de detección de intrusos o sistemas de cumplimiento normativo, para mejorar la protección de los datos.

Es importante mencionar que el software de monitoreo DLP no son una solución única para la prevención de la pérdida de datos y deben ser utilizados en conjunto con otras medidas de seguridad, como la implementación de políticas y procedimientos de seguridad sólidos, la capacitación y concientización de los empleados y la implementación de medidas de continuidad del negocio (Abrams, 2018).

Políticas de seguridad de la Información

Las políticas de seguridad de la información son un conjunto de reglas y directrices que establecen las normas y procedimientos para proteger los datos sensibles de una organización. Su objetivo principal es prevenir la pérdida, robo, acceso no autorizado, alteración o destrucción de los datos. La agencia de seguridad CISA (Cybersecurity and Infrastructure Security Agency) considera que una política de seguridad de la información es un documento técnico presentado de una manera formal en donde se especifica cómo una organización se protege a y como protege a sus activos (CISA, 2019).

Las políticas de seguridad de la información suelen incluir aspectos como: Identificación y clasificación de datos, análisis de riesgos, control de acceso, detección y respuesta a incidentes, continuidad del negocio, cumplimiento, entre otros.

En PwC (PricewaterhouseCoopers) se menciona que, un sistema sólido de seguridad de la información, que incluya políticas y procedimientos de seguridad,

es fundamental para proteger los activos de una organización (PwC, 2019). Una política de seguridad de la información es esencial para garantizar que los empleados entiendan y cumplan con los estándares de seguridad de la información de la organización (Forrester, 2019).

Como ejemplo de políticas de seguridad se tiene:

- La información estará protegida contra cualquier acceso no autorizado.
- La confidencialidad de la información, que relacionada con los datos de carácter personal de los empleados y clientes.
- La integridad de la información se mantiene en relación con la clasificación de la información (especialmente la “confidencial”).
- Políticas de descubrimiento que se aplican como medidas de recolección de información sobre el comportamiento del usuario

Análisis de riesgo de seguridad de la Información

El análisis de riesgos de seguridad de la información es un proceso que busca identificar y evaluar los riesgos a los que está expuesta una organización, con el objetivo de tomar medidas para minimizarlos. Es una parte esencial en la planificación y gestión de la seguridad de la información, ya que permite a las organizaciones conocer sus activos críticos, los riesgos a los que están expuestos y las medidas de seguridad necesarias para protegerlos.

La necesidad de proteger los datos en un entorno cada vez más digital y regulado ha llevado a un aumento en la importancia del análisis de riesgos de seguridad

de la información. El análisis de riesgos es un proceso continuo que ayuda a las organizaciones a identificar, evaluar y priorizar los riesgos de ciberseguridad y tomar decisiones informadas sobre cómo abordarlos (ISACA, Data Governance and Classification, 2019).

El análisis de riesgos de seguridad de la información suele incluir las siguientes etapas:

- **Identificación de activos:** Se busca identificar los activos críticos de la organización y su importancia en el negocio.
- **Identificación de amenazas y vulnerabilidades:** Se busca identificar las amenazas y vulnerabilidades que pueden afectar a los activos identificados.
- **Evaluación de impacto y probabilidad:** Se busca evaluar el impacto potencial y la probabilidad de que una amenaza o vulnerabilidad se materialice.
- **Selección de medidas de seguridad:** Se busca seleccionar las medidas de seguridad que mejor se adapten a los riesgos identificados.
- **Implementación y monitoreo:** Se busca implementar las medidas de seguridad seleccionadas y monitorear su efectividad.

Identificación y clasificación de Datos

La identificación y clasificación de datos es un proceso esencial en la gestión de la seguridad de la información, ya que permite a las organizaciones conocer qué datos tienen y cómo deben ser protegidos. La clasificación de los datos se refiere a la asignación de un nivel de confidencialidad, integridad y disponibilidad a los datos, y la identificación de los datos se refiere a la localización y recuperación de estos.

La clasificación de datos es una herramienta esencial para la seguridad de la información ya que ayuda a las organizaciones a interpretar qué datos deben protegerse y la manera de hacerlo (ISACA, Data Governance and Classification, 2019). La identificación y clasificación de datos también ayuda a las organizaciones a cumplir con regulaciones y estándares de seguridad de la información aplicables, como el RGPD de la Unión Europea o la Ley de Protección de Datos Personales de Ecuador.

El proceso de identificación y clasificación de datos suele incluir las siguientes etapas: Inventario de datos, clasificación de datos, implementación de controles de seguridad, monitoreo y auditorías.

La clasificación de datos es una parte importante de la gobernanza de datos y es esencial para implementar controles de seguridad adecuados y cumplir con regulaciones y estándares de seguridad de la información (McAfee, 2019).

Fundamentación Científica de la variable dependiente

Requerimientos de seguridad de la Información

Los controles necesarios para proteger la confidencialidad, integridad y disponibilidad de la información, se deben establecer políticas y objetivos claros de seguridad de la información para guiar la gestión (ISO, ISO/IEC 27001:2013, 2018). Los requerimientos de seguridad de la información son esenciales para garantizar la protección de la información confidencial y la prevención de amenazas y vulnerabilidades. Estos requerimientos incluyen medidas técnicas y administrativas para

proteger la información contra amenazas y vulnerabilidades, así como para cumplir con las regulaciones y normativas aplicables.

Los requerimientos de seguridad de la información son establecidos por normas y estándares internacionales como ISO/IEC 27001:2013, NIST y COBIT. Además, estas normativas proporcionan un enfoque sistemático para la identificación, evaluación y tratamiento de riesgos a la seguridad de la información y establecen los requisitos para establecer, implementar, mantener y supervisar un sistema de gestión de la seguridad de la información.

Detección y respuesta a incidentes de seguridad

La detección de incidentes se refiere a la identificación temprana de eventos o actividades sospechosas que pueden indicar un incidente de seguridad. Esto puede incluir, por ejemplo, la detección de actividades maliciosas en un sistema de seguridad, la detección de una violación de seguridad en una red o la detección de una posible intrusión en un sistema informático. Estos eventos pueden ser detectados mediante la utilización de herramientas de seguridad automatizadas, como firewalls, sistemas de detección de intrusos (IDS) o sistemas de detección de amenazas (TDS), o mediante la monitorización manual realizada por los profesionales de seguridad de la información.

La respuesta a incidentes hace referencia a las acciones tomadas para mitigar el impacto de un incidente de seguridad, tales como la contención, la eliminación y la recuperación. Es importante contar con un equipo dedicado a la gestión de incidentes de seguridad y un plan de respuesta a incidentes actualizado y comprendido por todos

los miembros de la organización. Es importante realizar pruebas regulares y simulacros para probar y mejorar el plan de respuesta a incidentes.

El proceso de detección y respuesta a incidentes de seguridad se compone de varios pasos, como la detección temprana de incidentes, la evaluación de riesgos y la respuesta rápida y efectiva a incidentes.

La detección y respuesta a incidentes de seguridad son procesos interdependientes y deben ser abordados de manera integrada para garantizar una respuesta efectiva a incidentes de seguridad. La detección temprana y la respuesta adecuada a los incidentes de seguridad son fundamentales para minimizar el impacto y los riesgos para la organización (Cybersecurity, 2020).

Planificación de seguridad de la información

La planificación de seguridad de la información es el proceso de establecer una estrategia para proteger la información de una organización y minimizar el impacto de incidentes de seguridad (NIST, 2020).

Este proceso incluye la identificación de activos críticos y la evaluación de riesgos para determinar los controles de seguridad necesarios para protegerlos. La identificación de activos críticos involucra el análisis de los sistemas y los datos de la organización para determinar cuáles son los activos más valiosos y críticos para la continuidad del negocio. La evaluación de riesgos, por otro lado, implica el análisis de los riesgos potenciales a esos activos y cómo podrían afectar el negocio (ISO, 2021).

Además, la planificación de seguridad de la información debe ser abordada de manera integrada con la gestión de riesgos y la gestión de continuidad del negocio (COBIT, 2019). Esto garantiza que se establezcan controles adecuados para minimizar el impacto de incidentes de seguridad en el negocio. La gestión de riesgos implica la identificación, evaluación y mitigación de los riesgos a los activos críticos. La gestión de continuidad del negocio, por otro lado, implica la planificación de cómo se manejarán incidentes de seguridad y cómo se asegurará la continuidad del negocio.

Cumplimiento Normativo de Seguridad de la información

El cumplimiento normativo de seguridad de la información se refiere a la conformidad con las regulaciones, estándares y leyes aplicables a la protección de la información (NIST, 2020). Estas regulaciones pueden incluir normas sectoriales, como HIPAA en el sector de la salud, o estándares internacionales como ISO 27001. El cumplimiento normativo también puede incluir la conformidad con leyes y regulaciones aplicables, como el Reglamento General de Protección de Datos (RGPD) en Europa.

El objetivo del cumplimiento normativo es garantizar que las organizaciones implementen controles de seguridad adecuados para proteger la información y cumplan con las regulaciones aplicables (ISO, 2018). La implementación de controles de seguridad adecuados puede incluir medidas de seguridad física y lógica, políticas y procedimientos, y un programa de gestión de seguridad de la información.

La conformidad con las regulaciones normativas también puede incluir la realización de auditorías y pruebas para garantizar que los controles de seguridad se

implementen y se cumplan (NIST, 2020). Esto puede incluir auditorías internas y externas, así como la realización de pruebas de penetración para evaluar la eficacia de los controles de seguridad.

Herramientas de Desarrollo

Software

Software DLP

Para la elección de la herramienta de Software DLP se tomaron en cuenta los aspectos descritos en la Tabla 2.

Tabla 2

Comparativa de Herramientas DLP

Característica	McAfee DLP	Symantec DLP	Trend Micro DLP	Forcepoint DLP	Teramind DLP	Open DLP
Configuración de políticas	Fácil	Media	Media	Media	Fácil	Difícil
Personalización de alertas	Sí	Sí	Sí	Sí	Sí	No
Integración con sistemas de gestión de incidentes	Sí	Sí	Sí	Sí	Sí	No

Característica	McAfee DLP	Symantec DLP	Trend Micro DLP	Forcepoint DLP	Teramind DLP	Open DLP
Despliegue en la nube	Sí	Sí	Sí	Sí	Sí	No
Arquitectura basada en la nube	No	No	No	Sí	Sí	No
Capacidad de monitoreo de nube	No	No	No	No	Sí	No
Capacidad de monitoreo de aplicaciones	Sí	Sí	No	No	Sí	Sí

Nota: Esta tabla muestra la comparativa entre las herramientas dlp existentes en el mercado y las características principales

En consideración como los parámetros descritos en relación con despliegue en nube, monitoreo, reglas y configuración el software a utilizar es Teramind DLP

Teramind DLP

Teramind DLP es un software de prevención de pérdida de datos desarrollado por la empresa Teramind. Este software está diseñado para ayudar a las organizaciones a proteger sus datos confidenciales mediante la detección y prevención de accesos no autorizados, la copia o el uso indebido de información confidencial.

Teramind DLP ofrece una variedad de características para ayudar a las organizaciones a cumplir con regulaciones y normativas de privacidad y seguridad de la información, tales como el RGPD y HIPAA.

Entre las características de Teramind DLP se incluyen: detección de contenido sensibles, control de acceso, auditoría y registro, control de dispositivos, control de aplicaciones, control de red, etc.

Teramind DLP se integra con otros sistemas de seguridad, como firewalls, sistemas de detección de intrusos y sistemas de gestión de identidades, para proporcionar una protección de datos más completa (Symantec, 2017).

Hardware

Características DLP Host

Teramind DLP maneja dos tipos de servicio on-premise y cloud, para el desarrollo de esta investigación se realizó el despliegue Cloud, ya que, de acuerdo con la arquitectura, el escalamiento se lo realiza conforme a la

necesidad, con esto se optimiza el tiempo de configuración y aplicación de políticas.

En términos técnicos, el software se ejecuta en servidores administrados por Teramind y se accede a través de una interfaz web.

- **Procesador:** Se recomienda un procesador de al menos 4 núcleos y 2.4GHz.
- **Memoria RAM:** Se recomienda al menos 8 GB de memoria RAM.
- **Espacio de almacenamiento:** Se recomienda al menos 500 GB de espacio de almacenamiento para la instalación y los datos de la solución.
- **Tarjeta de red:** Se recomienda una tarjeta de red de al menos 1 Gbps para garantizar un rendimiento adecuado.
- **Sistema operativo:** Se recomienda un sistema operativo compatible, como Windows Server o Linux, que cumpla con los requisitos de soporte de Teramind.
- **Adaptador de red:** se recomienda al menos 2 adaptadores de red para la redundancia.
- **Disco duro:** se recomienda al menos 2 discos duros en configuración RAID para garantizar la seguridad de los datos.

Lo mencionado anteriormente son recomendaciones proporcionadas por Teramind, para efectos del uso en este desarrollo se encuentra cubierto todos los puntos ya que el despliegue es en la nube y las capacidades de hardware son escaladas a demanda.

Características DLP consola Administración

Para el acceso a la consola de administración los requisitos mínimos son:

- **Procesador:** De al menos 2 núcleos y 2.4 GHz.
- **Memoria RAM:** Mínimo 4 GB de memoria RAM.
- **Espacio de almacenamiento:** No se requiere espacio de almacenamiento adicional ya que la solución se ejecuta en servidores administrados por Teramind.
- **Tarjeta de red:** Conexión a Internet de al menos 1 Mbps para garantizar un rendimiento adecuado.
- **Sistema operativo:** Se recomienda un sistema operativo compatible, como Windows, MacOS o Linux.
- **Navegador:** Se recomienda un navegador web actualizado, como Chrome, Firefox, Edge o Safari.
- **Resolución de pantalla:** De al menos 1024x768.

Características Agente DLP

Para el despliegue de los agentes las maquinas en las que se realizara la instalación deben tener los siguientes requisitos mínimos:

- **Procesador:** Se recomienda un procesador de al menos 2 núcleos y 1.8 GHz.
- **Memoria RAM:** Se recomienda al menos 2 GB de memoria RAM.
- **Sistema operativo:** El agente de Teramind DLP es compatible con Windows, MacOS, Linux y dispositivos móviles.

- **Conexión a internet:** El agente debe tener acceso a internet para poder comunicarse con el servidor de Teramind.
- **Espacio en disco:** Es recomendable al menos 1 GB de espacio libre en disco.
- **Puertos:** Se recomienda abrir los puertos 443,53,3389 para la comunicación con el servidor de Teramind.

Capitulo III

Desarrollo

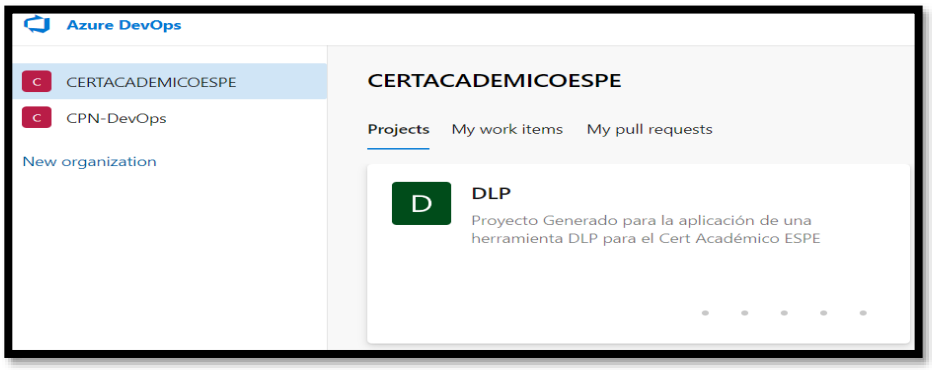
En este capítulo se detallan las fases de la metodología utilizada para el desarrollo de la solución.

SCRUM

Para la aplicación de la metodología scrum se utilizó la herramienta Azure DevOps como se muestra en la Figura 5

Figura 5

Creación de proyecto en azuredevops



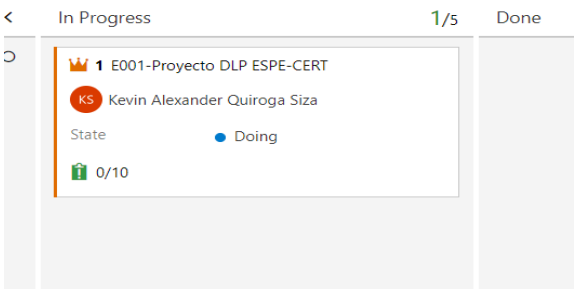
Nota. El gráfico representa la información de azuredevops

Se construyo el backlog del proyecto tomando en cuenta las características del proyecto como despliegue de la herramienta DLP con los siguientes artefactos.

- **Épica:** Se designa una historia de tipo épica que engloba todo el desarrollo del proyecto se lo nombra con el estándar de E000 donde la letra “E” indica que es tipo Épica como se muestra en la Figura 6

Figura 6

Creación de historia épica



Nota. El gráfico representa la visualización de la historia en azuredevops

- **Features:** se asigna a la historia épica features de desarrollo para aplicar la interacción o acción que se va a implementar en todo el proyecto se lo nombra con el estándar de F000 donde la letra “F” indica que es tipo Feature como se evidencia en la Figura 7

Figura 7

Features generados

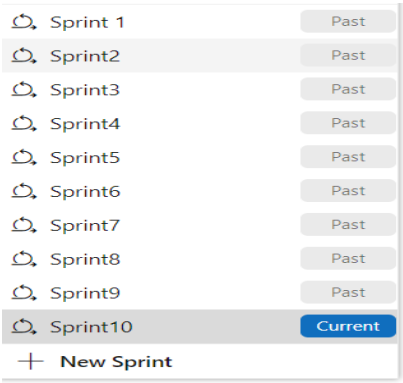
ID	Title	Assigned To
41	F017 Actualización de documento Tesis	Kevin Alexander Quiroga S...
40	F016 Pruebas de despliegue en Ambiente Controlado	Kevin Alexander Quiroga S...
39	F015 Validación de solución Teramind DLP stakeholder	Kevin Alexander Quiroga S...
35	F013 Actualización documento con apartado de Desarrollo	Kevin Alexander Quiroga S...
36	F014 Implementación de Prueba	Kevin Alexander Quiroga S...
31	F011 Busqueda Bibliográfica	Kevin Alexander Quiroga S...
32	F012 Analisis Teramind DLP	Kevin Alexander Quiroga S...
27	F010 Documentación Tesis	Kevin Alexander Quiroga S...
26	F009 Elección herramienta DLP	Kevin Alexander Quiroga S...
10	F003 Revisión de perfil de Tesis	Kevin Alexander Quiroga S...
23	F008 Levantamiento de Información para DLP	Kevin Alexander Quiroga S...
13	F004 Análisis de Herramientas DLP Parte2	Kevin Alexander Quiroga S...
14	F005 Fuentes Bibliográficas	Kevin Alexander Quiroga S...
22	F007 Políticas de Seguridad	Kevin Alexander Quiroga S...
3	F001-Herramientas DLP	Kevin Alexander Quiroga S...
15	F006 Análisis de Infraestructura para DLP	Kevin Alexander Quiroga S...
5	F002 Creación de Documento Formato Tesis	Kevin Alexander Quiroga S...

Nota. El gráfico representa la visualización de los features en azuredevops

- **Sprints:** para el desarrollo se dividió en 10 Sprints con una duración de 15 días que son registrados en la herramienta Azure DevOps como se muestra en la Figura 8.

Figura 8

Sprints generados para el proyecto



Nota. El gráfico representa la visualización de los sprints de proyecto

Cada uno de los Sprints consta de historias y tareas asignadas desde el inicio del proyecto hasta la entrega y presentación a continuación se detallan las actividades dentro de los Sprints.

Sprint1 10/1/2022- 10/15/2022

En la Figura 9 se evidencia las actividades realizadas y las historias generadas en el Sprint, además del estado de la ejecución.

Figura 9

Actividades sprint1

Order	ID	Title	Assigned To	State
1	10	F003 Revisión de perfil de Tesis	Kevin Alexand...	Doing
	11	Validación de Fuentes Bibliográficas	Kevin Alexand...	Done
	12	Comprobación de la Redacción	Kevin Alexand...	Done
2	3	F001-Herramientas DLP	Kevin Alexand...	Doing
	4	Análisis de la Herramientas DLP	Kevin Alexand...	Done
	8	Investigación sobre temas DLP	Kevin Alexand...	Done
3	5	F002 Creación de Documento Formato Tesis	Kevin Alexand...	Doing
	6	Validación Formato Tesis Biblioteca	Kevin Alexand...	Done
	7	Actualización de Documento	Kevin Alexand...	Done
	9	Validación formato de referencias bibliográficas	Kevin Alexand...	Done

Nota. El gráfico representa las actividades generadas dentro del sprint 1

Sprint2 10/16/2022- 10/31/2022

En la Figura 10 se evidencia las actividades realizadas y las historias generadas en el Sprint, además del estado de la ejecución.

Figura 10

Actividades Sprint2

Order	ID	Title	Assigned To	State
1	13	F004 Análisis de Herramientas DLP Parte2	Kevin Alexand...	Doing
	20	Validación de herramientas disponibles	Kevin Alexand...	Done
	21	Validación de integraciones	Kevin Alexand...	Done
2	14	F005 Fuentes Bibliográficas	Kevin Alexand...	Doing
	18	Revisión bibliográfica acerca de soluciones de seguridad ...	Kevin Alexand...	Done
	19	Creación de Referencias en formato APA	Kevin Alexand...	Done
3	15	F006 Análisis de Infraestructura para DLP	Kevin Alexand...	Doing
	16	Busqueda de información despliegues DLP	Kevin Alexand...	Done
	17	Validación de integraciones	Kevin Alexand...	Done

Nota. El gráfico representa las actividades generadas dentro del sprint 2

Sprint3 11/1/2022- 11/15/2022

En la Figura 11 se evidencia las actividades realizadas y las historias generadas en el Sprint, además del estado de la ejecución.

Figura 11

Actividades sprint3

Order	ID	Title	Assigned To	State
1	23	F008 Levantamiento de Información para DLP	Kevin Alexand...	Doing
	24	Investigación de documentación	Kevin Alexand...	Done
2	22	F007 Políticas de Seguridad	Kevin Alexand...	Doing
	25	Investigación sobre políticas de seguridad	Kevin Alexand...	Done

Nota. El gráfico representa las actividades generadas dentro del sprint 3

Sprint4 11/16/2022- 11/30/2022

En la Figura 12 se evidencia las actividades realizadas y las historias generadas en el Sprint, además del estado de la ejecución.

Figura 12

Actividades sprint4

Order	ID	Title	Assigned To	State
1	26	F009 Elección herramienta DLP	Kevin Alexand...	Doing
	29	Revisión Bibliografica	Kevin Alexand...	Done
	30	Validación de Herramienta Teramind DLP	Kevin Alexand...	Done
2	27	F010 Documentación Tesis	Kevin Alexand...	Doing
	28	Actualización de marco metodológico	Kevin Alexand...	Done

Nota. El gráfico representa las actividades generadas dentro del sprint 4

Sprint5 12/1/2022- 12/15/2022

En la Figura 13 se evidencia las actividades realizadas y las historias generadas en el Sprint, además del estado de la ejecución.

Figura 13

Actividades sprint5

Order	ID	Title	Assigned To	State
1	31	F011 Busqueda Bibliográfica	Kevin Alexand...	Doing
	34	Busqueda de información sobre herramienta Dlp y Terami...	Kevin Alexand...	Done
2	32	F012 Analisis Teramind DLP	Kevin Alexand...	Doing
	33	Validación de documentación Teramind	Kevin Alexand...	Done

Nota. El gráfico representa las actividades generadas dentro del sprint 5

Sprint6 12/16/2022- 12/31/2022

En la Figura 14 se evidencia las actividades realizadas y las historias generadas en el Sprint, además del estado de la ejecución.

Figura 14

Actividades sprint6

Order	ID	Title	Assigned To	State
1	36	F014 Implementación de Prueba	Kevin Alexand...	Doing
	37	Validación de tipos de despliegue Teramind DLP	Kevin Alexand...	Done
2	35	F013 Actualización documento con apartado de Desarr...	Kevin Alexand...	Doing
	38	Insertar imagenes de prueba y Desarrollo de el despliegu...	Kevin Alexand...	Done

Nota. El gráfico representa las actividades generadas dentro del sprint 6

Sprint7 1/2/2023- 1/15/2023

En la Figura 15 se evidencia las actividades realizadas y las historias generadas en el Sprint, además del estado de la ejecución.

Figura 15

Actividades sprint7

Order	ID	Title	Assigned To	State
1	40	F016 Pruebas de despliegue en Ambiente Controlado	Kevin Alexand...	Doing
	43	Creación de ambiente controlado Máquina Virtual	Kevin Alexand...	Done
	44	Despliegue de teramind dlp en la nube	Kevin Alexand...	Done
	46	Configuración de Usuario y acceso a la consola	Kevin Alexand...	Done
	47	Instalación de agente en maquina de prueba	Kevin Alexand...	Done
2	41	F017 Actualización de documento Tesis	Kevin Alexand...	Doing
	42	Actualización de documento con pruebas en ambiente co...	Kevin Alexand...	Done
	48	Actualización de evidencia para prueba	Kevin Alexand...	Done
3	39	F015 Validación de solución Teramind DLP stakeholder	Kevin Alexand...	Doing
	45	Reunión validación Ing Mario Ron informante	Kevin Alexand...	Done

Nota. El gráfico representa las actividades generadas dentro del sprint 7

Sprint8 1/16/2023- 1/31/2023

En la Figura 16 se evidencia las actividades realizadas y las historias generadas en el Sprint, el estado de la ejecución además de la reunión de revisión de avance.

Figura 16

Actividades sprint8

Order	ID	Title	Assigned To	State
1	59	F021 Sprint Review	Kevin Alexand...	Done
	60	Reunión Virtual Ing Walter Fuertes	Kevin Alexand...	Done
2	51	F020 Documentación Pruebas	Kevin Alexand...	Done
	52	Toma de capturas y evidencia de pruebas	Kevin Alexand...	Done
	57	Actualización de documento con nuevas capturas y refere...	Kevin Alexand...	Done
3	49	F018 Análisis de Conectividad Teramind	Kevin Alexand...	Done
	53	Pruebas de conexión de agente con la consola Teramind	Kevin Alexand...	Done
	54	Validación de acceso usuarios nuevos a consola	Kevin Alexand...	Done
4	50	F019 Verificación de actividad en consola TeramindDLP	Kevin Alexand...	Done
	55	Validación de registro de máquina en consola Teramind	Kevin Alexand...	Done
	56	Validación de estado de máquina	Kevin Alexand...	Done

Nota. El gráfico representa las actividades generadas dentro del sprint 8

Sprint9 2/1/2023- 2/15/2023

En la Figura 17 se evidencia las actividades realizadas y las historias generadas en el Sprint, además del estado de la ejecución.

Figura 17

Actividades sprint9

Order	ID	Title	Assigned To	State
1	62	Generación de Políticas en Teramind	Kevin Alexand...	Done
	63	Creación de políticas y reglas de descubrimiento para mo...	Kevin Alexand...	Done
	64	Despliegue de políticas y pruebas	Kevin Alexand...	Done
2	61	Revisión de estado herramienta Teramind	Kevin Alexand...	Done
	65	Validación de registros y alertas en consola	Kevin Alexand...	Done
	67	Seguimiento de alertas y paneles de Información	Kevin Alexand...	Done
3	58	F022 Actualización documento con revisiones	Kevin Alexand...	Done
	66	Actualización con políticas y pruebas nuevas	Kevin Alexand...	Done

Nota. El gráfico representa las actividades generadas dentro del sprint 9

Sprint10 2/16/2023- 2/28/2023

En la Figura 18 se evidencia las actividades realizadas y las historias generadas en el Sprint, el estado de la ejecución además de las reuniones de revisión del proyecto.

Figura 18

Actividades sprint10

Order	ID	Title	Assigned To	State
1	71	F028 Revisión Documento	Kevin Alexand...	Done
	72	Validación de documento y observaciones	Kevin Alexand...	Done
2	70	F027 Configuración de consola Teramind en Cert Académico...	Kevin Alexand...	Done
	73	Ingreso desde máquinas operadoras a Consola de Terami...	Kevin Alexand...	Done
	74	Socialización del uso de la consola	Kevin Alexand...	Done
3	69	F026 Pruebas en Cert Académico ESPE	Kevin Alexand...	Done
	75	Registro de Usuario Operador Cert Académico Ing Marco...	Kevin Alexand...	Done
	76	Verificación de políticas aplicadas para registro de activid...	Kevin Alexand...	Done
4	68	F025 Sprint Review	Kevin Alexand...	Done
	77	Reunión presencial Ing Walter Fuertes revisión	Kevin Alexand...	Done
	78	Reunión presencial Ing Marco Bonilla Operador Cert Aca...	Kevin Alexand...	Done

Nota. El gráfico representa las actividades generadas dentro del sprint 10

Design Science

Entorno

Para el desarrollo se tomaron en cuenta 2 entornos uno de administración a cargo del Cert Académico ESPE y otro en donde se realiza el despliegue del agente para el monitoreo como se describe a continuación

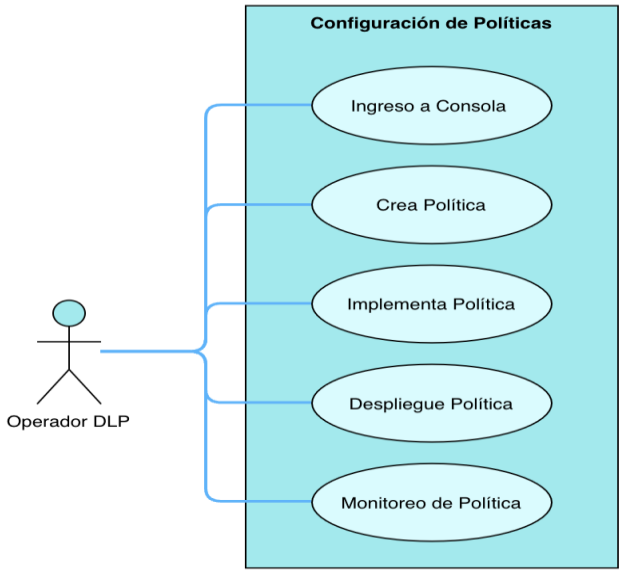
- Entorno de Administración: Se encuentra la consola de administración en donde se puede configurar reglas y agente

- Máquinas con agente: Son las maquinas terminales o endpoints en donde se realiza la instalación de un agente de comunicación mediante el cual se conecta con la máquina de administración.

Casos de Uso

Figura 19

Diagrama caso de uso configuración de políticas



Nota. El gráfico representa la interacción del actor con la interfaz de políticas

Tabla 3

Descripción caso de uso configuración de políticas DLP

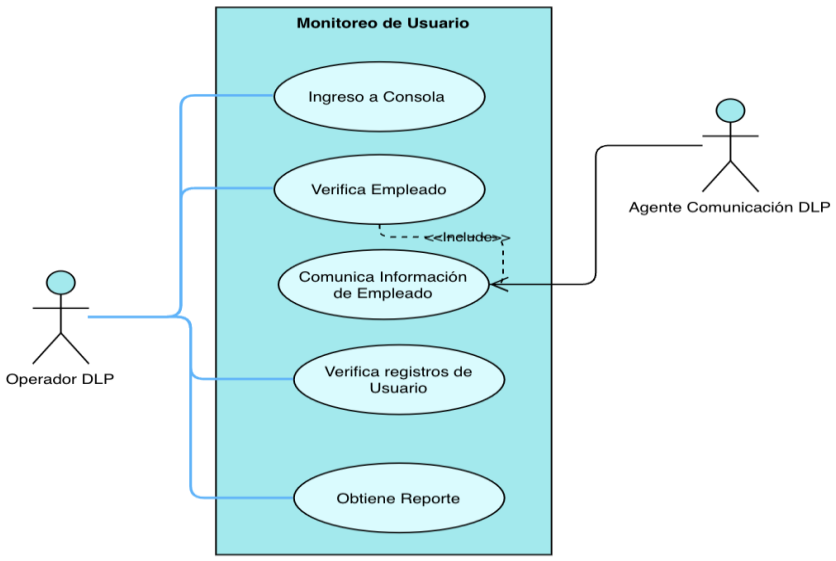
Caso de Uso	**Configuración de Políticas**
Autor	Kevin Quiroga
Objetivo	Configurar políticas nuevas para su implementación
Actores	Operador DLP
Flujo Normal	1. Iniciar Sesión en consola 2. Acceder al menú de comportamiento-políticas 3. Acceder a la opción de creación de política 4. Configurar las reglas 5. Implementar la política 6. Habilitar la política 7. Monitorear alerta de uso de

Caso de Uso	Configuración de Políticas
	política
Flujo Alternativo	
Precondiciones	Iniciar Sesión y permiso de administrador
Postcondiciones	Supervisar la aplicación de la política

Nota: Esta tabla muestra el desarrollo del caso de uso para la configuración de políticas

Figura 20

Diagrama caso de uso monitoreo de usuario



Nota. El gráfico representa la interacción del actor con la interfaz de monitoreo de usuario

Tabla 4

Descripción caso de uso monitoreo de usuario

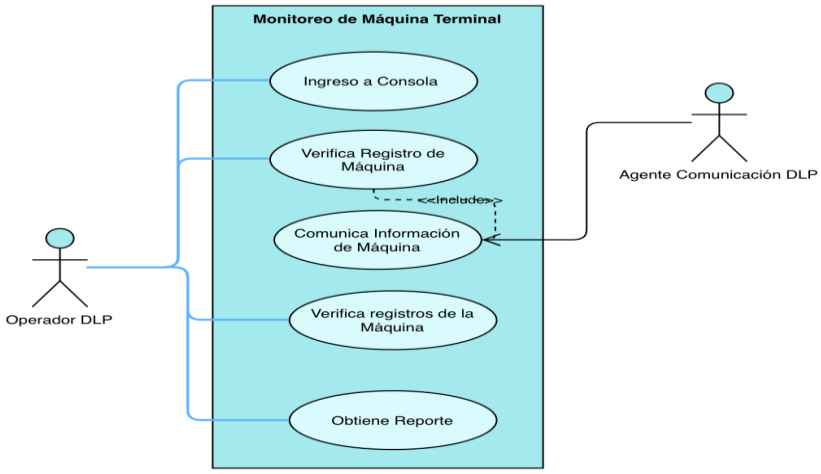
Caso de Uso	Monitoreo de Usuario
Autor	Kevin Quiroga
Objetivo	Monitorear el comportamiento del usuario
Actores	Operador DLP, Agente de comunicación dlp
Flujo Normal	1. Iniciar Sesión en consola 2. Acceder al menú de empleados

Caso de Uso	Monitoreo de Usuario
	3. Acceder al usuario determinado 4. Valida que el usuario sea correcto y este monitoreado 4.1. El agente de comunicación envía la información a la consola 5. Valida los registros del usuario en los logs 6. Obtiene reporte del usuario
Flujo Alternativo	1. Iniciar Sesión en consola 2. Acceder al menú de computadoras 3. Acceder a máquina donde el usuario haya iniciado sesión 4. Valida que el usuario sea correcto y este monitoreado 4.1. El agente de comunicación envía la información a la consola 5. Valida los registros del usuario en los logs 6. Obtiene reporte del usuario
Precondiciones	Iniciar Sesión y permiso de administrador
Postcondiciones	Revisar alertas y logs de usuario

Nota: Esta tabla muestra el desarrollo del caso de uso para el monitoreo de usuario

Figura 21

Diagrama caso de uso monitoreo máquina terminal



Nota. El gráfico representa la interacción del actor con la máquina terminal

Tabla 5

Descripción caso de uso monitoreo de máquina terminal

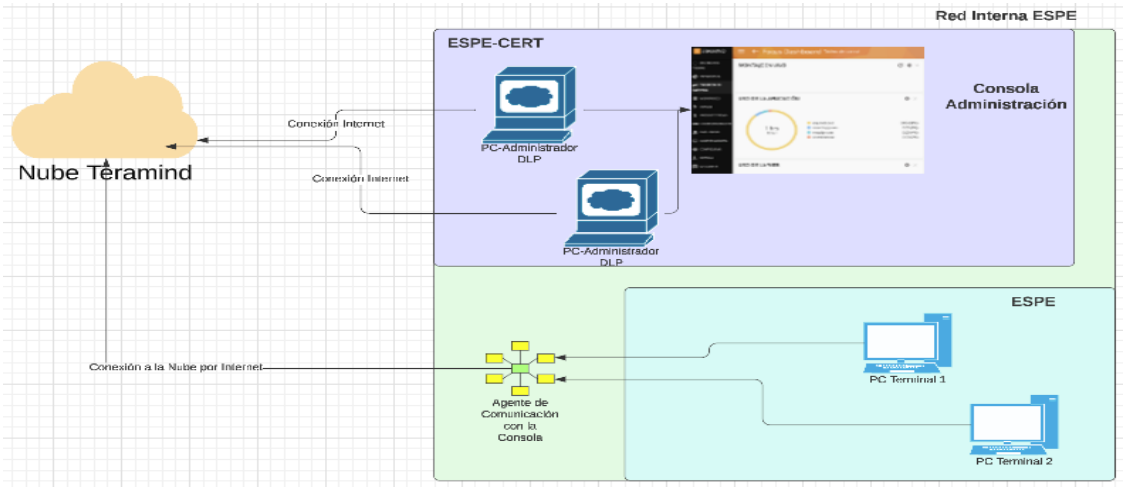
Caso de Uso	**Monitoreo de máquina terminal**
Autor	Kevin Quiroga
Objetivo	Monitorear el comportamiento del usuario en una maquina
Actores	Operador DLP, Agente de comunicación dlp
Flujo Normal	1. Iniciar Sesión en consola 2. Acceder al menú de computadoras 3. Acceder a máquina donde el usuario haya iniciado sesión 4. Valida que el usuario sea correcto y este monitoreado 4.1. El agente de comunicación envía la información a la consola 5. Valida los registros del usuario en los logs 6. Obtiene reporte del usuario
Flujo Alternativo	1. Iniciar Sesión en consola 2. Acceder al menú de empleados 3. Acceder al usuario determinado 4. Valida que el usuario sea correcto y este monitoreado 4.1. El agente de comunicación envía la información a la consola 5. Valida los registros del usuario en los logs 6. Obtiene reporte del usuario
Precondiciones	Iniciar Sesión y permiso de administrador
Postcondiciones	Revisar alertas y logs de usuario

Nota: Esta tabla muestra el desarrollo del caso de uso para el monitoreo de máquina terminal

Arquitectura y Diseño

Figura 22

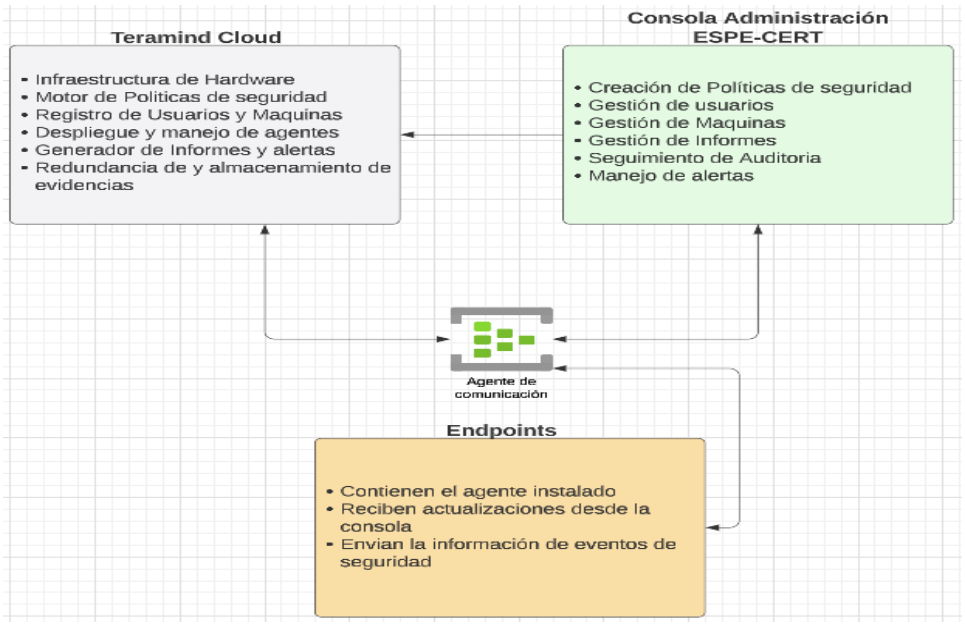
Diagrama de comunicación entre teramind con cert académico ESPE y máquinas terminales



Nota. El gráfico representa la conexión entre las máquinas terminales y la nube teramind que se encuentra en el internet

Figura 23

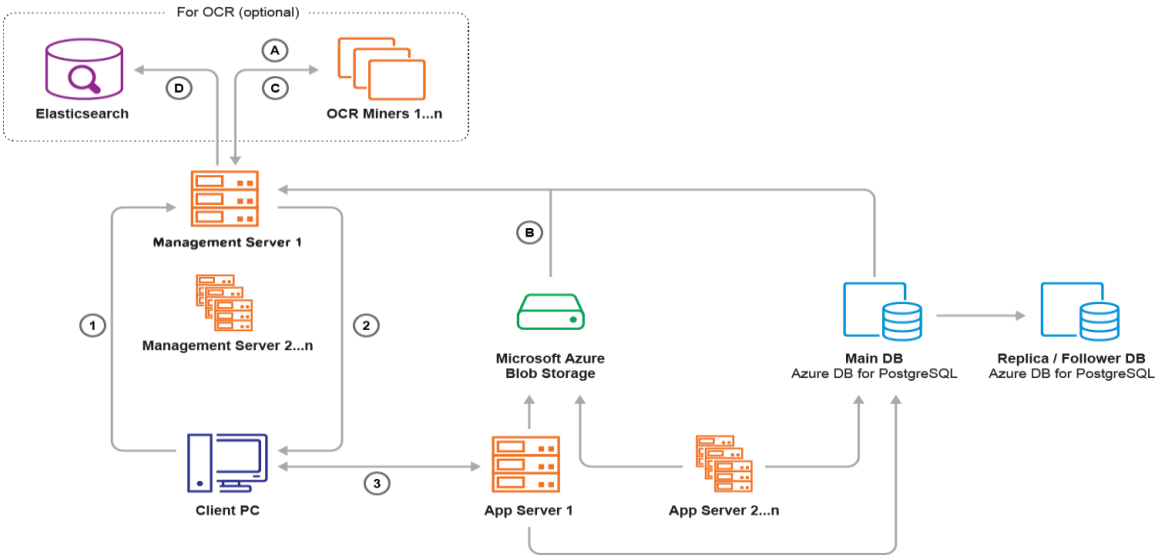
Nota conceptual



Nota. Explicación conceptual de la Figura 22

Figura 24

Diagrama de arquitectura despliegue teramind en azure



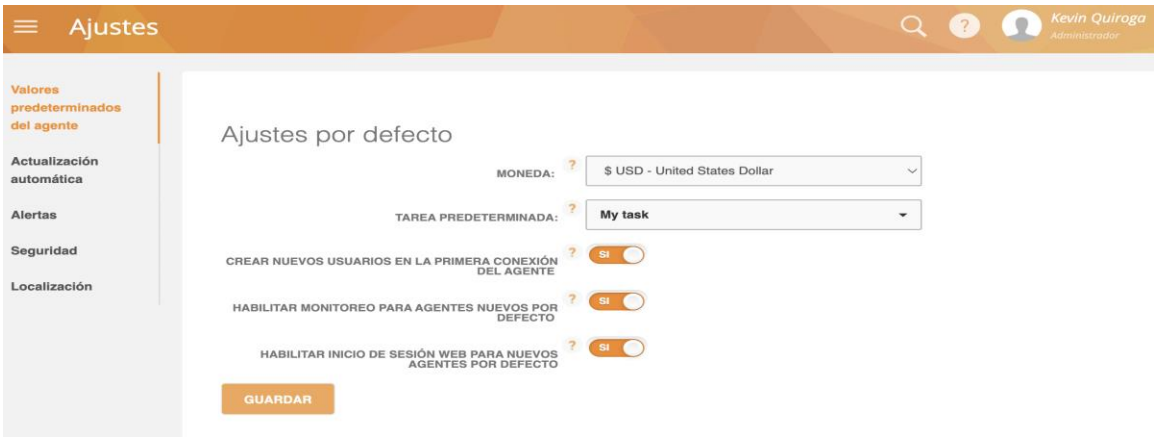
Nota. La figura representa el despliegue teramind en azure

Configuración

Configuración inicial consola de administración

Figura 25

Ajustes iniciales de la consola



Nota. El gráfico representa la consola con los ajustes iniciales

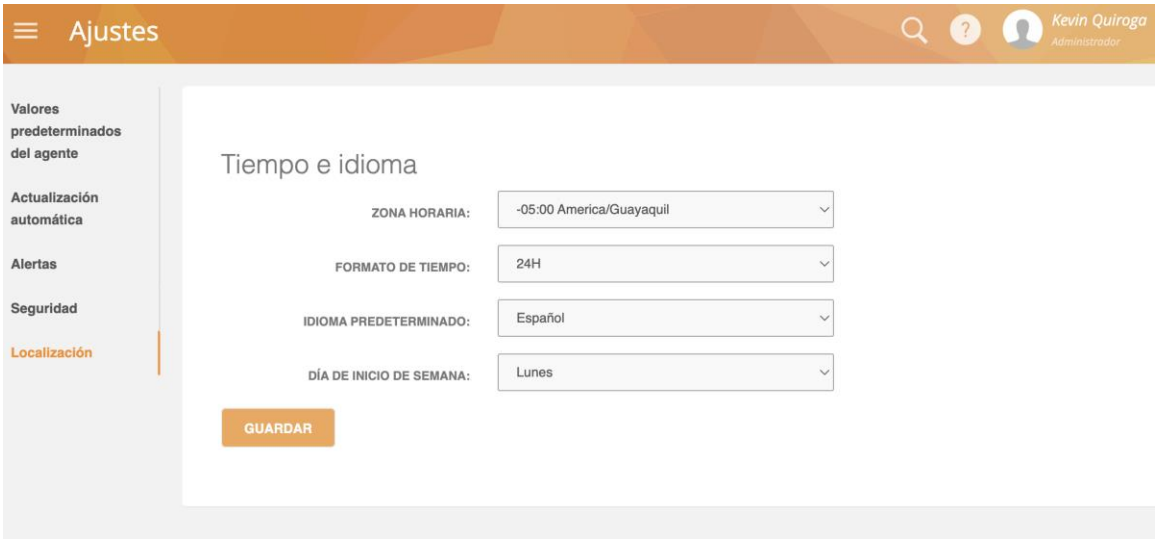
Figura 26

Ajustes de agente

Nota. El gráfico muestra el ajuste inicial del agente

Figura 27

Configuración regional



Nota. El gráfico muestra el ajuste inicial para la región de uso

Configuración inicial para despliegue de Agente

Figura 28

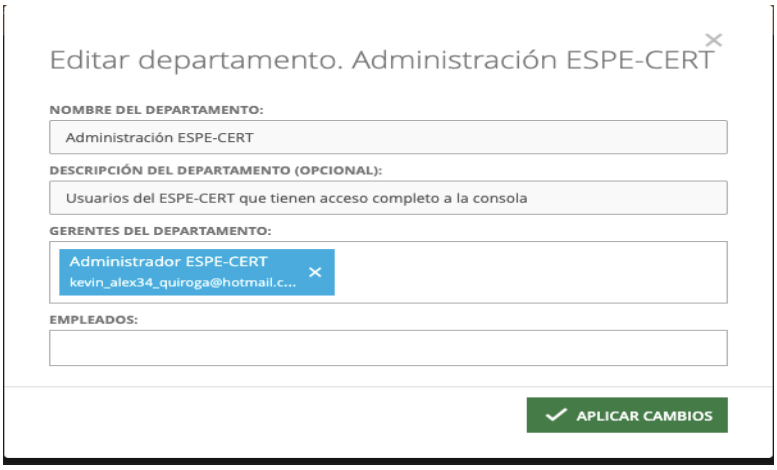
Configuración de tipo de agente

Nota. El gráfico muestra el ajuste del agente y sus variantes

Creación de departamento Administración Cert Académico Espe y el acceso de los usuarios para tener el seguimiento de su uso como se presenta en la Figura 29

Figura 29

Configuración inicial de Grupo



Nota. El gráfico muestra la creación del departamento de administración

Creación de usuarios Administración Cert Académico ESPE

Figura 30

Creación de usuario administrador controlador cert académico ESPE

Nota. El gráfico muestra la creación del usuario controlador

Capítulo IV

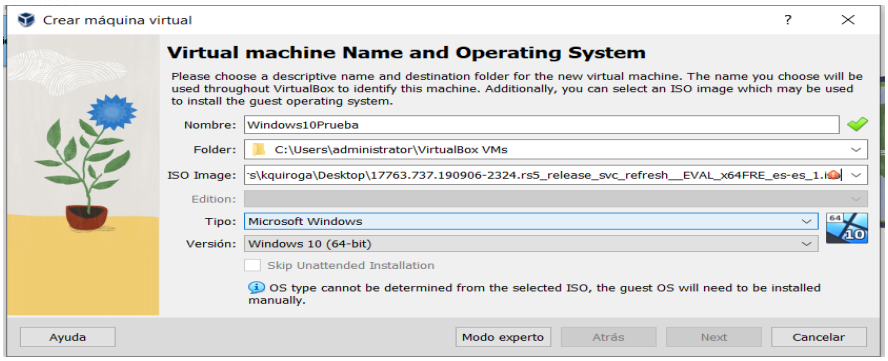
Evaluación

Despliegue Entorno Controlado

- Instalación de una máquina virtual en Virtual Box con Windows 10 Home, para la instalación de agente y prueba de políticas como se observa en la Figura 31.

Figura 31

Creación máquina virtual

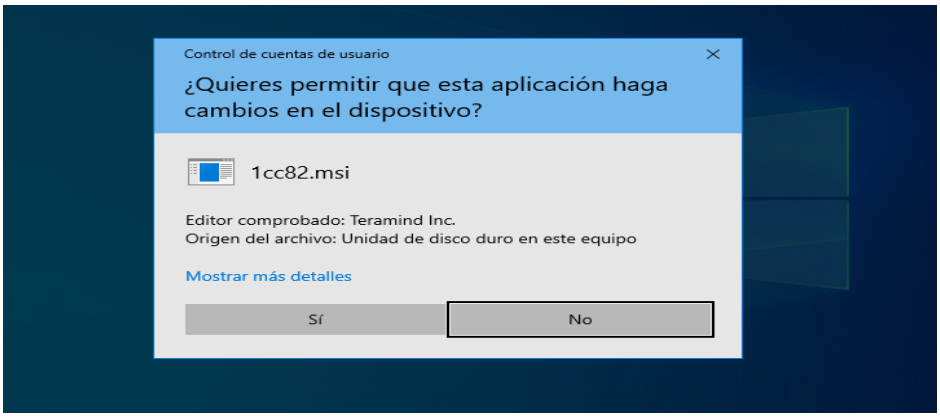


Nota. El gráfico muestra la configuración inicial de la máquina virtual

- Instalación de Agente de comunicación entre el equipo terminal y la consola de administración en la nube como se evidencia en la Figura 32

Figura 32

Instalación agente de comunicación

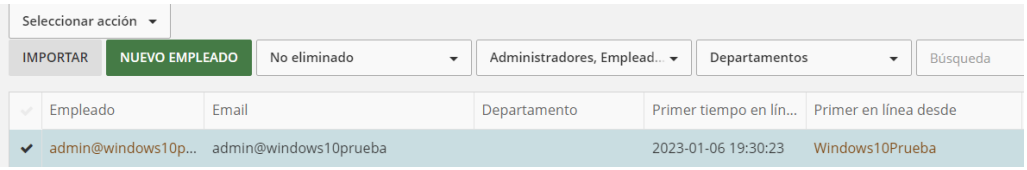


Nota. El gráfico muestra la instalación del agente en la maquina host

- Se valida el registro del usuario en la consola, en donde el nombre de usuario se registra seguido del nombre de la maquina donde se inició sesión véase Figura 33

Figura 33

Registro de usuario en la consola



Nota. El gráfico muestra el usuario creado en la consola de administración

- Se valida el registro de la maquina en la consola, en donde el nombre del computador lo toma desde el hostname de la máquina y la fecha de registro como se muestra en la Figura 34

Figura 34

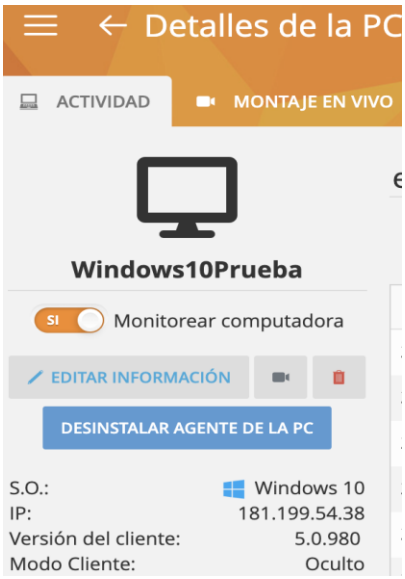
Registro de máquina en la consola

Nota. El gráfico muestra la máquina creada en la consola de administración

- Se realiza la verificación de las características de la máquina registrada y la opción de monitoreo activada para poder hacer el seguimiento como se muestra en la Figura 35.

Figura 35

Detalles del pc



Nota. El gráfico muestra las características de la máquina

- Se accede a la consola para la verificación de registros de actividad de la maquina a de más de confirmar si son las acciones realizadas en la máquina de prueba como se evidencia en la Figura 36.

Figura 36

Consola de actividad

Nota. El gráfico muestra los registros de actividad de la máquina

Políticas

ISO 27001

La tarea principal de la seguridad informática es minimizar el riesgo. En este caso, los riesgos provienen de muchas partes: la entrada de datos, el medio a través del cual se transfiere la información, el hardware utilizado para enviarla y recibirla, y el propio usuario. Implementado, pero la tarea principal siempre es minimizar el riesgo y lograr una seguridad cada vez mayor (ISO, 2021).

Como parte de la estrategia de seguridad, es útil seguir algunas pautas que le permiten fortalecer los procesos relacionados activos de información. Es por esto por lo que la norma ISO 27001: 2013 cumple con las especificaciones necesarias que aportan a la seguridad que se pretende ejercer con el sistema DLP (ISO, 2021).

Siguiendo las recomendaciones de la ISO 27001 se generan las siguientes políticas de monitoreo:

- Verificación de envío de correos a dominios distintos a @espe.edu.ec, en donde se registran en log solo los correos que se envían a un dominio externo como se puede observar en la figura 37 (registro) y figura 38 (descripción).

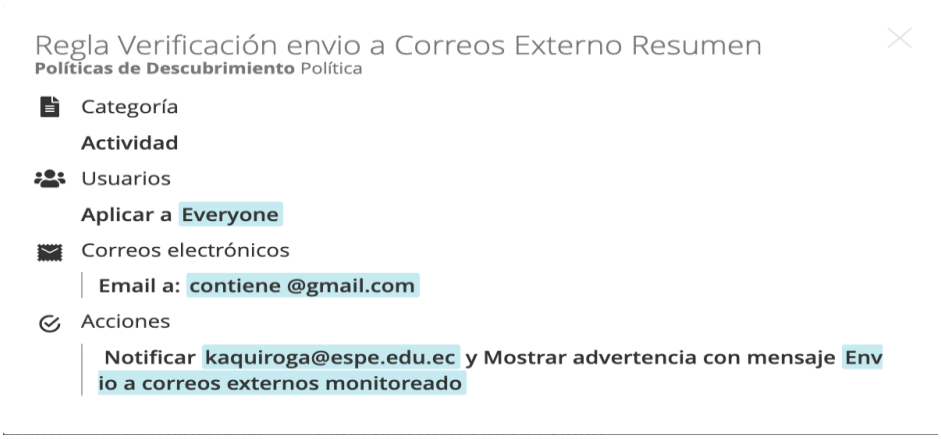
Figura 37

Registro de política verificación de envío a correos externos

Nota. El gráfico muestra el registro de la política en la consola

Figura 38

Descripción de regla envío a correos externos



Nota. El gráfico muestra la descripción completa de la regla creada

- Verificación si el cuerpo de correo contiene la palabra confidencial, mediante el cual se realiza un monitoreo a los correos que están siendo enviados y que en la redacción del cuerpo del correo tenga la palabra confidencial como se puede observar en la figura 39 (registro) y figura 40 (descripción).

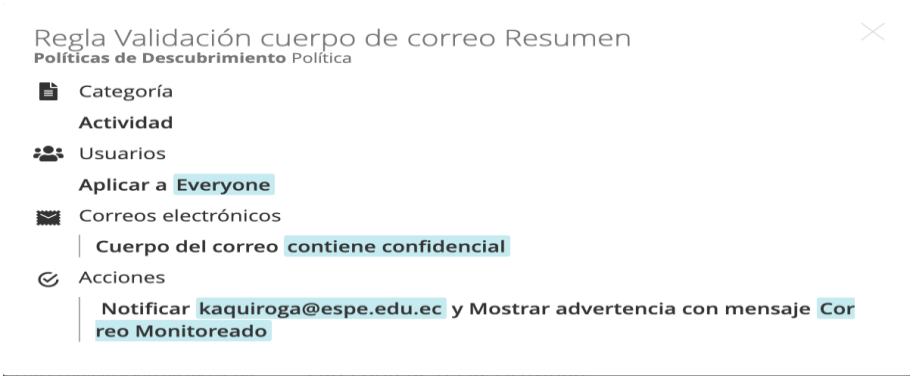
Figura 39

Registro de política verificación de envío a correos externos

Nota. El gráfico muestra el registro de la política en la consola

Figura 40

Descripción de regla envío a correos externos



Nota. El gráfico muestra la descripción completa de la regla creada

- Seguimiento a capturas de pantalla y herramienta de recortes en donde se registra el monitoreo y notificación como se observa en la figura 41 (registro) y figura 42 (descripción).

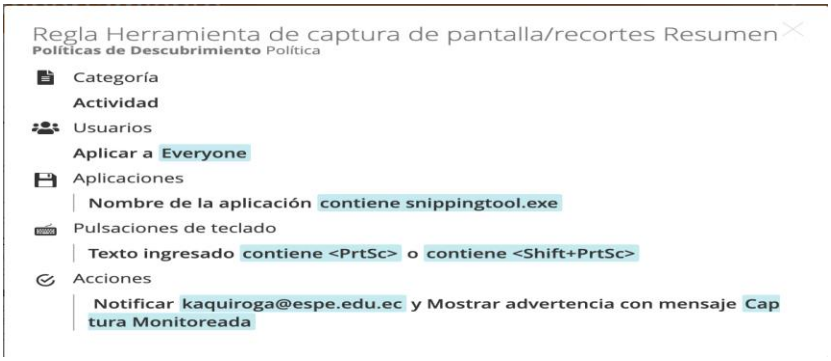
Figura 41

Registro de política herramienta de captura de pantalla

Nota. El gráfico muestra el registro de la política en la consola

Figura 42

Descripción de regla captura de pantalla



Nota. El gráfico muestra la descripción completa de la regla creada

- Regla para los archivos que se cargan a la nube donde se realiza el seguimiento y gestión como se observa en la figura 43 (registro) y figura 44 (descripción).

Figura 43

Registro de política subir archivos a la nube

Nota. El gráfico muestra el registro de la política en la consola

Figura 44

Descripción de regla subir archivos a la nube

Nota. El gráfico muestra la descripción completa de la regla creada

- Seguimiento a los archivos que se guardan en un medio extraíble y su almacenamiento como se observa en la figura 45 (registro) y figura 46 (descripción).

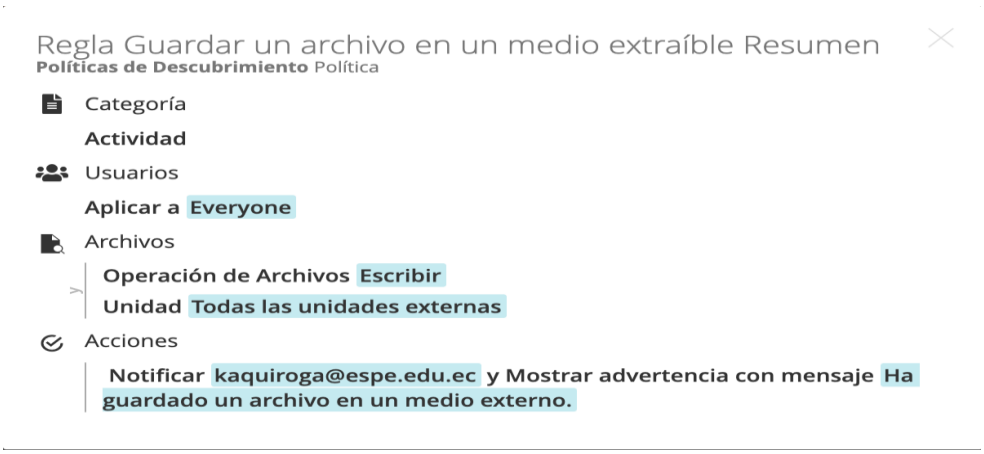
Figura 45

Registro de política guardar archivos en un medio extraíble

Nota. El gráfico muestra el registro de la política en la consola

Figura 46

Descripción de regla guardar archivos en un medio extraíble



Nota. El gráfico muestra la descripción completa de la regla creada

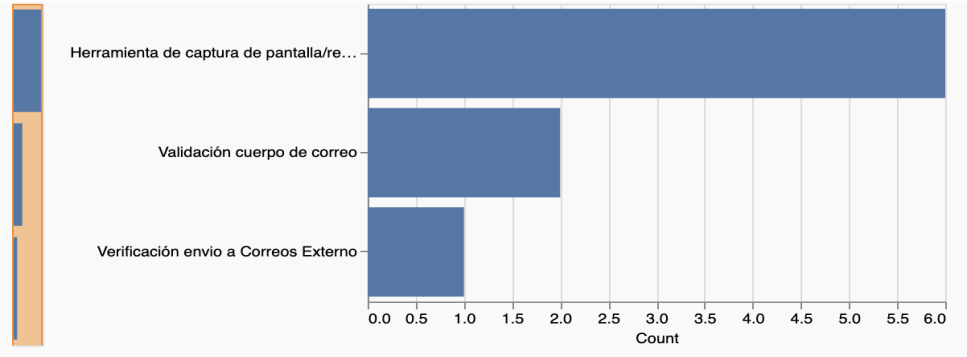
Evaluación de resultados Entorno Controlado

Los resultados obtenidos de las reglas de descubrimiento y administración de usuarios son los siguientes:

- Principales reglas de descubrimiento ejecutadas y resultados de los eventos generados sobre la máquina de prueba presentes en el diagrama de barras de la Figura 47

Figura 47

Diagrama de barras sobre eventos generados de las reglas aplicadas

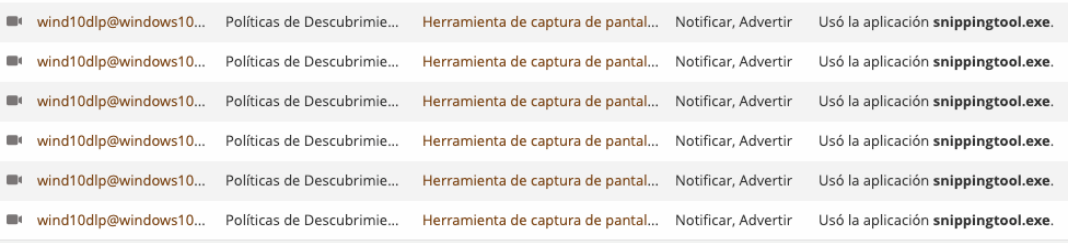


Nota. El gráfico muestra un diagrama de barras donde se hace un conteo de los eventos generados

- Monitoreo y registro de ejecuciones con resultados de los eventos generados sobre la máquina de prueba presentes en la consola de administración que se observan en la Figura 48.

Figura 48

Registro de eventos de captura de pantalla

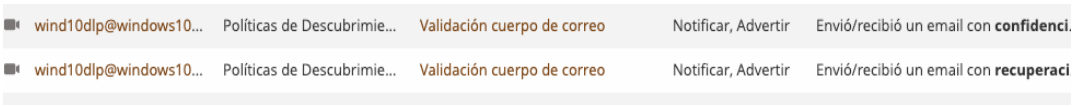


Nota. El gráfico muestra los eventos registrados en la consola sobre captura de pantalla

- Monitoreo validación cuerpo de correo electrónico con resultados de los eventos generados sobre la máquina de prueba presentes en la consola de administración que se observan en la Figura 49.

Figura 49

Registro de eventos de cuerpo correo electrónico

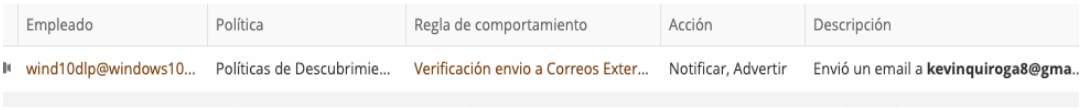


Nota. El gráfico muestra los eventos registrados en la consola sobre correo electrónico

- Monitoreo validación de envío correos externos con resultados de los eventos generados sobre la máquina de prueba presentes en la consola de administración que se observan en la Figura 50.

Figura 50

Registro de evento correos externos

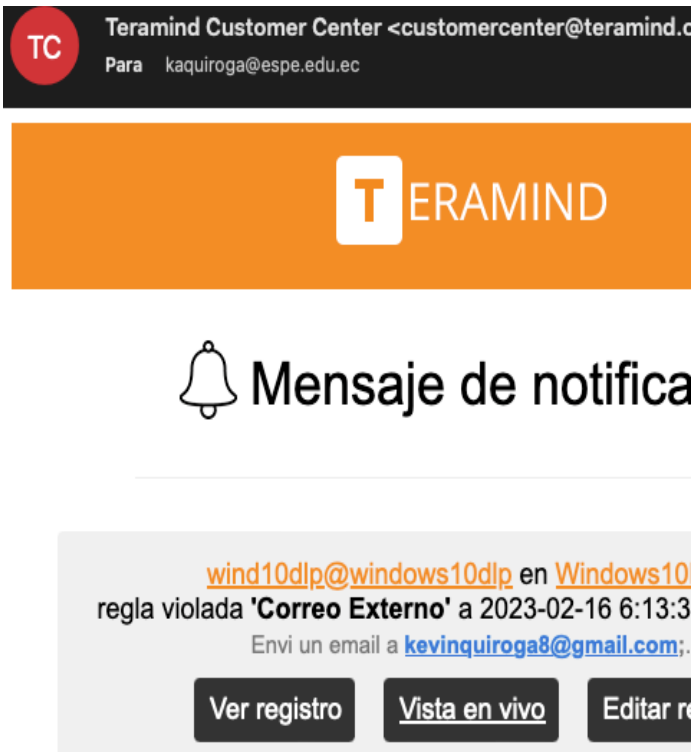


Nota. El gráfico muestra los eventos registrados en la consola sobre correo electrónico externo

- Verificación correos electrónico con la notificación de alerta de incidente de seguridad generado en la máquina de prueba que se evidencia en la Figura 51.

Figura 51

Envío de correo de notificación de incidente



Nota. El gráfico muestra la notificación de incidente enviada por correo

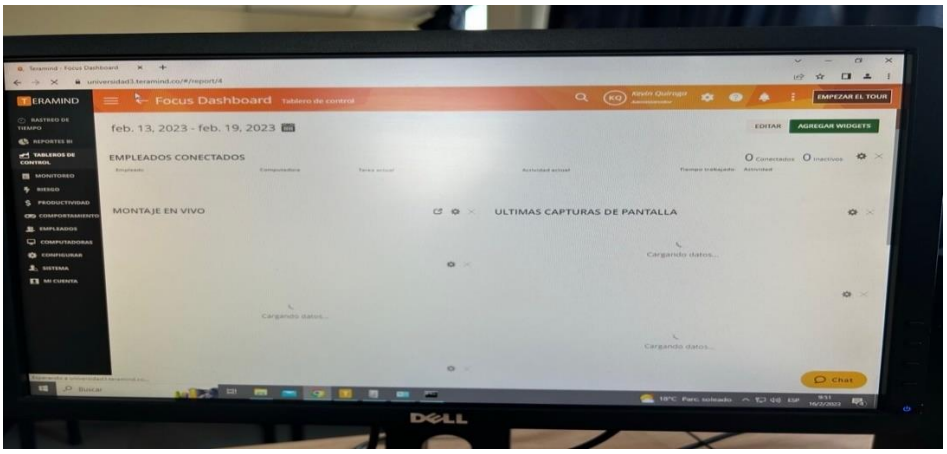
Despliegue Cert Académico ESPE

Entorno Cert Académico ESPE: Se realiza el despliegue en las máquinas para el monitoreo donde se realizan las siguientes actividades:

- Validación de acceso a consola maquina Operador Espe1 donde se accede a la consola mediante un enlace directo en el navegador de internet como se muestra en la Figura 52.

Figura 52

Acceso a consola desde operador Espe1

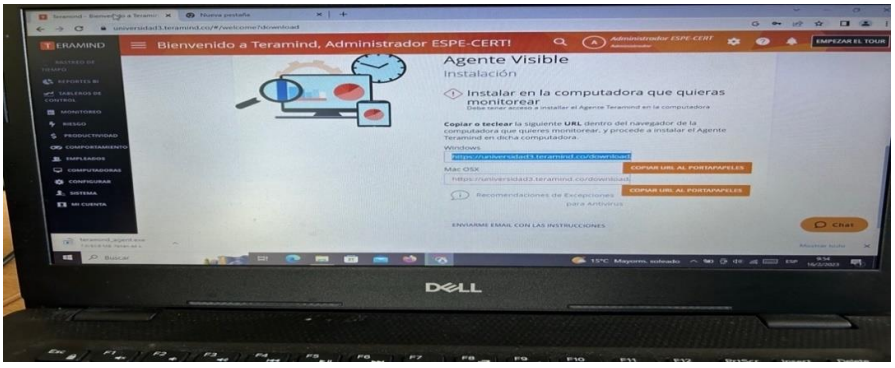


Nota. El gráfico muestra el acceso a la consola en la máquina del operador en el laboratorio

- Validación de acceso a consola maquina Operador Espe2, el acceso se lo realiza mediante un navegador web con el usuario y contraseña generado como se evidencia en la Figura 53.

Figura 53

Acceso a consola desde operador Espe2

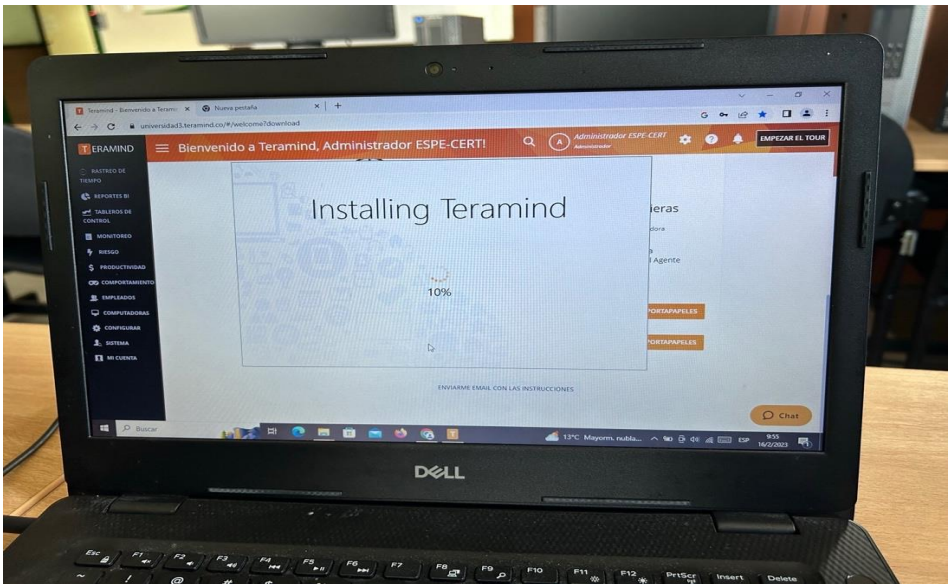


Nota. El gráfico muestra el acceso a la consola en la máquina del operador en el laboratorio

- Instalación de agente en maquina operador del Cert Académico ESPE para probar la conectividad de la consola de administración con una maquina en la red de la ESPE como se evidencia en la Figura 54.

Figura 54

Instalación de agente en máquina operador



Nota. El gráfico muestra la instalación del agente en la máquina del operador

- Validación de registro del usuario en la consola de la maquina operador con el usuario host que se inició sesión como se observa en la Figura 55.

Figura 55

Consola de administración de pc

Empleado	Email	Departamento	Primer tiempo en lín...	Primer en línea desde
usuario@espe04	usuario@espe04		2023-02-16 10:07:27	espe04

Nota. El gráfico muestra la creación de la máquina del operador en la consola

- Verificación de la información del registro de la Pc del operador Espe2 además de las características y el monitoreo que se evidencia en la Figura 56.

Figura 56

Características pc operador Espe

Nota. El gráfico muestra las características de la máquina del operador

Capítulo V

Conclusiones y recomendaciones

Conclusiones

- Con los datos de prueba obtenidos, se determinó que las políticas de descubrimiento implementadas alertaron el comportamiento del usuario.
- Con el despliegue en el Cert Académico ESPE se logró identificar que la conexión del agente dentro de la red Espe necesita de permiso de comunicación mediante Firewall

- Se detecto que hay un uso frecuente de la herramienta de captura de pantalla a de más de envío de correos fuera del dominio @espe.edu.ec
- Con la información recolectada se genera tableros y reportes para el manejo de los operadores del Cert Académico ESPE

Recomendaciones

- Se recomienda tener un control y seguimiento de las alertas que se generan dentro de la herramienta a fin de que se pueda realizar un análisis de los registros obtenidos.
- Para la comunicación correcta del agente con la consola se recomienda revisar la conectividad de las maquinas terminales a la siguiente dirección y puerto: 141.144.250.131:32600
- Se recomienda analizar el uso de herramientas de recorte o de captura de pantalla para poder mitigar la captura de contenido sensible además de los destinatarios de correo electrónico
- Se recomienda generar reportes semanales para dar un correcto seguimiento de los incidentes de seguridad

Bibliografía

Abrams, R. y. (2018). Data Loss Prevention. O'Reilly Media, Inc.

Al-Kilani, H. N. (2019). Data exfiltration techniques and data loss prevention system. 2019 International Arab Conference on Information Technology (ACIT), págs. 124-127. doi:https://doi.org/10.1109/ACIT47987.2019.8991131

Alsuwaie, M. A. (2021). Data leakage prevention adoption model & DLP maturity level assessment. 2021 International Symposium on Computer Science and Intelligent Controls (ISCSIC), págs. 396-405. doi:https://doi.org/10.1109/ISCSIC54682.2021.00077

Bass, L. (2018). Data Loss Prevention: A Comprehensive Guide. Syngress.

CISA. (2019). Cybersecurity and Infrastructure Security Agency. Obtenido de https://www.cisa.gov/information-security-policy-and-guidance

COBIT. (2019). Objetivos de Control para las Tecnologías de la Información y Relacionadas. Obtenido de https://www.isaca.org/cobit

COBIT. (2020). COBIT 2019: IT Governance Framework.

Cybersecurity, J. o. (2020). Effective incident response: A review of incident response frameworks and best practices. Obtenido de https://cybersecurity.jmir.org/2020/3/e12361/

Forrester. (2019). The Forrester Wave™: Security Policy Management, Q4 2019. Obtenido de https://www.forrester.com/report/The+Forrester+Wave+Security+Policy+Management+Q4+2019/-/E-RES146896

Gartner. (2019). Gartner's 2019 Magic Quadrant for Data Loss Prevention. Obtenido de https://www.gartner.com/en/documents/3947717

Hevner, A. (2007). A Three Cycle View of Design Science Research. Scandinavian Journal of Information Systems, 19(2), 87-92.

IDC. (2019). Worldwide Data Loss Prevention Software Market Shares, 2018: Vendor Shares and Market Forecast. Obtenido de https://www.idc.com/getdoc.jsp?containerId=US44952419

International Organization for Standardization, &. I. (2013). Information technology - Security techniques - Information security management systems - Requirements (ISO/IEC 27001:2013). Geneva, Switzerland: ISO/IEC.

ISACA. (2019). Data Governance and Classification. Obtenido de https://www.isaca.org/resources/research/researchdeliverables/2019/data-governance-and-classification

ISACA. (2019). The Importance of Risk Assessment in Cybersecurity. Obtenido de https://www.isaca.org/resources/research/researchdeliverables/2019/the-importance-of-risk-assessment-in-cybersecurity

ISO. (2018). ISO/IEC 27001:2013. Obtenido de https://www.iso.org/standard/64599.html

ISO. (2018). ISO/IEC 27032: Information technology - Security techniques - Guidelines for cyber security incident management.

ISO. (2020). ISO/IEC 27001: Information technology - Security techniques - Information security management systems - Requirements.

ISO. (2021). Evaluación de Riesgos de Seguridad de la Información. Obtenido de https://normaiso27001.es/operacion-en-iso-27001/#h2

McAfee. (2019). A Framework for Data Governance and Classification. Obtenido de https://www.mcafee.com/es/resources/white-papers/wp-data-governance-classification.pdf

Miloslavskaya, N. M. (2017). DLP as an integral part of network security intelligence center. 2017 IEEE 5th International Conference on Future Internet of Things and Cloud (FiCloud), (págs. 297-304). doi:https://doi.org/10.1109/FiCloud.2017.15

NIST. (2020). Cybersecurity Framework. Obtenido de https://www.nist.gov/cyberframework

NIST. (2020). Guide for Conducting Risk Management Framework (RMF) for Information Systems and Organizations.

PwC. (2019). Protecting your assets: A guide to building a cyber security framework. Obtenido de https://www.pwc.com/gx/en/services/cyber-security/cyber-security-framework.html

Schwaber, K. &. (2020). Guía de Scrum: La guía definitiva de Scrum: Las reglas del juego.

Symantec. (2017). Symantec DLP Report. Obtenido de https://www.symantec.com/content/dam/symantec/docs/reports/dlp-report-2017-en.pdf

Valladares, P. F. (2017). Dimensional data model for early alerts of malicious activities in a CSIRT. doi:https://doi.org/10.23919/SPECTS.2017.8046771