OFICINA DE POSGRADOS

Tema:

SISTEMA DE CIFRADO PARA COMPUTADORES PORTÁTILES EN INSTITUCIÓNES PÚBLICAS ECUATORIANAS

Proyecto de Investigación y Desarrollo previo a la obtención del título de Magister en Ciberseguridad

Línea de Investigación:

Protección de datos y comunicaciones, seguridad de la información

Autor:

Ing. Juan Roberto Sandoval Perugachi

Director:

Ing. Santiago Alejandro Acurio Maldonado, Mg.

Ambato – Ecuador

Noviembre 2021

PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR

SEDE AMBATO

HOJA DE APROBACIÓN

Tema:

SISTEMA DE CIFRADO PARA COMPUTADORES PORTÁTILES EN INSTITUCIÓNES PÚBLICAS ECUATORIANAS

Línea de Investigación:

Protección de datos y comunicaciones, seguridad de la información

Autor:

Juan Roberto Sandoval Perugachi

Santiago Alejandro Acurio Maldonado, Mg. f._____

CALIFICADOR

Alberto Leopoldo Arellano Aucancela, Mg. f._____

CALIFICADOR

José Marcelo Balseca Manzano, Mg. f._____

CALIFICADOR

Juan Carlos Acosta, Padre, PhD. f._____

COORDINADOR DE LA OFICINA DE POSGRADOS

Hugo Rogelio Altamirano Villarroel, Dr. f._____

SECRETARIO GENERAL PUCESA

Ambato – Ecuador

Noviembre 2021

DECLARACIÓN DE AUTENCIDAD Y RESPONSABILIDAD

Yo: **JUAN ROBERTO SANDOVAL PERUGACHI,** con CC. **171927064-5** autor del trabajo de graduación intitulado: "SISTEMA DE CIFRADO PARA COMPUTADORES PORTÁTILES EN INSTITUCIÓNES PÚBLICAS ECUATORIANAS", previa a la obtención del título profesional en **MAGISTER EN CIBERSEGURIDAD,** en la **OFICINA DE POSGRADOS.**

1. Declaro tener pleno conocimiento de la obligación que tiene la Pontificia Universidad Católica del Ecuador, de conformidad con el artículo 144 de la Ley Orgánica de Educación Superior, de entregar a la SENESCYT en formato digital una copia del referido trabajo de graduación para que sea integrado al Sistema Nacional de Información de la Educación Superior del Ecuador para su difusión pública respetando los derechos de autor.
2. Autorizo a la Pontificia Universidad Católica del Ecuador a difundir a través de sitio web de la Biblioteca de la PUCE Ambato, el referido trabajo de graduación, respetando las políticas de propiedad intelectual de Universidad

Ambato, noviembre 2021

JUAN ROBERTO SANDOVAL PERUGACHI

CC. 171927064-5

AGRADECIMIENTO

A Dios por guiar mi camino. A la Pontificia Universidad Católica Sede Ambato. A mis profesores, en especial al Ing. Santiago Acurio, quien me apoyo con su profesionalismo y experiencia para realizar el presente trabajo de titulación.

DEDICATORIA

A mi pequeña gran familia.

RESUMEN

Debido a los acontecimientos actuales que el mundo atraviesa, las instituciones públicas del país, se han visto obligadas a realizar teletrabajo parcial o permanente. Para esto, los funcionarios utilizan computadores de escritorio y portátiles, lo cual, ocasiona la exposición de los dispositivos a un alto riesgo de fuga de información por pérdida o robo. Con este antecedente, el presente proyecto consiste en implementar un sistema de cifrado disco completo en computadores portátiles en una institución pública y dar cumplimiento al control criptográfico de protección de datos sensibles manipulados en dispositivos móviles, actividad establecida en el Esquema Gubernamental de Seguridad de la Información (EGSI). El desarrollo del proyecto tiene un enfoque cualitativo; además, se hace uso de las metodologías tipo cualitativo, descriptivo y explicativo, utilizados para el levantamiento de información, se establecen las características del sistema de cifrado según las necesidades de la institución y la generación de la documentación técnica. Los resultados obtenidos demuestran que el software antivirus con el que cuenta la institución, cumple con los parámetros técnicos necesarios para la implementación del sistema de cifrado; por otra parte, se mitiga la fuga de información, esta, se mantiene ilegible y no ser utilizada por personal no autorizado.

Palabras clave: Cifrado, Encriptación, Cifrado de disco completo, Seguridad de la información, Esquema Gubernamental de Seguridad de la Información, Fuga de información, Integridad, Confidencialidad.

ABSTRACT

Due to the current worldwide events, the country's public institutions have been forced to carry out a partial or permanent tele-working system. The government officials use desktops and laptop computers, which causes the exposure of these devices to a high risk of information leakage due to loss or theft. With this background, this project consists on the implementation of a full hard-disk encryption system on laptops in a public institution and complying with the cryptographic control of protection of sensitive data manipulated on mobile devices, which is an established activity in the Government Information Security Schetch (EGSI). The development of the project has a qualitative approach; In addition, the use of the qualitative, descriptive and explanatory methodologies are being used to collect the information, characteristics of the encryption system are established according to the needs of the institution and the generation of technical documentation. The obtained result show that the institution‘s antivirus software, complies with the necessary technical parameters for the implementation of the encryption system; on the other hand, information leakage is mitigated, it, remains illegible and cannot be used by unauthorized personnel.

Keywords: encryption, full Disk encryption, information security, Government Information Security Scheme, information leakage, integrity, confidentiality.

ÍNDICE

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

INTRODUCCIÓN

Como parte del proceso de implementación del Esquema Gubernamental de Seguridad de la Información en las instituciones públicas que insta a cumplir normas internacionales de seguridad como la ISO 27001, que establece en uno de sus controles la implementación del cifrado de información en tránsito[1].

La institución[2] seleccionada para la investigación, maneja y procesa información confidencial, como parte de los productos que genera, los mismos que son procesados a nivel de servidores, sin embargo, productos intermedios (levantamiento de información) son elaborados directamente en los equipos de usuario final, lo cual, produce una brecha de seguridad; el personal que utiliza computadores portátiles es vulnerable a la sustracción de los equipos, cuando se moviliza fuera de la institución.

A partir del año 2020, la institución entró a un proceso de transparencia y de liberalización de bases de datos para entregar al país cifras de calidad, de manera adecuada y oportuna. Para esto la institución ha implementado portales y servidores proveedores de información de las encuestas realizadas para garantizar la disponibilidad de este servicio. Así como, también, ha efectuado mecanismos didácticos de difusión estadística y segmentación de la información.

Desde el año 2013, la institución, se planteó nuevos desafíos, entre los, cuales, se destaca el de convertirse en un referente a nivel nacional e internacional en la generación de estudios, documentos de análisis e investigaciones científicas, que permitan mejorar el diagnóstico, evaluación y diseño de políticas públicas y que provean información oportuna y de calidad para la toma de decisiones de entes públicos y privados.

[1] Información en tránsito: se transfiere a través de cables y transmisión inalámbrica a otras ubicaciones dentro o entre sistemas informáticos. Estos datos viajan a través de una red y estos son leídos, actualizados y procesados.
[2] Por motivos de confidencialidad de la información, se reserva el nombre de la institución.

Durante este tiempo el equipo de investigadores de la institución, se ha consolidado, al obtener resultados concretos, los, cuales, se han plasmado en las publicaciones realizadas a través de sus diversas líneas editoriales.

El 19 de septiembre de 2003, se emitió el Acuerdo Ministerial No. 166 publicado mediante Registro Oficial No. 88 del 25 de septiembre de 2013, que dispone la implementación del Esquema Gubernamental de Seguridad de la Información (EGSI), basado en las Normas Técnicas Ecuatorianas NTE INEN ISO/IEC 27000, las cuales, contienen las directrices para la implementación de Sistemas Gestión de Seguridad de la Información, en las entidades públicas dependientes de la función ejecutiva en concordancia con el Plan Nacional de Gobierno Electrónico 2014-2017 del Ecuador, refuerza, de esta forma el principio de garantizar la seguridad y confianza y como parte del Plan Estratégico de Seguridad y Protección de datos.

El establecimiento e implementación del Esquema Gubernamental de Seguridad (EGSI) de la Información, están influenciados por las necesidades y objetivos de la institución, los requisitos de seguridad, los procesos utilizados, el tamaño su estructura. El EGSI ayuda a preservar la privacidad, integridad y disponibilidad de datos sensibles por medio de un proceso que gestiona los riesgos a los, cuales, se encuentra expuesta la información, además, proporciona una serie de controles para solventar vulnerabilidades encontradas.

El EGSI es un instrumento de vital importancia para todos los actores del plan nacional: ciudadanos, servidores, empresas, gobierno y otros actores del estado; con su implementación, se busca preservar el activo más importante del Estado Ecuatoriano, la información.

La Organización Internacional de Normalización (ISO) y la Comisión Electrotécnica Internacional (IEC) forman un sistema especializado para la normalización a nivel mundial. El Comité Técnico Conjunto 1 (JTC1), es el encargado de desarrollar, mantener y promover el uso de estándares en el campo de la Tecnología e Información (TI) y la Tecnología de la Información y Comunicación (TIC).

El estándar ISO/IEC 27001 es una norma internacional de Seguridad de la Información que pretende asegurar la confidencialidad, integridad y disponibilidad de la información de una organización y de los sistemas y aplicaciones que la tratan.

En la actualidad tanto usuarios como grandes corporaciones a nivel mundial usan ampliamente el cifrado de equipos informáticos para proteger sus datos confidenciales. Manejar adecuadamente la información, hace que los usuarios no sufran las consecuencias de un ataque, se tiene en cuenta que el tema de privacidad de las comunicaciones está en pleno debata internacional, el concepto de cifrado, se popularizo como una forma de mantener la información segura.

El nivel de movilización de los computadores portátiles fuera de la institución es alto; existe personal administrativo y operativo que recopila información en campo, y existen varios mecanismos de entrega. En ciertas ocasiones cuando la sincronización del equipo cliente con el servidor no es posible por falta de cobertura de los servicios de internet a nivel nacional, la información reposa en los equipos hasta, que se realice la transferencia de datos.

La institución cuenta con un parque informático considerable, aproximadamente 900 equipos, de estos, el 30% son computadores portátiles, el nivel de movilidad fuera de la institución es permanente, esto, genera el riesgo potencial de pérdida de información sensible.

Los datos, que se manejan dentro la institución tiene gran interés para los ciudadanos ecuatorianos, sin embargo, la información, que se presenta en los trámites no siempre es de orden público, sino más bien, mantenerse en recaudo para no atentar a los derechos de los usuarios. La información sensible, no se exhibe abiertamente en los equipos móviles; que al salir de la cobertura de seguridad que ofrece físicamente las redes internas de datos de la institución, se mantienen expuestos a las redes públicas que ofertan otros proveedores de servicios de conexión.

En este contexto, el problema científico, se expresa de la siguiente forma:

¿Cómo proteger la información confidencial de los computadores portátiles de las instituciones públicas?

El objetivo general de este trabajo de investigación es: Implementar un sistema de cifrado para computadores portátiles en una Institución Pública Ecuatoriana.

Para el cumplimiento del objetivo principal, se han propuesto los siguientes objetivos específicos:

1. Fundamentar teóricamente los sistemas de cifrado a ser utilizados en las empresas públicas ecuatorianas.
2. Diagnosticar la información del estado actual de los activos de información y hardware de computadores portátiles.
3. Implementar el sistema de cifrado de información en los computadores portátiles correspondientes a la ciudad de Quito, acorde a cronograma establecido con las autoridades de la institución.
4. Generar la documentación normativa y operativa que permita su implementación a nivel nacional.

Se toma en consideración que la institución cuenta con un software implementado para la seguridad de su parque informático, se utiliza la herramienta de cifrado incluida en este para la implementación del sistema de cifrado.

La herramienta de cifrado, se integra con un servidor de directorio activo existente, cuenta son gestión centralizada de todos los dispositivos administrados, con capacidad de integración de nuevos complementos para reforzar la protección de la información de la institución.

Para la implementación del control criptográfico establecido en el Esquema Gubernamental de Seguridad de la Información (EGSI), se adopta una metodología lineal.

Al implementar esta solución de cifrado, se mitiga la fuga de información contenida en los computadores portátiles de la institución y, se garantiza que esta sea accedida

solo por personal autorizado, adicional, los datos contenidos en los discos duros, se mantienen ilegibles para personal no autorizado y no serán usados para otros fines.

Se elabora la documentación necesaria para la implementación del Sistema de Cifrado a nivel nacional.

CAPÍTULO I. ESTADO DEL ARTE Y LA PRÁCTICA

1.1 Sistemas de cifrado

Explican Medina Vargas y Miranda Mendez (2015), el origen de los sistemas de cifrado, se remonta a los orígenes del hombre desde que aprendió a comunicarse. Desde entonces, tuvo que encontrar medios para asegurar la confidencialidad de una parte de su comunicación. El principio básico de la criptografía, es mantener una comunicación entre dos personas de forma que sea incomprensible para el resto.

INCIBE (2015), indica, la criptografía consiste en ofuscar la información por medio de técnicas de codificación, se evita así que los datos sean legibles para cualquier persona que desconozca la clave de decodificación. Esta técnica, es la mejor opción para la transmisión y almacenamiento de información confidencial en dispositivos móviles.

Uno de los primeros mecanismos de seguridad de la información, es el uso de las claves o contraseñas; que son mezclas de símbolos (números, letras, signos de puntuación, entre otros), esto hace que los delincuentes informáticos realicen ataques de fuerza bruta para identificar las posibles combinaciones de símbolos hasta encontrar la clave correcta. Vanegas Lopez (2018), recomienda tomar las siguientes medidas para evitar este tipo de ataques:

- **Utilizar Claves de longitud extensa:** de 512 bytes a 4096 bytes, esto hace que el atacante requiera gran cantidad de recursos informáticos, para encontrar la clave correcta con rapidez.
- **Cambiar la clave con regularidad:** así, se limita el tiempo del atacante, la contraseña está en constante cambio.
- **Usar la mayor cantidad de caracteres:** con esto, la clave, se vuelve difícil de encontrar, está compuesta de letras, números, letras y caracteres especiales.
- **No utilizar palabras predecibles:** como nombres propios o de mascotas, palabras del diccionario, fechas, entre otras.

- **Detectar intentos fallidos en intervalos cortos de tiempo:** por ejemplo, el teléfono celular, se bloquea por un lapso al ingresar un PIN incorrecto tres veces consecutivas. (Vanegas López 2018)

Por su parte, Héctor Corrales Sánchez (2012), señala, las empresas necesitan mantener sus comunicaciones seguras para proteger su información, además, es necesario brindar privacidad y seguridad a las personas. Con el surgimiento del Internet y la oferta masiva de servicios en línea como acceso a entidades financieras, citas médicas, entre otras, se ofrecerán confidencialidad y seguridad a estos servicios.

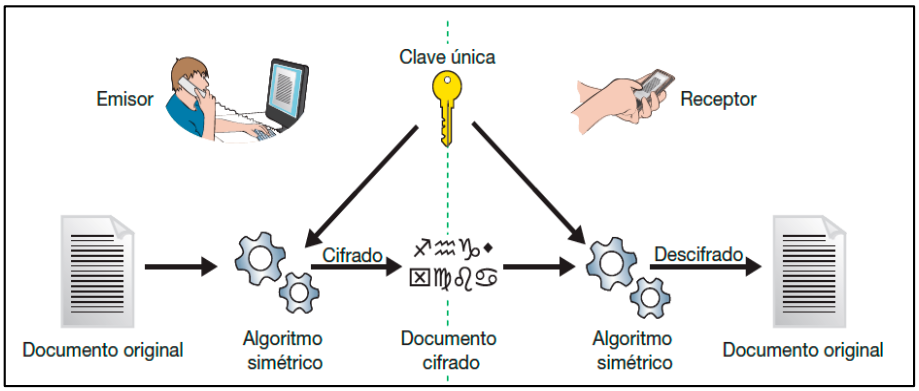
MINTEL (2013) detalla los cuatro requisitos u objetivos básicos que la criptografía ofrece:

- **Privacidad o confidencialidad:** solo acceden a la información aquellas personas que estén autorizadas a obtenerla.
- **Integridad:** el receptor del mensaje, es capaz de comprobar que este no ha sido modificado durante su camino.
- **Autenticación:** cuando, se establece una comunicación segura entre emisor y receptor, cada uno tiene la posibilidad de verificar la identidad de la otra parte de manera irrefutable.

No repudio: los participantes de la comunicación no serán capaces de negar que recibieron o transmitieron una determinada información, existen pruebas de envío.

Uno de los primeros mecanismos utilizados para mantener la información cifrada, es la criptografía simétrica. Este mecanismo utiliza una sola clave para el proceso de cifrado y descifrado. Es bastante eficientes, pues, consume pocos recursos computacionales y tardan poco tiempo en cifrar y descifrar (Héctor Corrales Sánchez 2012). A continuación, se describe el funcionamiento la criptografía simétrica:

Figura 1. Criptografía simétrica



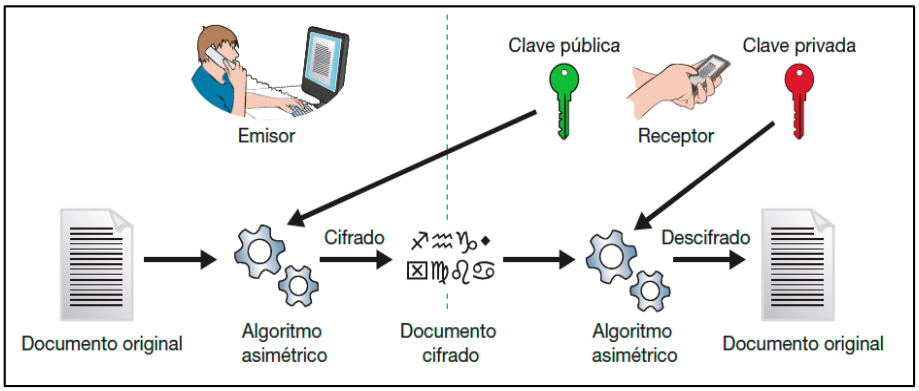
Fuente: Roca Busó (2015)

El emisor necesita enviar un documento al receptor. Toma el documento y le aplica el algoritmo simétrico, usa la clave única para cifrar, que, también, la conoce el receptor, con esto, se obtiene un documento cifrado. Al recibir el documento encriptado, el receptor, usa la misma clave y algoritmo para desencriptar, si, no se presentan cambios o alteraciones de un punto a otro y la contraseña sigue intacta, se accede al texto original.

En los años 70 los criptógrafos Diffie y Hellman publicaron sus investigaciones sobre la criptografía asimétrica, también, llamados sistemas de cifrado de clave pública. Este sistema de cifrado utiliza dos claves diferentes, una es la clave pública, la misma que es enviada a cualquier persona y otra llamada clave privada, de uso personal y solo el aludido tiene acceso a ella. (Corrales Sanchez, 2012).

Para enviar un documento, el remitente usa la clave pública del destinatario para cifrar los datos. Una vez cifrado el mensaje es descifrado con la clave privada del destinatario, la persona que generó el documento tampoco tiene acceso para descifrarlo, de esta forma, se consigue que solo el receptor acceda a la información.

Figura 2. Criptografía asimétrica



Fuente: Roca Busó (2015)

En su trabajo de investigación, María Belén Gómez Rivadeneira (2013) describe, el proceso de encriptación y desencriptación en los sistemas de cifrado usan algoritmos de cifrado, estos trabajan en conjunto con una llave para transformar texto claro en texto no legible, para no ser revertidos con facilidad por usuarios no autorizados.

Los algoritmos de cifrado, se clasifican en: algoritmos simétricos y algoritmos asimétricos.

Los algoritmos de cifrado simétrico usan la misma clave para encriptar y desencriptar los datos. El proceso de encriptación lo conforman dos elementos: un algoritmo y una clave ingresada por el usuario, esta, es independiente del texto a cifrar (Gómez Rivadeneira, 2013).

Existen dos tipos de algoritmos de cifrado simétrico: algoritmos simétricos de cifrados de bloque y algoritmo simétricos de cifrado de flujo.

María Belén Gómez Rivadeneira (2013), propone que los algoritmos de cifrado de flujo son los más indicados para trabajar en transmisiones de datos de alta velocidad, por ejemplo, en cifrado de conversaciones telefónicas, donde los datos viajan en tiempo real y en pequeños fragmentos (8 bits o 1 bit), debido a estos algoritmos la comunicación emisor-receptor es rápida, segura y sin cortes.

Por su parte, Hernán Serrano Losada (2019), describe que los algoritmos de cifrado por bloques dividen a los datos en pequeñas partes de longitud fija, aproximadamente de 64 o 128 bits, usa la misma clave de cifrado para cada bloque. Para el cifrado, se toma un bloque de texto plano o claro como entrada, esto produce un bloque de tamaño similar de texto cifrado. La transformación, es controlada al usar la clave secreta. Para el descifrado, se realiza el proceso inverso.

Entre los algoritmos de cifrados por bloques más importantes, se citan los siguientes: DES (*Data Encryption Standard*),3DES (Triple DES), AES (*Advanced Encryption Standard*).

Medina Vargas y Miranda Mendez (2015), proporcionan una comparación de rendimiento entre los tres algoritmos más importantes: DES, 3DES y AES, donde destacan la seguridad y rendimiento de estos.

Tabla 1. Comparación entre AES, 3 DES Y DES

PARAMETROS	AES	3DES	DES
LONGITUD DE CLAVE (bits)	128 - 192 - 256	168	56
TIPO DE CIFRADO	Bloque	Bloque	Bloque
TAMAÑO DE BLOQUE (bits)	128 - 192 - 256	64	64
VULNERABILIDAD	No ha sido vulnerado	Es tres veces mas seguro que DES pero por este motivo es tres veces mas lento	Dejo de ser utilizado en 1998 por haber sido vulnerado
SEGURIDAD	Alto	Bajo	Bajo
CANTIDAD DE CLAVES	$2^{128} - 2^{192} - 2^{256}$	2^{112} - 2^{168}	2^{57}
REVISION DE CLAVES	Para una clave de 128 bits 50 años	Para una clave de 112 bits 2,1 años	Para una clave de 56 bits 1,1 años
USO	En uso	Poco uso	sin uso

Fuente: Modificado a partir de Medina Vargas y Miranda Mendez (2015)

El articulo concluye; luego de realizar el estudio comparativo entre los tres principales algoritmos de cifrado por bloques, este demostró que AES, es mejor que DES y 3DES. Describen al algoritmo AES, como una combinación de seguridad, rendimiento, eficiencia aplicabilidad y flexibilidad. El algoritmo AES tiene mejor rendimiento en software y trabaja eficientemente en hardware de pequeños dispositivos como smartphones, tarjetas inteligentes, computadores portátiles, entre

otros, debido a esto muchas instituciones públicas y privadas lo utilizan para asegurar sus comunicaciones, información y datos confidenciales almacenados en sus equipos tecnológicos (Medina Vargas y Miranda Mendez 2015).

Por otro lado, están los algoritmos de datos asimétricos que usan dos claves, una publica para cifrar los datos y una privada para descifrarlos.

Gómez Rivadeneira (2013), explica la diferencia entre los algoritmos asimétricos con respecto a los algoritmos simétricos; esta radica en la longitud de la clave, 128 bit para un algoritmo simétrico y de al menos 1024 bits para un algoritmo asimétrico, otra diferencia, es la rapidez con la que trabajan; los algoritmos simétricos son aproximadamente mil veces más rápidos que los asimétricos.

Los algoritmos asimétricos usan un cálculo complejo que los vuelve lentos y por esta razón no son usados para cifrar grandes cantidades de información.

Entre los principales algoritmos de este tipo están: Diffie-Hellman, RSA (Rivest, Shamir y Adleman), DSA (Algoritmo de Firma Digital).

Las firmas electrónicas utilizan este tipo de algoritmo de cifrado para garantizar la integridad de un documento o mensaje.

INCIBE (2013), en su investigación “Protección de la Información”, describe, en el campo de la tecnología, la encriptación o cifrado de datos es la transformación de un texto claro a un texto codificado, al que se tiene acceso solamente después de descifrarlos por medio de un algoritmo clave.

La encriptación, es elemental para la seguridad de la información y, es el principal medio con, el cual, se protegen datos de posibles robos o accesos no autorizados, es ampliamente usado en la actualidad por todas las personas para proteger sus datos en el internet, también, lo usan empresas de todos los tamaños, con esto garantizan que sus datos, se encuentren seguros mientras viajan en la red.

La encriptación ofrece los siguientes beneficios:

- **Resguardar información privada:** el cifrado protege datos sensibles, como, información financiera, información personal de los usuarios, políticas internas, normativas institucionales, entre otros. (ESET, 2014).

- **Resguardar la imagen y prestigio de una empresa:** la información confidencial, es protegida para que no llegue a manos equivocadas y dañen su imagen corporativa. (ESET, 2014).
- **Resguardar equipos móviles:** los dispositivos que salen del perímetro seguro de una institución como, celulares, tabletas o computadores portátiles, se pierden o son hurtados, estas posibles circunstancias, hacen necesario asegurar la información contenida para que personas no autorizadas tengan acceso a estos equipos. (ESET, 2014)

1.2 Seguridad de la Información en Instituciones Públicas

La seguridad de la información en las entidades públicas no ha sido uno de los puntos fuertes del gobierno, esto, se evidencia claramente, ciertas instituciones no cuentan con una area especifica de seguridad o por lo menos una persona encargada de la misma (Manosalvas García, 2015).

En la actualidad las Tecnologías de la Información y Comunicación (TIC) son de vital importancia en el mundo, esto conlleva a la creación de una nueva rama dentro de la informática, que se denomina, “Seguridad de la Información”, además, se han creado normas y estándares tanto nacionales como internacionales para su control, gestión y desarrollo.

Entonces, la seguridad de la información es definida como las directrices a tomar para proteger la información. Al aplicar un estándar de seguridad de la información, todos los datos que se encuentren almacenados en dispositivos electrónicos o magnéticos, cumplirán con los parámetros de, confidencialidad, integridad y disponibilidad (Cáceres Tarco y Mena González 2015).

En el contexto legal ecuatoriano, para precautelar el acceso a la información, en el sector público, existe la “Ley Orgánica de Transparencia y Acceso a la Información Pública” (LOTAIP), donde, se encuentran definidas las características de la información y su modo de acceso.

El artículo 1, describe el Principio de publicidad de la información pública: "*El acceso al a información pública es un derecho de las personas que garantiza el Estado"*. Esto aplica a instituciones públicas y entidades que manejan o administran dinero del estado, los datos generados por estas, estarán a disposición de la ciudadanía en general. (Congreso Nacional del Ecuador, 2004)

La LOTAIP, también, determina tipos de acceso a la información en los artículos:

> *Art. 5.- "Información Pública. - Se considera información pública, todo documento en cualquier formato, que se encuentre en poder de las instituciones públicas y de las personas jurídicas a las, que se refiere esta ley, contenidos, creados u obtenidos por ellas, que se encuentren bajo su responsabilidad o, se hayan producido con recursos del estado.*
>
> *Art. 6.- Información Confidencial. - Se considera información confidencial aquella información pública personal, que no está sujeta al principio de publicidad y comprende aquella derivada de sus derechos personalisticos y fundamentales, especialmente aquellos señalados en los artículos 23 y 24 de la Constitución Política de la República* (Congreso Nacional del Ecuador, 2004)*."*

El artículo 6 de la LOTAIP disminuye el dominio de confidencialidad para las instituciones públicas, en este caso, las directrices a tomar son las siguientes:

> En toda institución sin importar su giro de negocio, existe información confidencial, que es revisada y validada antes de ser expuesta como versión final y aprobada para ser publicada. Dado que en el sector público, se toman decisiones de aplicación nacional, la confidencialidad de la información en sus primeras etapas es primordial para evitar malas interpretaciones (Cáceres Tarco y Mena González 2015).
>
> El principio de publicidad, se lo aplica al solicitar vía escrita al titular de la institución pública que genera la información, como lo indica la LOTAIP en su artículo 19. Esto da acceso a la información a personas que lo requieran de

manera obligatoria en todas las entidades públicas (Cáceres Tarco y Mena González 2015).

En su artículo 9, la LOTAIP, establece, que las solicitudes del ciudadano serán atendidas en un plazo máximo de diez días en todas las entidades del sector público, aquí la disponibilidad es primordial, en el caso de no entregar la información existen sanciones para los servidores públicos (Congreso Nacional del Ecuador, 2004).

La LOTAIP en su artículo 10, habla sobre sobre el dominio de la integridad, "*Quienes administren, manejen, archiven o conserven información pública, serán personalmente responsables, solidariamente con la autoridad de la dependencia a la que pertenece dicha información y/o documentación, por las consecuencias civiles, administrativas o penales a que pudiera haber lugar, por sus acciones u omisiones, en la ocultación, alteración, perdida y/o desmembración de documentación e información pública* (Congreso Nacional del Ecuador, 2004)*.* "

Con estos antecedentes, es fundamental que las empresas públicas implementen medidas para el control de los dominios de la seguridad de la información detallados en la LOTAIP, para atender este requerimiento del gobierno, está, el Esquema Gubernamental de Seguridad de la Información (EGSI) (Cáceres Tarco y Mena González 2015).

El Ministerio de Telecomunicaciones y de la Sociedad de la Información emite El Esquema Gubernamental de seguridad de la Información versión 2 (EGSI v2) en el acuerdo ministerial 025 publicado en el Registro Oficial el 10 de enero de 2020, este decreto deroga al Acuerdo 166 publicado el 25 de septiembre de 2013 y el Artículo 1 que dispone "*El uso obligatorio de las Normas Técnicas Ecuatorianas NTE INEN-ISO/IEC 2700 para la Gestión de la Seguridad de la Información* (Perugachi Betancourt, 2020).

El EGSI v2 en su Artículo 3 recomienda a las Instituciones de la Administración Pública utilizar "*como guía Las Normas Técnicas Ecuatorianas NTE INEN-ISO/IEC 2700 para la Gestión de la Seguridad de la Información*" (MINTEL 2020).

El EGSI constituye las pautas primordiales para la implementación de los sistemas de gestión de seguridad de la información, también, ayuda a las instituciones adjuntas a la función ejecutiva iniciar un proceso de mejora continua (MINTEL 2020). La norma INEC ISO/IEC 27002 "*TECNOLOGÍAS DE LA INFORMACIÓN — TÉCNICAS DE SEGURIDAD — CÓDIGO DE PRÁCTICA PARA LOS CONTROLES DE SEGURIDAD DE LA INFORMACIÓN*" (INEN, 2017), no es reemplazada por el EGSI.

El EGSI basa su estructura totalmente en la Norma INEN ISO/IEC 27002, los controles sugeridos en esta, serán implementados según la necesidad de la institución. A lo largo de sus 14 capítulos (dominios), se definen más de 900 hitos para el control de la seguridad de información, contienen 35 controles de seguridad principales (objetivos de control) y 115 controles, a continuación, se observa un resumen de los dominios de seguridad.

Tabla 2. Controles EGSI V2

	CAPÍTULO	CONTROLES	OBJETIVOS
1	POLÍTICA DE SEGURIDAD DE INFORMACIÓN	2	1
2	ORGANIZACIÓN DE LA SEGUIDAD DE LA INFORMACIÓN	8	2
3	SEGURIDAD DE LOS RECURSOS HUMANOS	6	3
4	GESTIÓN DE ACTIVOS	10	3
5	CONTROL DE ACCESO	14	4
6	CRIPTOGRAFÍA	2	1
7	SEGURIDAD FISICA Y DEL ENTORNO	15	2
8	SEGURIDAD DE LAS OPERACIONES	14	7
9	SEGURIDAD DE LAS COMUNICACIONES	7	2
10	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS	13	3
11	RELACIONES CON PROVEEDORES	5	2
12	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	7	1
13	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN PARA LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	4	2
14	CUMPLIMIENTO	8	2
TOTAL		115	35

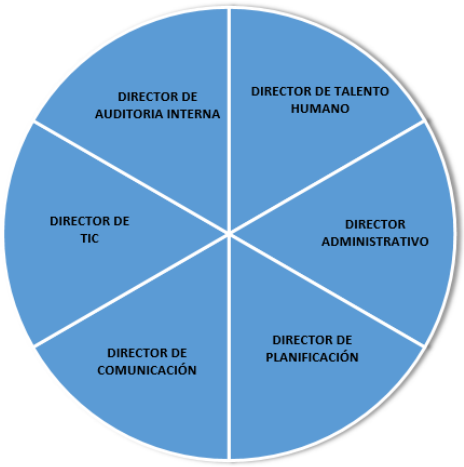
Fuente: Modificado a partir de MINTEL (2020)

El presente trabajo de investigación enfoca su atención en el control 6.1.1.3 "*Utilizar controles de cifrado para la protección de la información sensible transportada a través de medios extraíbles, móviles, removibles, por dispositivos especiales, o a través de las líneas de comunicación* (MINTEL 2020)", del dominio 6 del EGSI, donde, se hace referencia a la importancia de garantizar la seguridad de la información considerada confidencial o critica mediante el uso de técnicas criptográficas.

Entre los puntos obligatorios del EGSI, se menciona, que toda institución pública tiene la obligación de contar con una persona que desempeñe el cargo de Oficial de seguridad quien, se encarga de dar seguimiento y hacer cumplir el EGSI, este funcionario es quien informa al MINTEL el avance de implementación del EGSI (Manosalvas García, 2015).

Además, de designar formalmente a un responsable de Seguridad del Área de Tecnología y conformar un Comité de Seguridad de la Información su objetivo principal es verificar que el EGSI sea implementado como un Sistema de gestión de seguridad de la información (SGSI), sus integrantes son:

Figura 3. Integrantes del comité de seguridad de la información



Fuente: Modificado a partir de MINTEL (2020)

El MINTEL (2020), con la finalidad de llevar un reporte y control a los programas y proyectos de las Instituciones Públicas, usa el sistema Gobierno por Resultados (GPR), y, debido a que la implementación del EGSI v2 es obligatoria, su avance, es registrado en este sistema.

En base a lo indicado, (MINTEL 2020), con fecha de corte septiembre 2020, se toma como referencia los datos ingresados por las Instituciones al sistema GRP y, se generó un ranking de Entidades Públicas que han implementado el EGSI, donde, se evaluó un total de 82 instituciones, y, se presentan los siguientes resultados, con respecto al semáforo de calificación:

Tabla 3. Semáforo de calificación

Resultado	Franja	Ponderación	Acciones
Buena	Verde	100%-90%	Emisión de comunicado favorable y recomendaciones de mejora continua.
Regular	Amarillo	89%-60%	Emisión de observaciones y hallazgos para correcciones a la implementación.
Mala	Naranja	59%-30%	Emisión de observaciones y hallazgos para correcciones inmediatas. Definición de hoja de ruta
Muy Mala	Rojo	29%-0%	Emisión de observaciones y hallazgos para correcciones inmediatas. Estado urgente.

Fuente: Modificado a partir de MINTEL (2020)

- De las 82 instituciones evaluadas, solo dos (2), lo que corresponde al 2,44% han implementado el EGSI en su totalidad.
- Alrededor del 19,51% de instituciones (16 de 82 listadas) tienen un nivel de cumplimento Bueno.
- El 69,51% de instituciones (57 de 82 listadas) tienen un nivel de cumplimiento Regular.
- Otro 8,54% de instituciones (7 de 82 listadas) tiene un nivel de cumplimiento Mala.

Después de la implementación del EGSI, se reducirán significativamente amenazas, riesgos y vulnerabilidades relacionadas a la seguridad de la información,

física o digital que procesa una institución. También, ayuda a establecer un proceso de mejora continua de la gestión de la seguridad de la información e incrementar la cultura de protección de la información, que es manipulada por los servidores públicos para el desempeño de sus funciones (Cáceres Tarco & Mena González, 2015).

1.3 Cifrado de dispositivos móviles en instituciones publicas

En este apartado, se realiza una revisión bibliográfica de trabajos de investigación relacionados a la misma temática de estudio, se obtienen los siguientes trabajos:

La investigación realizada por (Perugachi Betancourt, 2020) expone los bajos niveles de seguridad de la información en una institución pública ecuatoriana, se analiza su estado actual, para esto, se utilizó la metodología MAGERIT de gestión de riesgos para determinar los activos de información y sus características de confidencialidad, integridad y disponibilidad, además, permite documentar el inventario de activos y realizar valoraciones cuantitativas sobre estos; con la ayuda de una encuesta realizada a 18 funcionarios, donde, se identificó que no cuentan con procesos o métodos para almacenar información considerada como confidencial o restringida en discos o dispositivos externos, servidores NAS y computadores. Para reducir los riesgos de los activos de información propone una Política de Seguridad de la Información con base a la norma ISO 27002:2013 y el EGSI, en uno de sus puntos de control recomienda, para toda copia de información considerada confidencial, se establece un etiquetado y esta, es cifrada con la finalidad de salvaguardar la confidencialidad, integridad y disponibilidad de la información. Además, señala la autora, con la implementación de dichas políticas, se espera, un impacto menor hacia la entidad en caso de ocurrir una amenaza.

Por otra parte, (Ledezma Espín, 2015) llevó a cabo un estudio en una institución pública con el propósito de la elaboración de un plan de políticas de seguridad de la información, para la recolección de información, se entrevistó a dos funcionarios de la institución, de acuerdo a las entrevistas realizadas, se determinó que las personas entrevistadas no tienen claros sus roles respecto a la gestión de procesos y de

seguridad de la información, y esto conlleva a que la entidad este expuesta a vulnerabilidades y amenazas. Para la implementación, se aplica la Metodología de Cascada. Uno de los controles incluido en el documento habla sobre la importancia del respaldo de información sensible, ubicado dentro del mismo computador portátil, adicional, “es importante realizar una copia de seguridad en la partición secundaria del disco duro, el departamento de TIC determina el método de cifrado a utilizar para proteger dicha información”, señala la autora, la finalidad principal, es fortalecer la seguridad de la información institucional referente a la gestión de las TICS, dichas políticas son guías que aseguran la protección e integridad de la información y ayudan a cumplir las disposiciones gubernamentales dadas en el EGSI.

En Nicaragua, en una investigación desarrollada por Vanegas Lopez (2018), se muestra que en una universidad pública, existen vulnerabilidades de seguridad en sus computadores portátiles, sus discos duros no se encuentran protegidos con algún método de cifrado. El objetivo de la investigación fue la implementación de un sistema de cifrado en dispositivos portátiles. La investigación tuvo un enfoque cualitativo y, se desarrolló con una metodología tipo cascada, se trabajó en un entorno virtual con 8 equipos, se aplica una prueba previa para la recopilación de información, se observa que el acceso a los datos contenidos en los disco duros es sumamente fácil y personal no autorizado la manipula sin problemas, se realizan pruebas posteriores donde, se corrobora que después de la implementación del sistema de cifrado en los dispositivos portátiles, se mitiga la vulnerabilidad de acceso a la información contenida en los discos duros de los computadores portátiles en caso de robo o pérdida, no se accede a la misma.

En Colombia, estudios realizados por Chala (2019); indaga sobre métodos de encriptación y su importancia al ser aplicados en entidades colombianas sin importar su giro de negocio, la técnica utilizada para la recolección de información fue documental y bibliográfica, y, se utilizó una metodología documental. El autor, realiza una un análisis de la información recopilada, se llega a la conclusión que en la actualidad, Colombia, no cuenta con una normativa clara sobre criptografía, por tal motivo las empresas no establecen procedimientos de encriptación de información en

sus políticas de seguridad internas, el autor recomienda implantar normativas y métodos con el objetivo de prevenir la fuga de información que las instituciones generen; también, sugiere, la implementación de dichas políticas sean realizadas con la ayuda de herramientas criptográficas para el cifrado de correo electrónico y discos duros, además, enfatiza el uso de la firma electrónica para validación de documentos, y utilizar dispositivos criptográficos basados en hardware, esto ayuda a generar, almacenar y proteger claves criptográficas, con la finalidad de aportar soluciones para salvaguardar la información generada y manipulada por toda institución

CAPÍTULO II. DISEÑO METODOLÓGICO

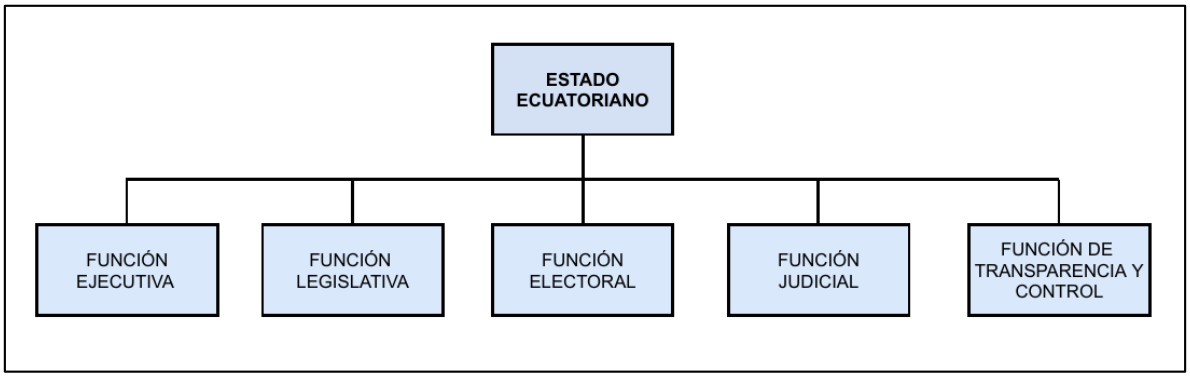
El presente capitulo está organizado en tres partes:

La primera parte, es la caracterización de la institución, donde, se implementa la solución de cifrado; en la segunda parte, se establecen los aspectos de la investigación realizada, como son: el métodos y enfoque de investigación, tipos de investigación, teóricos y prácticos a utilizar, población, y, finalmente, la tercera parte aborda la metodología de desarrollo.

2.1 Caracterización de la Institución

La estructura orgánica del sector público ecuatoriano, se encuentra detallado en el artículo 225 de la Constitución de la República del Ecuador, a continuación, se aprecia su organización (Asamblea Nacional del Ecuador, 2015).

Figura 4. Estructura del estado



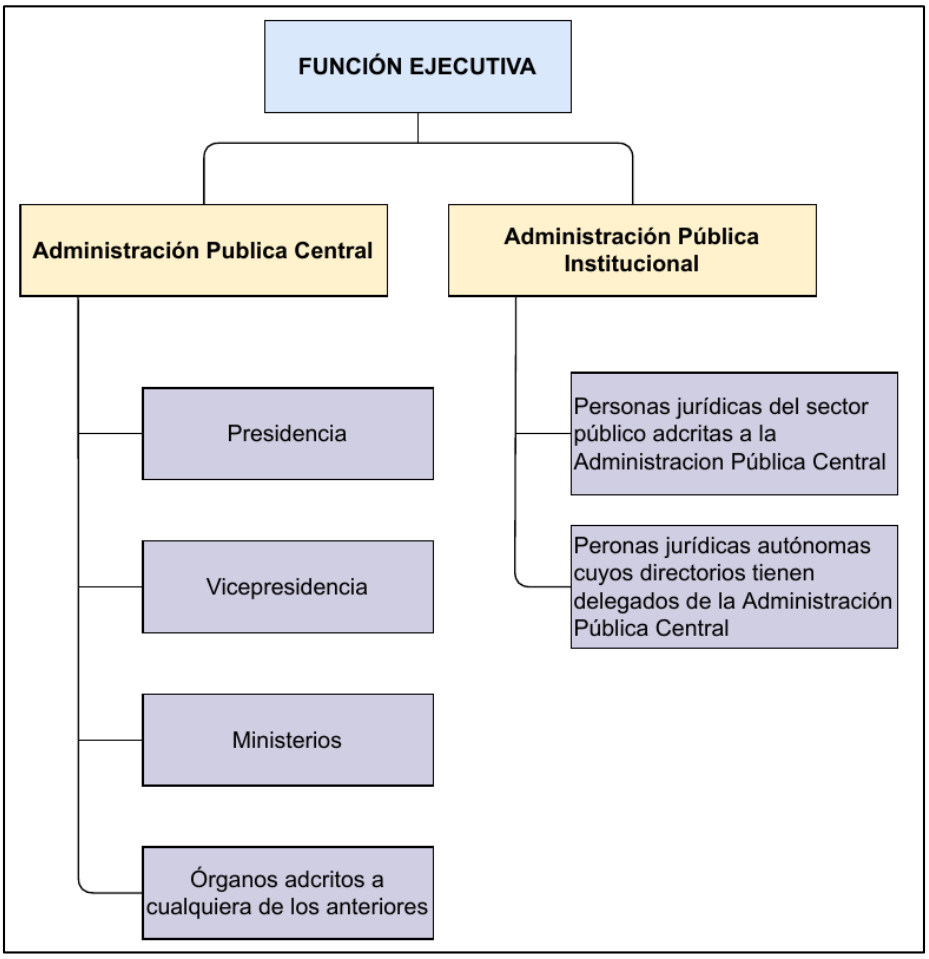
Fuente: Tomado a partir de Asamblea Nacional del Ecuador (2015)

"*Para sus efectos, la función Ejecutiva comprende:*

a. *La Presidencia y la Vicepresidencia de la Republica y los órganos dependientes o adscritos a ellas;*
b. *Los Ministerios de Estado y los órganos dependientes o adscritos a ellos; […]*

Los órganos comprendidos en los literales a) y b) conforman la Administración Pública Central […] y las personas jurídicas del sector público señaladas en los demás literales.(Presidencia del Ecuador, 2011)"

Figura 5. Estructura de la función ejecutiva



Fuente:(Presidencia del Ecuador, 2011)

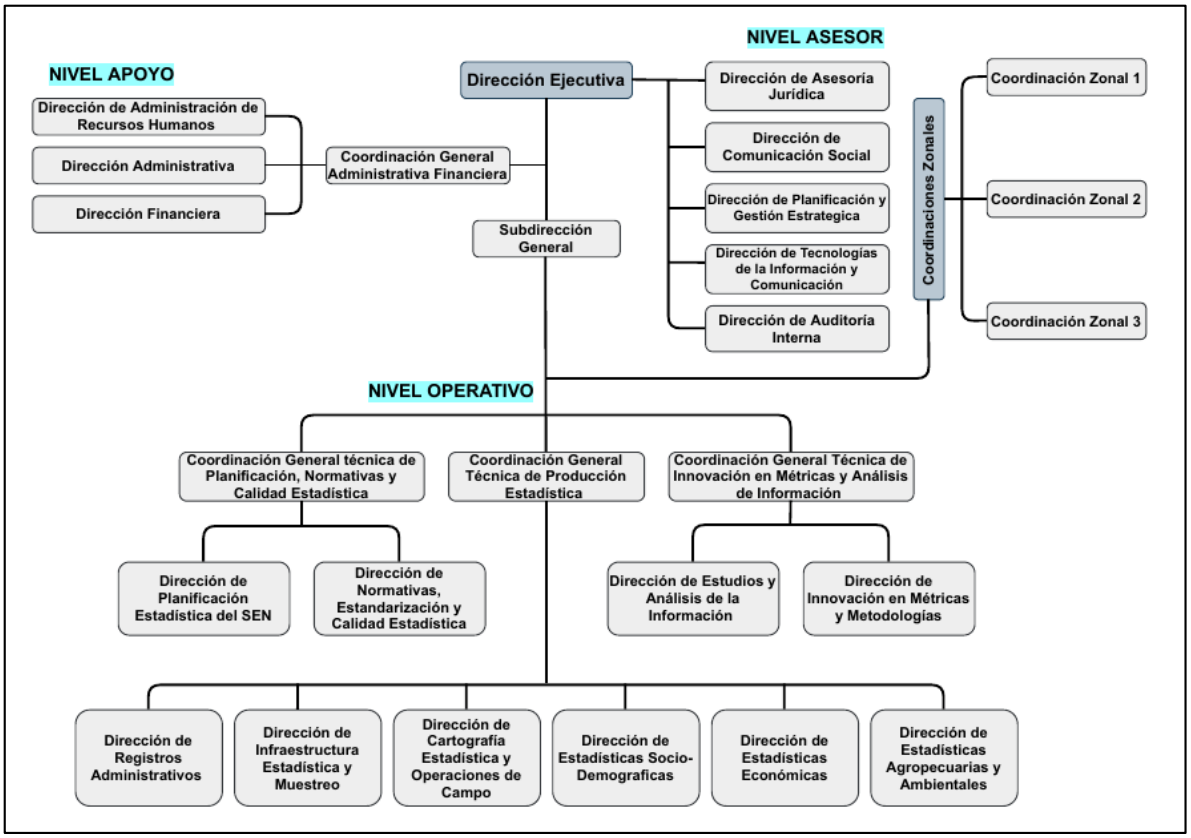
Características de la empresa

Institución adscrita a la Función Ejecutiva, establecida como una entidad pública que, para fines técnicos, administrativos, operativos y financieros, ejerce sus funciones y atribuciones de manera independiente y desconcentrada, con domicilio principal en la ciudad de Quito, Distrito Metropolitano.

Su principal servicio es la de entregar cifras de calidad para la elaboración de Políticas de Estado.

La entidad tiene presencia en las principales ciudades del país y está formada por 500 empleados aproximadamente, en la figura 6, se aprecia la estructura de la institución.

Figura 6. Orgánico funcional de la institución



Fuente: Modificado a partir de (INEC, 2020)

Infraestructura tecnológica

La infraestructura tecnológica comprende el hardware y software que ayuda a la institución a brindar sus servicios a los usuarios finales. Este apartado del documento comprende el levantamiento de información de los computadores de portátiles que tiene la institución en su edificio matriz.

Explica INEN (2015), el proceso de identificación de activos de información es primordial para conocer, cuales, están involucrados en los procesos de la institución. Los activos de información específicos que intervienen en el proceso de cifrado, se encuentran detallados, a continuación.

Tabla 4. Tipos de activos de información

ACTIVO	TIPO DE ACTIVO
Servidores	Hardware
Computadores/Laptops	Hardware
Sistemas operativos	Software
Diagramas de infraestructura	Datos/Información

Fuente: Elaboración propia

A continuación, se detallan los resultados del proceso de levantamiento de inventario realizado en la institución.

Toda la información contenida en los discos duros de los computadores portátiles de la institución es considerada confidencial y sensible, su divulgación está prohibida, para el resguardo de la misma, se solicita asesoría a DITIC (mesa de ayuda) con el proceso de cifrado de dispositivos móviles implementado actualmente[3].

Tabla 5. Inventario de equipos

Descripción	Cantidad
COMPUTADOR DE ESCRITORIO INTEGRADO	3
CPU	11
CPU - MONITOR -	1
CPU - MONITOR - TECLADO - MOUSE	599
PORTATIL	312
Total	**926**

Fuente: Elaboración propia

De los datos obtenidos, se observa que actualmente la institución cuenta con un parque informático de 926 computadores; de los, cuales, 312 son computadores

[3] Documento interno de la Institución.

portátiles objeto del presente estudio. A continuación, se describe la distribución de los computadores portátiles y sus características.

Tabla 6. Distribución por departamentos de computadores portátiles

UBICACIÓN	CANTIDAD
COORDINACIÓN 1	3
COORDINACIÓN 2	2
COORDINACIÓN 3	2
DIRECCIÓN DE RECURSOS HUMANOS	16
DIRECCIÓN ADMINISTRATIVA	114
DIRECCIÓN JURÍDICA	3
DIRECCIÓN DE AUDITORIA	2
DIRECCION 1	32
DIRECCION DE COMUNICACION SOCIAL	3
DIRECCIÓN 2	6
DIRECCIÓN 3	14
DIRECCIÓN 4	24
DIRECCIÓN 5	6
DIRECCIÓN 6	10
DIRECCIÓN 7	8
DIRECCIÓN 8	9
DIRECCIÓN 9	8
DIRECCIÓN DE PLANIFICACIÓN	21
DIRECCIÓN 10	3
DIRECCION DE TECNOLOGIAS DE LA INFORMACIÓN Y COMUNICACIÓN	8
DIRECCION EJECUTIVA	6
DIRECCION FINANCIERA	9
SUBDIRECCIÓN GEENRAL	3
Total	**312**

Fuente: Elaboración propia

La administración de los computadores portátiles, se realiza por medio de un servidor de Directorio Activo (AD), que tienen las siguientes características.

Tabla 7. Servidor de usuarios

UBICACIÓN		
DATA CENTER		
SOFTWARE		
NOMBRE	**DESCRIPCIÓN**	**SISTEMA OPERATIVO**
Directorio Activo (AD)	Software para la administración de usuarios	Windows Server 2008 R2 Enterprise

Continuación Tabla 2.4.

HARDWARE			
NOMBRE	**ESPACIO DISCO**	**MEMORIA**	**PROCESADOR**
serverdomain	1 Tb	16 Gb	Intel Xenon X5550 @ 2,67 GHz

Fuente: Elaboración propia

Por políticas de seguridad los equipos portátiles tienen configurados tres usuarios descritos, a continuación:

Tabla 8. Perfiles de usuario

DESCRIPCIÓN	PERFIL	PERMISOS
ADMINISTRADOR LOCAL	Administrador	Acceso total
ADMINISTRADOR DE DOMINIO	Administrador	Acceso total
USUARIO LOCAL	Estándar	Operador de configuración de red

Fuente: Elaboración propia

- **Usuario Administrador Local**: para configuraciones iniciales del equipo.
- **Usuario Administrador de Dominio**: para configuraciones globales del equipo una vez que se encuentre dentro del dominio principal.
- **Usuario Local**: usuario que utiliza el equipo, no cuenta con permisos para realizar cambios en la computadora, si necesita realizar algún cambio en la configuración debe solicitarlo por medio de la mesa de ayuda, cuenta con permisos de configuración de red para modificar su ip en caso de que el dispositivo salga de la institución, por políticas de seguridad de acceso a la red de datos los computadores portátiles utilizan una IP fija.

El sistema operativo predominante es Windows 7 Professional con licencia original, venía preinstalado en los equipos al momento de la compra.

Tabla 9. Cantidad de equipos por sistema operativo

SISTEMA OPERATIVO	CANTIDAD
Microsoft Windows 10 Enterprise 2016 LTSB	1
Microsoft Windows 10 Pro	108
Microsoft Windows 7 Professional	196
Microsoft Windows 8 Professional	2
Microsoft Windows 8.1 Pro	2
Microsoft Windows XP Professional	2
Microsoft Windows Vista Home Basic	1
Total	**312**

Fuente: Elaboración propia

Actualmente, la institución se encuentra en proceso de migración de sistemas operativos a Windows 10 en todos los computadores que comprenden el parque informático, sistemas operativos previos a este, no cuentan con soporte técnico por parte del fabricante y representan una amenaza para la seguridad de la institución.

Los computadores portátiles, se encuentran divididos en tres gamas: alta, media y baja.

Tabla 10. Clasificación de equipos por gama

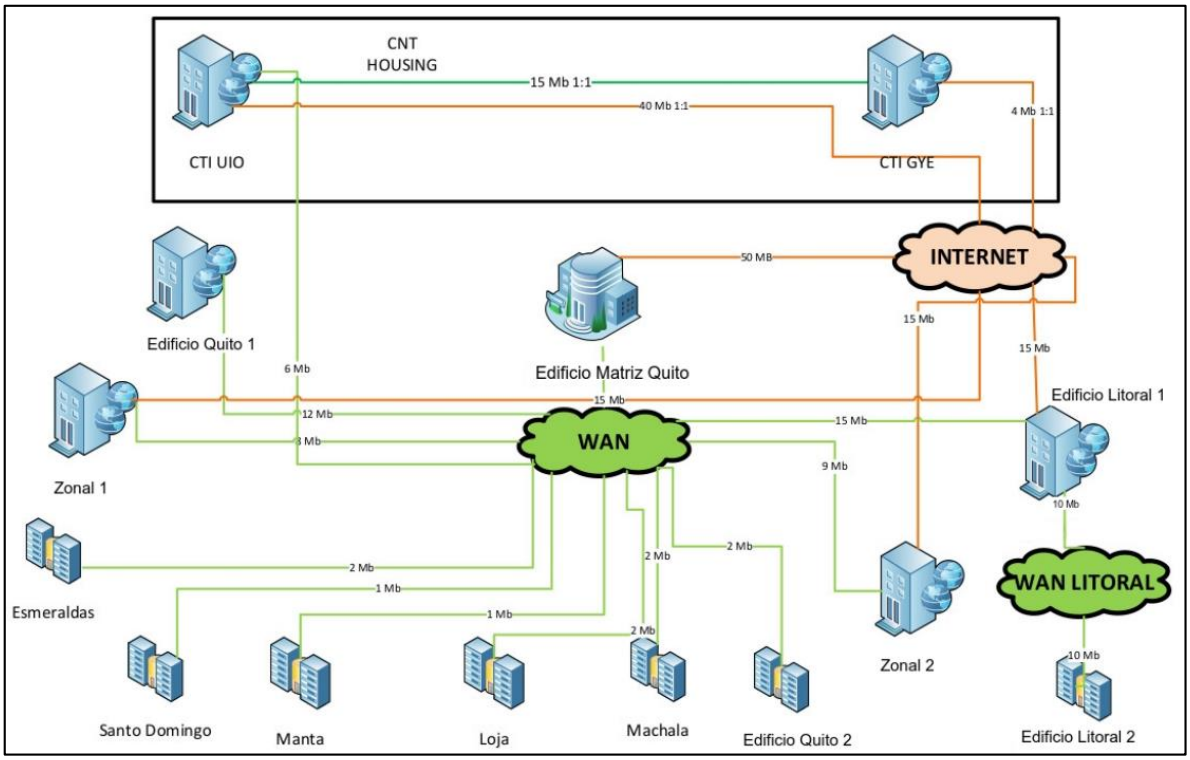
GAMA	DESCRIPCIÓN		
ALTA	PROCESADOR RAM DISCO	Intel Core i7 8 Gb -32 Gb 120 Gb SDD - 1Tb HDD	160
MEDIA	PROCESADOR RAM DISCO	Intel Core i5 4 Gb - 8 Gb 500 Gb HDD	66
BAJA	PROCESADOR RAM DISCO	Intel Core i3 / Intel Core 2 duo/ AMD Turion / Intel Atom 2 Gb - 4 Gb 500 Gb HDD	86
TOTAL			**312**

Fuente: Elaboración propia

Para la distribución de computadores portátiles a los usuarios, se evalúan los requerimientos del cargo y, según sus necesidades, se asigna un computador, si el funcionario no procesa datos, se asigna un equipo de características básicas.

Con la finalidad de actualizar el parque informático de la institución, el año pasado, se adquirieron 70 computadores portátiles de gama alta, los mismos, que se encuentran asignados a uno los proyectos emblemáticos del país que desarrolla la institución. A continuación, se aprecia la estructura de red WAN de la institución.

Figura 7. Esquema red WAN de la institución



Fuente: Elaboración propia

En el grafico anterior, se observa la red WAN de la institución con sus respectivos enlaces y anchos de banda, la red WAN proporciona conexión entre todas las localidades de la institución, además, de interconectividad para la compartición de recursos y acceso a base de datos compartidas de la entidad.

2.2 Metodología de Investigación

Enfoque de investigación

El enfoque de investigación utilizado para el desarrollo del presente proyecto es el cualitativo, el cual, nos ayuda con la recopilación de información; para esto, es necesario indagar y analizar sobre tecnologías de cifrado existentes para computadores portátiles, también, las características tecnológicas de los equipos, que se utilizan en la implementación y tener una referencia en sistemas de cifrado, para ser replicado en las instituciones públicas.

Tipo de Investigación

Los tipos de investigación a utilizar son las siguientes: descriptivo, explicativo, debido a, que se establece como un proceso descriptivo-explicativo. Al aplicar el método descriptivo, se muestran las características y necesidades que presenta el sistema de cifrado, todo lo que conlleva, mientras que el método explicativo muestra el estado actual de la institución y vincula los requerimientos y funcionalidades del sistema de cifrado, además, nos ayuda con la creación de manuales técnicos necesarios del proceso de implementación y uso.

Técnicas e Instrumentos de investigación

Para la recolección de datos, se utilizó las siguientes técnicas de recopilación de información:

Entrevista

La entrevista, se define como una conversación formal entre dos o más personas, donde, se obtiene información respecto al tema especificado. (Diaz Bravo et al., 2013). La entrevista, se aplicó a la Directora de Tecnologías de la Información y Comunicación (TICS) en calidad de patrocinadora ejecutiva del proyecto de Implementación del Sistema de Cifrado, la finalidad de la entrevista fue reunir los antecedentes y datos del proceso del sistema de cifrado, además, características e impacto del mismo a nivel nacional, también, se entrevistó a los responsables de la

implementación del sistema de cifrado, con la finalidad de reunir las evidencias para cada hito del proyecto.

Instrumentos

Para las entrevistas, se utilizó un cuestionario no estructurado con el mismo formato. Para Diaz Bravo et al. (2013), los cuestionarios no estructurados son descritos como conversaciones mantenidas con un propósito específico: recopilar datos sobre el estudio de investigación. El formato, de la entrevista, que se aplicó a la directora de TICS de la Institución y a los responsables de la implementación del sistema de cifrado. El documento indicado, se lo apreciamos en el Anexo 3.

Para diagnosticar el acceso a la información contenida en los discos duros de los computadores portátiles, se retira el disco duro sin cifrar y con la ayuda de un enclosure[4], se conecta a otro equipo, con el objetivo de mostrar el fácil acceso a la información almacenada.

Se realiza un análisis de aplicaciones de cifrado de disco completo existentes en el mercado para determinar, cual, es la más idónea para la implementación del presente proyecto.

Además, se realizó un PreCheck a los computadores portátiles con la finalidad de determinar los equipos óptimos para la implementación del sistema de cifrado.

Población

La población de estudio que interviene en este trabajo de investigación, la conforman 70 computadores portátiles adquiridos recientemente por la institución, marca DELL, modelo Precision 3541, estos equipos son los más importantes del inventario por la información que manejan, y por ser parte de un proyecto de alcance nacional que lleva la institución, además, sus altas características técnicas facilitarán

[4] Enclosure: Permite convertir un disco duro SATA en una unidad de almacenamiento portátil externa para conexión USB.

la implementación del sistema de cifrado. A continuación, se detallan sus características.

Tabla 11. Muestra

DELL PRECISION 3541	
Procesador	Intel(R) Core(TM) i7-9750H CPU @ 2.60 GHz
Disco duro	120 Gb SSD / 1Tb HDD
Ram	32 Gb
S.O.	Windows 10 Pro
Gama	Alta

Fuente: Elaboración propia

Resultados de los instrumentos de investigación

Análisis y conclusión de la entrevista

La encuesta realizada al personal de DITIC de la institución, se conformó de cinco preguntas, los resultados obtenidos, se muestran, a continuación.

Tabla 12. Inventario de computadores portátiles

Pregunta 1: ¿Usted conoce cuantos computadores portátiles tiene la institución en su inventario, de estos, que porcentaje salen de las instalaciones para teletrabajo?
R1: En la institución a nivel Nacional, existen un total de 400 computadores portátiles, de los, cuales, el 100% de equipos en este momento han salido de la institución para temas de teletrabajo, existe una necesidad de los colaboradores de solventar temas laborales, en muchos casos, hubo la necesidad de que el personal, se lleve equipos de escritorio, por la situación de la pandemia.
R2: Actualmente, en la institución existen alrededor de 400 computadores portátiles, de los, cuales, 312 equipos, se encuentran en el edificio matriz de la ciudad de Quito, de estos, aproximadamente un 90% han salido de la institución por temas de teletrabajo.
R3: En el último reporte de inventario, se contabilizó 312 equipos portátiles, presumo que debido al teletrabajo salieron de la institución un75% de estos.
Análisis: De las respuestas obtenidas de parte del personal del Departamento de DITIC, se observa que tienen conocimiento de la cantidad de computadores portátiles con los que cuenta la institución en el edificio matriz de la ciudad de Quito y a nivel nacional, esto indica, que se mantiene un inventario actualizado y de conocimiento general dentro del departamento, además, se determina que aproximadamente el 90% de equipos portátiles, se encuentran fuera de la institución por razones de teletrabajo.

Fuente: Elaboración propia

Tabla 13. Características técnicas de los equipos

Pregunta 2: ¿Qué características técnicas tienen los equipos portátiles, que se encuentran en teletrabajo, los sistemas de protección de datos instalados son fiables, usted considera que estos sistemas de protección protegen la confidencialidad de la información?
R1: Las características técnicas, son distintas, existen varias marcas y modelos, en base a las fechas que fueron adquiridas en la institución, se han implementado controles de seguridad para evitar fuga de información y confidencialidad, sin embargo, siempre existe la necesidad de complementar y mejorar los controles, sin que esto implique que sean 100% seguros, al tomar una fotografía a la información, se perdería el control, la seguridad, es una suma de controles tecnológicos, operativos y sobre todo de concientización al usuario final. Por lo que la consulta que habla de fiables no es correcta, los sistemas cumplen sus funciones dentro de un proceso adecuado de instalación, configuración y procedimientos normados que busquen establecer que vulnerabilidad es la que se desea mitigar.
R2: Las características técnicas de los equipos, que se encuentran en teletrabajo son variadas, han sido adquiridas en diferentes lapsos de tiempo, entre estas tenemos computadores con procesadores Intel core 2 dúo, core i3, core i5 y core i7, para la protección de la información generada por los usuarios, se han implementado sistemas de seguridad, los, cuales, cumplen con proteger la confidencialidad e integridad de la información contenida en los discos duros, sin embargo, es necesario implementar medidas de seguridad adicionales para mitigar la fuga de información en caso de robo o pérdida de los equipos portátiles.
R3: Son equipos ideales para el buen funcionamiento de teletrabajo. Características básicas: Procesador Core i3 / Core i5 / Core i7, memoria RAM de 4 GB a 8 GB, disco duro de 500 GB o superior, pantalla de entre 13″ a 15″ Entradas USB 2.0, multilector de tarjetas. Actualmente, se encuentra en proceso el cifrado de discos en equipos portátiles, que sirve para el cuidado y uso de información confidencial.
Análisis: De los resultados obtenidos, se concluye que la institución cuenta con equipos de diferentes marcas y características divididos en 3 gamas: gama alta, media y baja según su procesador, además, el sistema de resguardo de información no es 100% fiable, debido a que los datos generados por los usuarios, se encuentran en un formato legible y son de fácil acceso a personal no autorizado, por tal motivo, ante esta problemática, se requiere la implementación de controles adicionales para mitigar la fuga de información.

Fuente: Elaboración propia

Tabla 14. Equipos considerados para el sistema de cifrado

Pregunta 3: ¿De los equipos portátiles, que se encuentran actualmente en el inventario de la institución, ¿cuáles cree usted que son los más importantes a ser considerados para la implementación del sistema de cifrado de datos?
R1: Todos los equipos son susceptibles a la implementación incluidos los equipos servidores como los de estación de trabajo, se ha considerado el tema de equipos portátiles, porque tienen un riesgo mayor a ser sustraídos, perdidos o desatendidos por parte del usuario, esta vulnerabilidad, es la, que se desea controlar, con el fin de que si el bien, se pierde, no implique perdida de confidencialidad de la información, que se encuentra en el equipo.
R2: Todos los equipos del inventario de la institución, se consideran importante para la implementación del sistema de cifrado, con esto, se protege el acceso a la información que es propiedad de la institución, se inicia con los equipos portátiles por su alta movilidad fuera de la oficina, de estos equipos, los adquiridos recientemente por la institución son los más importantes para ser considerados en la implementación del sistema de cifrado.
R3: Se considera, que todos los equipos son importantes para la implementación de sistema de cifrado, se protege la información pertinente a nuestro ejercicio gubernamental como servidores públicos, de vital importancia el cifrado de los equipos adquiridos recientemente por la institución.

Análisis: Conforme a los resultados obtenidos, la implementación del sistema de cifrado aplica al 100% de equipos de la institución incluidos computadores de escritorio y servidores, inicialmente, se consideran primordiales los computadores portátiles por su alta movilidad fuera de las instalaciones, esto los vuelve susceptibles a pérdidas o robos, finalmente, se determina que los equipos portátiles adquiridos recientemente por la institución serán con los, que se inicie el proceso de cifrado de discos duros por ser parte de un proyecto de alcance nacional que lleva la institución.

Fuente: Elaboración propia

Tabla 15. Aplicación del cifrado

Pregunta 4: ¿El sistema de protección de datos instalado en los computadores portátiles de la institución brinda la opción de cifrado de datos, considera que la encriptación del disco duro mejora la seguridad de los equipos portátiles?
R1: El sistema antivirus, tiene la opción de encriptar discos y en base a ello, se consideró la implementación de este control de seguridad, que aporta y apoya a mejorar la seguridad del equipo, sin que esto implique, que se ha completado los temas de seguridad, como, se mencionó son varios factores los que serán implementados y el usuario final es el eslabón más débil en este proceso.
R2: Actualmente la institución cuenta con una herramienta de antivirus que tiene la opción de cifrado de disco completo, esto ayuda a la implementación del sistema de cifrado, y aporta con la seguridad de los equipos portátiles, mitiga la fuga de información confidencial, además, proporciona integridad, disponibilidad y de la información contenida en los discos duros.
R3: Por supuesto, el cifrado de datos protege información confidencial generada por los usuarios de la entidad, esto ayuda a salvaguardar la información en caso de pérdida o robo de los equipos portátiles, también, ayuda a prevenir al acceso de personal no autorizado
Análisis: En base a las respuestas dadas por los entrevistados, se evidencia que la institución cuenta con una herramienta que cuenta con la capacidad de cifrar discos duros en su totalidad, por tal motivo, se considera la implementación del control de cifrado para la seguridad de la información, también, se concluye que la implementación de este sistema ayuda a mejorar la seguridad de los equipos portátiles frente a posibles amenazas de accesos no autorizados.

Fuente: Elaboración propia

Tabla 16. Beneficios del cifrado

Pregunta 5: ¿Cuáles son las ventajas que brindaría el sistema de cifrado implementado en los computadores portátiles de la institución?
R1: Permite un control automático e independiente del usuario, en caso de pérdida del equipo, sustracción u olvido del mismo, un tercero no tiene acceso a la información de la institución y del funcionario, con lo, cual, se garantiza que no exista pérdida de confidencialidad de la información, que se encontraba en el equipo. Este control es transparente para el usuario y no afecta en sus funciones diarias y en base a las pruebas realizadas no afecta en la respuesta y procesamiento del equipo en su trabajo diario.
R2: La ventaja principal del sistema de cifrado es mantener ilegible la información contenida en los discos duros en caso de pérdida o robo de los equipos portátiles, con esto la información, no es utilizada por personal no autorizado, además, el sistema de cifrado garantiza la confidencialidad de la información contenida en el equipo.
R3: Entre las ventajas del sistema de cifrado mencionaremos, integridad de la información, esta, no es modificada por personal no autorizado, la información contenida en los computadores portátiles solo sea accedida si se conoce la contraseña de acceso y en el caso de que un equipo sea sustraído, se formatea el mismo para ser utilizado, lo que implica la pérdida total de la información.
Análisis: En conclusión, con los comentarios obtenidos por parte del personal de la institución, la ventaja principal del sistema de cifrado de discos duros de las computadoras portátiles, es la mitigación

de la amenaza de fuga de información confidencial y delicada en caso de pérdida o robo de los equipos, además, se garantiza la confidencialidad de la información contenida en el equipo, esta, se mantiene ilegible para personal no autorizado. También, el sistema de cifrado es transparente y no afecta el funcionamiento del equipo, esto lo hace imperceptible al usuario, por tal motivo sus actividades diarias, no se verán afectadas.

Fuente: Elaboración propia

Conclusiones del diagnóstico de computadoras portátiles

Luego de pruebas realizadas a los discos duros de los computadores portátiles con la ayuda del enclosure, se determina que el acceso a la información almacenada en estos, es muy fácil, debido a, que se encuentra legible para toda persona, y es utilizada para cualquier finalidad.

Por lo tanto, se concluye que la implementación de un sistema de cifrado de discos duros en equipos portátiles, es de suma importancia para evitar posibles fugas de información en caso de robo o pérdida de los equipos, además, con esto, se mitiga por completo el acceso a datos confidenciales y delicados por parte de personal no autorizado.

Análisis y conclusiones de aplicaciones de cifrado

Existen varias herramientas de cifrado de disco completo en el mercado, encontramos aplicaciones gratuitas y licenciadas. Entre las aplicaciones gratuitas más importantes para la encriptación de disco completo tenemos Bitlocker y VeraCrypt.
La institución donde, se desarrolla el presente proyecto, cuenta con dos herramientas de antivirus licenciadas para la protección de sus dispositivos, estas son, McAfee y Kaspersky.
A continuación, se muestran las principales características de estas aplicaciones.

Tabla 17. Características principales herramientas de cifrado

Aplicación	Desarrollador	Tipo de licencia	Consola de administración	Algoritmo	Sistema operativo Servidor	Sistema operativo Cliente
BitLocker	Windows	Open	No	AES 128	No aplica	Windows 7 Windows 8 Windows 10 Windows 11 Windows server 2016 o superior
VeraCrypt	IDRIX	Open	No	AES 256	No aplica	Windows Xp Windows 7 Windows 8 Windows 10 Windows server 2003 Windows server 2008 Windows server 2012
McAfee Complete EndPoint Protection – Business (CEB)	McAfee	Comercial Licencia por host	Si	No aplica	Windows server 2003 Windows server 2008 Windows server 2012	Windows Xp Windows 7 Windows server 2003 Windows server 2008 Windows server 2012
Kaspersky Endpoint Security for Business	Kaspersky	Comercial Licencia por host	Si	AES 256	Windows server 2008 Windows server 2012 Windows server 2016 Windows server 2019	Windows 7 Windows 8 Windows 10 Windows 11 Windows server 2008 o superior

Fuente: Elaboración propia

Después de comparar las principales características de las aplicaciones, se concluye, las herramientas Bitlocker y VeraCrypt, no cumplen con los requisitos básicos para la implementación del sistema de cifrado de disco completo, no cuentan con gestión centralizada y, no es posible integrarlas al *Active Directory*, al no contar con esta opción, la administración de los dispositivos, se complica, estas herramientas son útiles cuando la cantidad de dispositivos a cifrar son mínimas.

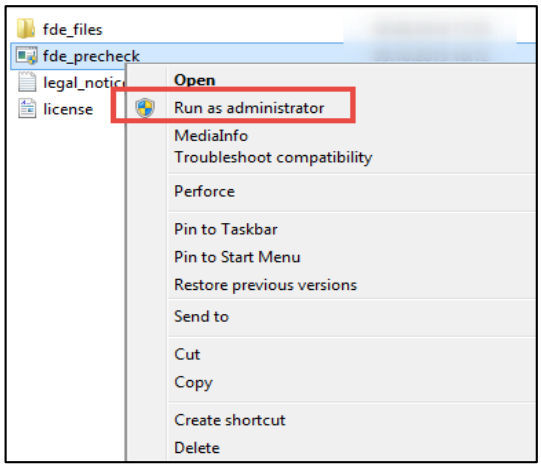
Las aplicaciones licenciadas McAfee *Complete EndPoint Protection Business* (CEB) y Kaspersky *Endpoint Security for Business* cumplen con la gestión centralizada, se integran al *Active Directory*, con esto, la administración de los computadores portátiles es más fácil y rápida, la aplicación de políticas y directivas de seguridad, se realiza de manera inmediata una vez instalado el aplicativo en el

dispositivo cliente. Como, se observa en las características de las aplicaciones licenciadas, la herramienta de McAfee no cumple con los requisitos básicos para la implementación del presente proyecto, no cuenta con el módulo de cifrado de disco completo activo, además, al ser un aplicativo desactualizado está orientado a ser utilizado en sistemas operativos clientes Windows XP y Windows 7, por tal motivo, se elige a la herramienta de Kaspersky para la implementación del sistema de cifrado de disco completo, cumple con todos los requisitos del proyecto a implementar. Además, para facilitar el proceso de encriptación de disco completo, la herramienta de cifrado de Kaspersky incluye la aplicación PreCheck, la misma que realiza un análisis previo de hardware a los computadores, con la finalidad de establecer, cuales, son los equipos idóneos para la implementación del sistema de cifrado.

Análisis y conclusión de la verificación previa de los computadores portátiles

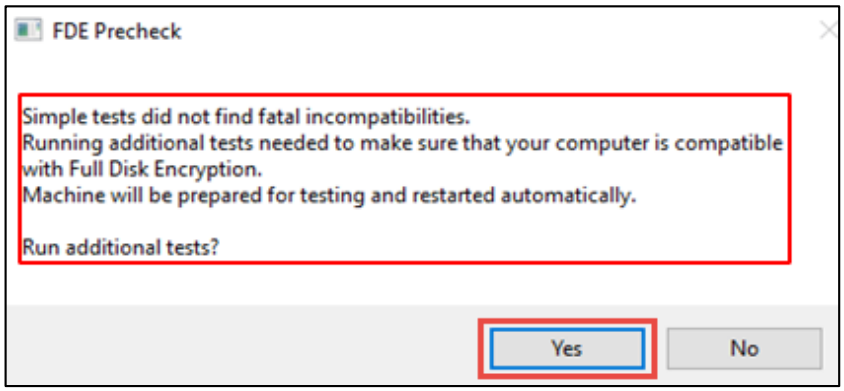
Con la ayuda del aplicativo PreCheck, se realiza una verificación previa a los 312 computadores portátiles, esta aplicación ejecuta un test rápido de compatibilidad del equipo con el cifrado de disco completo. Si las pruebas finalizan con éxito, la aplicación realiza pruebas adicionales.

Figura 8. Aplicativo PreCheck



Fuente: Elaboración propia

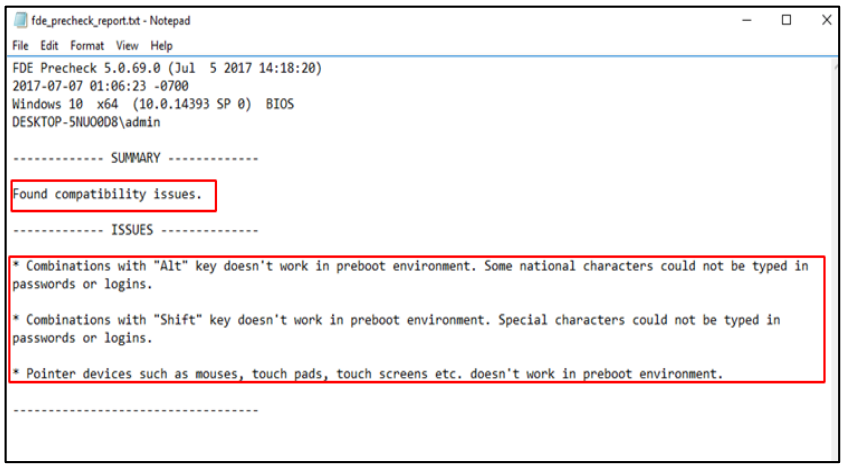
Figura 9. Pruebas adicionales



Fuente: Elaboración propia

Luego de este proceso, si el equipo, no es compatible, la aplicación muestra un informe con las incompatibilidades encontradas, ya sea, video, teclado memoria, entre otros, con esto, se descarta al equipo debido a que no cumple con las características básicas para la implementación del sistema de cifrado.

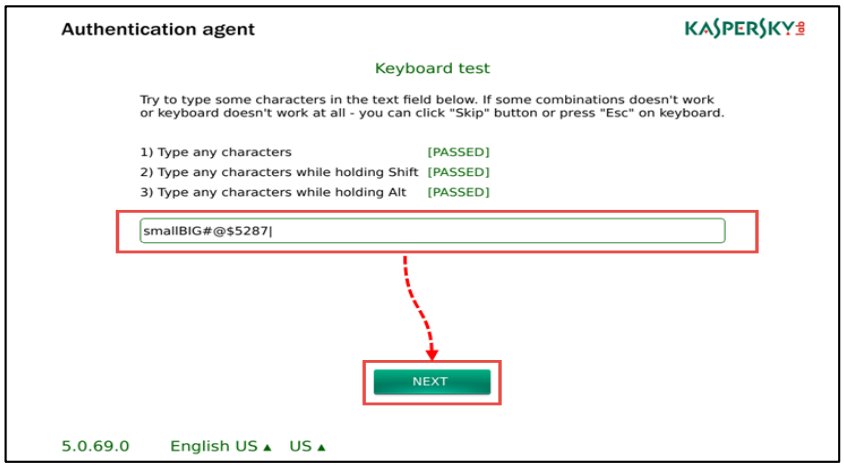
Figura 10. Informe de incompatibilidades



Fuente: Elaboración propia

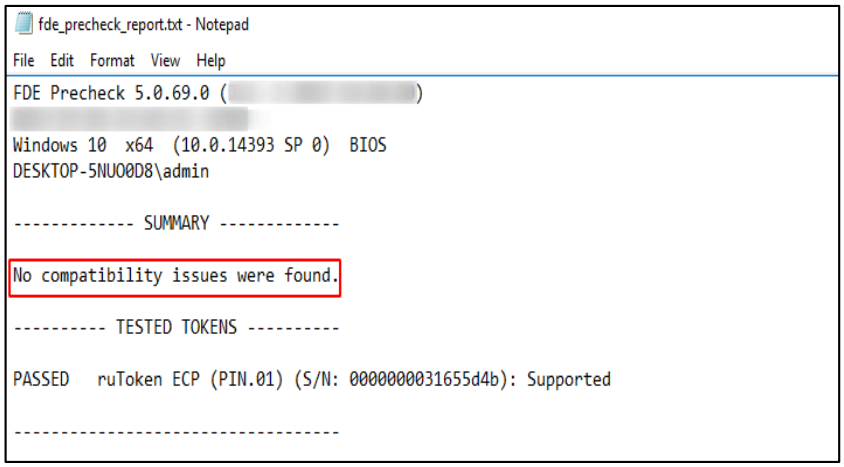
En el caso de equipos compatibles, las pruebas adicionales de teclado, mouse, touch y tockens, se desarrollan con normalidad y el equipo, se reinicia, el aplicativo genera el informe correspondiente.

Figura 11. Test teclado



Fuente: Elaboración propia

Figura 12. Sin problemas de compatibilidad



Fuente: Elaboración propia

Luego de realizar el PreChek, 152 equipos de 312, se encuentran en condiciones óptimas para el desarrollo del proyecto, los dispositivos, se encuentran distribuidos entre las gamas alta y media superan el proceso sin inconvenientes. En el siguiente listado, se muestran sus modelos.

Tabla 18. Equipos óptimos para el cifrado

Modelo	Cantidad	Gama
HP EliteBook 2540p	6	Alta
HP EliteBook 8470p	12	Alta
HP EliteBook 8570w	7	Alta
HP ProBook 440 G1	19	Alta
DELL Latitude E6410	17	Alta
DELL Precision 3541	70	Alta
HP EliteBook 2560p	8	Media
HP ProBook 6450b	13	Media
TOTAL	**152**	

Fuente: Documento de la institución

De los equipos óptimos, se concluye que los 70 equipos marca DELL, modelo Precision 3541 cumplen con las características técnicas ideales para la implementación del sistema de cifrado por sus altas prestaciones a nivel de hardware y software.

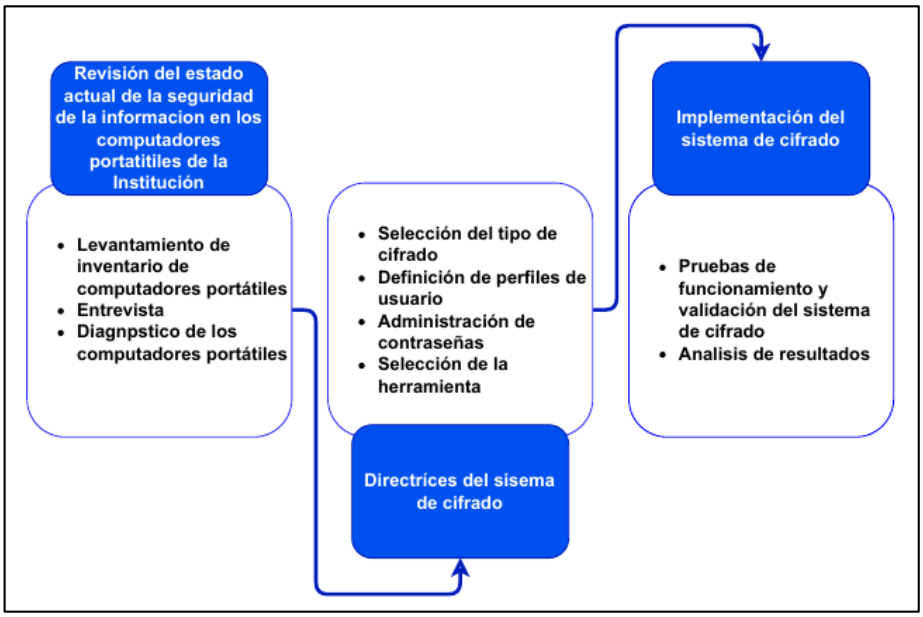
2.3 Metodología de desarrollo

Para la implementación del sistema de cifrado en computadores portátiles, y para llevar una ejecución ordenada, se inicia con el levantamiento de inventario de información de los computadores portátiles, se evaluó el estado actual del acceso a la información contenida en estos equipos, además, se analizan las directrices del sistema de cifrado según las necesidades de la institución.

El sistema de cifrado de computadores portátiles, se integra con un servidor de Directorio Activo (*Active Directory*) existente en la institución lo que facilita la gestión de dispositivos, además, se plantea la elaboración de la documentación técnica y normativa para la implementación del sistema de cifrado a nivel nacional.

La metodología utilizada en la implementación del sistema de cifrado, se la muestra, a continuación.

Figura 13. Metodología utilizada



Fuente: Modificado a partir de (Vanegas Lopez, 2018)

Selección de los tipos de cifrado

El estudio de sistemas y tipos de cifrado realizado en el capítulo uno del presente trabajo, determinó que el cifrado simétrico por bloques es el más adecuado para la implementación del sistema de cifrado de computadores portátiles por su rapidez de trabajo al momento de cifrar grandes cantidades de datos, además, se determina que el algoritmo AES con una longitud de clave de 256 bits es el indicado para la encriptación de información, es una combinación de rendimiento en software y eficiencia en hardware de dispositivos pequeños. Su comparativa con otros algoritmos de cifrado, se detallan en la Tabla 1.

Por su parte, la institución por medio del Oficial de seguridad recomienda utilizar el sistema de cifrado simétrico, y algoritmo AES con tamaño de clave de 256 bits, a la fecha, estas son consideradas las más seguras, además, se recomienda verificar esta

condición periódicamente con el objeto de efectuar las actualizaciones correspondientes[5].

Con los antecedentes descritos anteriormente, para la implementación del sistema de cifrado de computadores portátiles de selecciona el tipo de cifrado asimétrico por bloques con algoritmo de cifrado AES con una llave de longitud de 256 bits, por el alto grado de seguridad que brinda a la información confidencial y sensible de la institución.

Definición de perfiles de usuario

Para la administración del sistema de cifrado de computadores portátiles, se asigna un perfil de usuario maestro con la finalidad de controlar el cifrado y descifrado de los discos duros de los equipos, también, es necesario la creación de perfiles de consulta y administración de consola para la implementación del sistema de cifrado a nivel nacional.

Según directrices dadas por el Oficial de Seguridad de la información de la institución, se procede a la creación de los siguientes perfiles de usuario con sus responsables y funciones[6].

[5] Documento interno de la Institución.
[6] Documento interno de la Institución.

Tabla 19. Perfiles de usuario

Perfil	Responsable	Funciones	Observaciones
Super Admin	• Seguridad de la Información • Soporte al Usuario	• Administrador Principal	• Permisos totales • Usuario creado directamente en la consola del sistema de cifrado • Perfil con clave compartida
Consulta	• Seguridad Informática • Seguridad de la Información	• Agente de Seguridad Informática • Auditor	• Procesos de control • Consulta • Mismo usuario y contraseña del Active Directory
Operador	• Analista de Soporte Técnico	• Operador de Instalación • Operador de Endpoint • Operador de Vulnerabilidades y Parches	• Procesos de Instalación • Usuario y contraseña de envía por medio de correo electrónico
Supervisor	• Jefe de Soporte al Usuario	• Supervisor	• Supervisión de actividades • Mismo usuario y contraseña del Active Directory
Infraestructura	• Analista de Infraestructura	• Administrador de Vulnerabilidades y Parches • Administrador del Servidor • Administrador de Instalación	• Administración de Servidores • Mismo usuario y contraseña del Active Directory

Fuente: Modificado a partir de Documento de la Institución

Administración de contraseñas

La herramienta para utilizar en la implementación del sistema de cifrado de computadores portátiles garantiza la recuperación de claves de acceso en caso de olvido, además, de garantizar el acceso a la información, descifrando el disco duro, en caso de daños de sistema operativo o fallos físicos del equipo.

Herramienta para la implementación del sistema de cifrado

Con la finalidad de asegurar la operación diaria de los funcionarios y mantener protegida la información generada por estos, actualmente la institución posee una herramienta de Detección y Respuestas de Endpoints[7] (EDR) capa Advanced que dispone de una interfaz de gestión centralizada, permite la instalación, activación, configuración, actualización y administración de manera integral, que unifica la gestión de seguridad, a continuación, se muestra su descripción.

[7] Endpoint: Son equipos informáticos que forman parte de una red de datos, entre estos, tenemos: computadores de escritorio, computadores portátiles, impresoras entre otros.

Tabla 20. Descripción de antivirus institucional

Herramienta EDR			
Marca	**Version**	**Tipo**	**Observaciones**
Kaspersky	Kaspersky Endpoint Security for Business	Advanced	Licencia para protección de estaciones de trabajo, Servidores de Archivos y Dispositivos Móviles

Fuente: Elaboración propia

Entre sus principales características tenemos:

- Exploración de antivirus para contenido de disco.
- Protección de ataques desde la red.
- Potente anti-malware para terminales.
- Protección y seguridad de móvil para Smartphone y tabletas.
- Protección antihacker, antispyware.
- Actualización permanente y automática de firmas de virus.
- Consola de administración centralizada para equipos dentro de la red y en la nube.
- Control de dispositivos.
- Protección para sistemas operativos Windows y Linux.
- Cifrado.
- Capacidad de cifrar completamente el disco duro de la máquina, agrega un ambiente de preboot para autenticación de usuario.
- El acceso al recurso cifrado (archivo, carpeta o disco) garantizado aun en caso de que el usuario haya olvidado la contraseña, a través de procedimientos de recuperación.
- Utiliza, como mínimo, un algoritmo AES con llave de 256 bits.
- Capacidad de seleccionar carpetas y archivos (por tipo o extensión) para ser cifradas automáticamente gestionado por la misma consola de manera transparente para el usuario.

Dado que el EDR de la institución cubre todas las necesidades por sus características y prestaciones técnicas, se determina que esta herramienta posee todas las especificaciones necesarias para la implementación y realización de pruebas en el sistema de cifrado de computadores portátiles.

Implementación del sistema de cifrado

Los requisitos mínimos de hardware y software para el servidor de administración indicados en la página de Kaspersky son:

Tabla 21. Requisitos mínimos del servidor

Hardware		Software	
CPU	1,4 GHz Mínimo	**S.O.**	Windows Server 2012 o superior Windows 7 SP1 o superior
RAM	4 Gb Mínimo	**BD**	Microsoft SQL Server 2012 Express 64x o superior
Disco	10 Gb Mínimo 100 Gb Recomendable	Microsoft Data Access Components (MDAC) 2.8	
Arquitectura	32x 64x	Microsoft Windows DAC 6.0	
		Microsoft Windows Installer 4.5	

Fuente: Elaboración propia

Para la implementación del sistema de cifrado de computadores portátiles, la institución a designado un servidor virtualizado que tiene las siguientes características:

Tabla 22. Características del servidor

Hardware		Software	
CPU	2.7 GHz	**S.O.**	Windows Server 2012 Standart
RAM	8 Gb	**BD**	SQL Server 2014
Disco	300 Gb	Microsoft ODBC 11	
Arquitectura	64X	Incluido en Windows Server	
		Microsoft Windows Installer 5.0.9200	

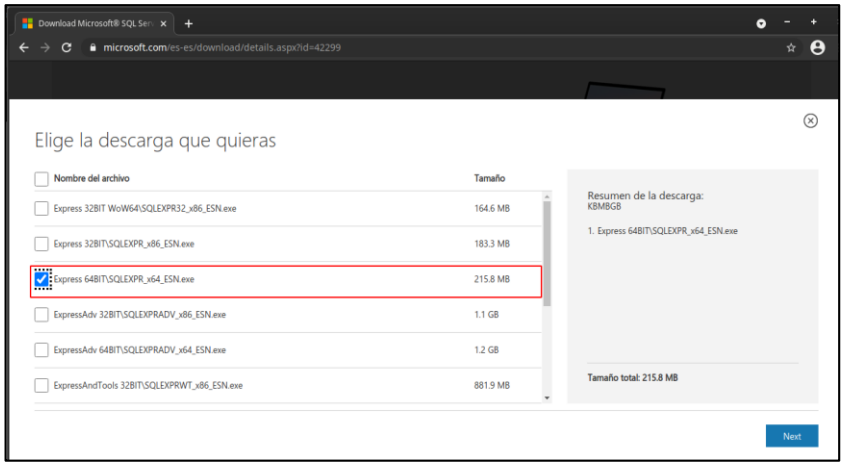
Fuente: Elaboración propia

Implementación de la consola de administración del sistema de cifrado

Instalación de motor de base de datos

- Se procede con la descarga de SQL server 2014 Express, de la página oficial de Microsoft, este sistema de administración de datos es gratuito, fiable y potente.

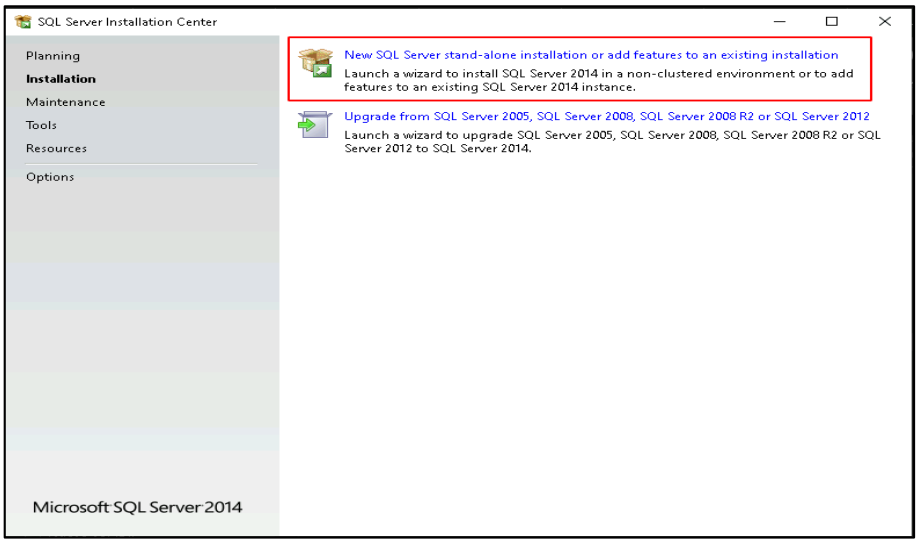
Figura 14. Descarga de SQL server 204 express



Fuente: Elaboración propia

- Ejecutamos el paquete de instalación, y seguimos el proceso de instalación por defecto.

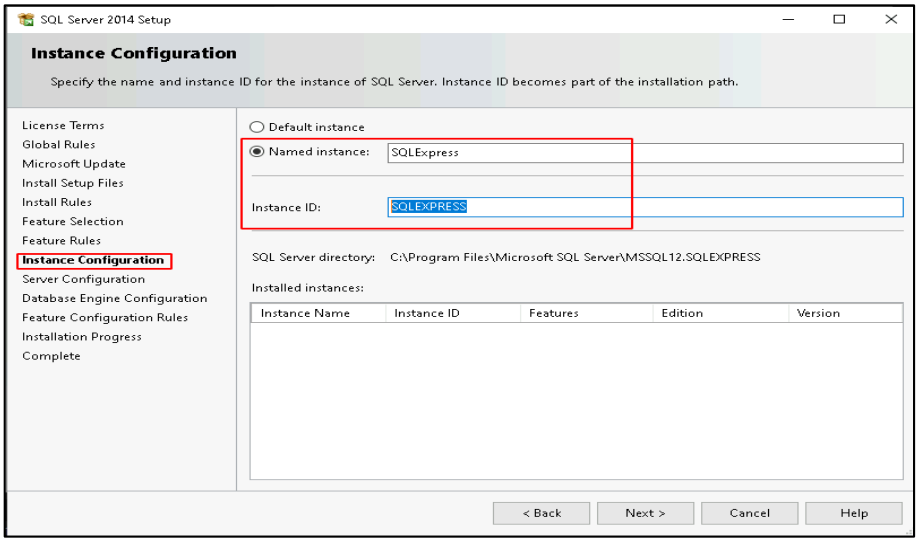
Figura 15. Instalación de SQL server



Fuente: Elaboración propia

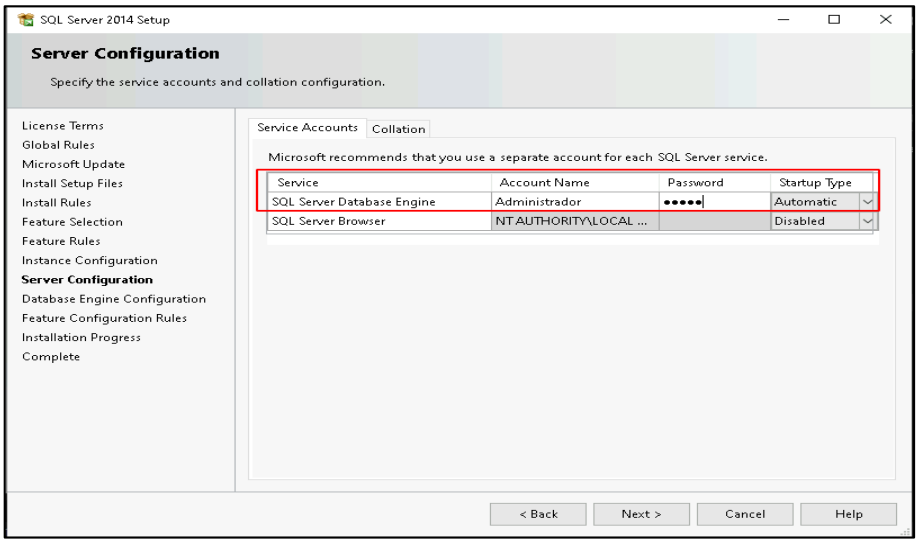
- Creamos una instancia y una base de datos para la Consola de Administración del Kaspersky.

Figura 16. Creación de instancia



Fuente: Elaboración propia

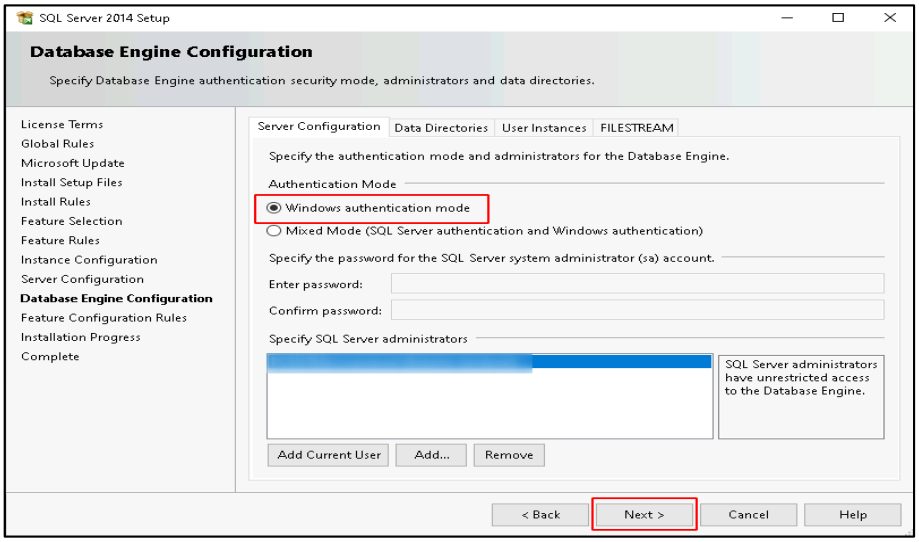
Figura 17. Creación de usuario para la base de datos



Fuente: Elaboración propia

- Seleccionamos la opción *Windows autentication mode* para ingresar a la base de datos con el usuario de dominio de Windows.

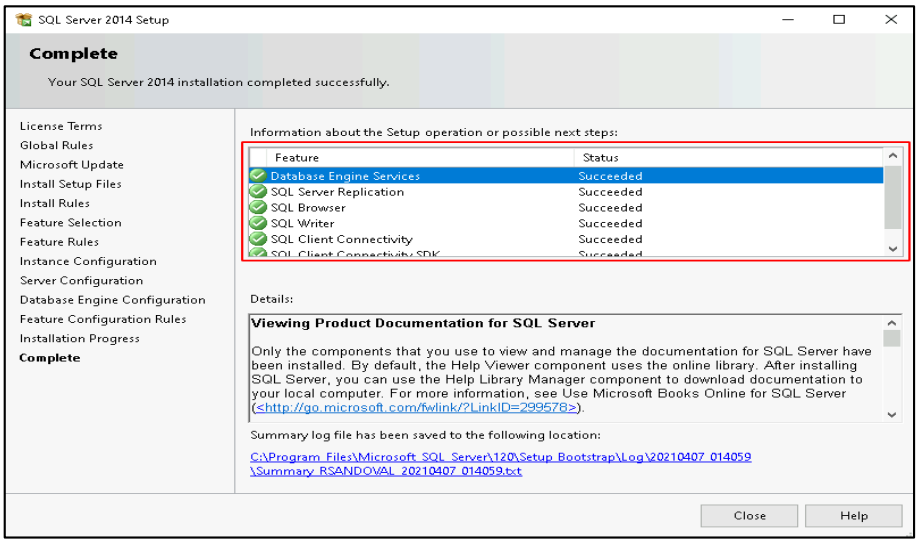
Figura 18. Autenticación del usuario en la base de datos



Fuente: Elaboración propia

- Una vez instalados todos los complementos de SQL Server cerramos la instalación.

Figura 19. Complementos de SQL server



Fuente: Elaboración propia

Instalación de consola de administración de cifrado

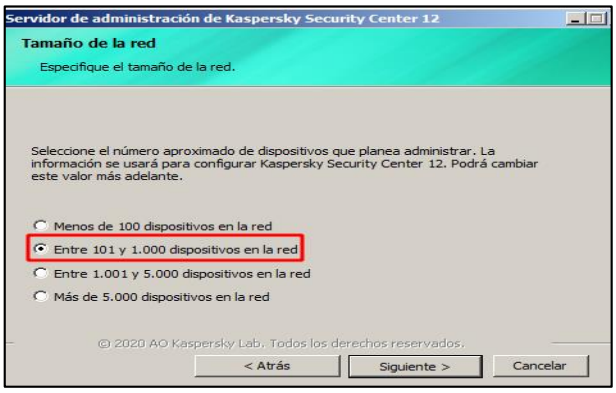
- Descargamos el instalador de la consola de Kaspersky Security Center de la página oficial, una vez descargado, se instala el software requerido, para la implementación del sistema de cifrado, se necesita instalar el software Kaspersky Security Center 12 o superior.

Figura 20. Instalación de kaspersky security center versión 12

Fuente: Elaboración propia

- La instalación, se realiza por defecto, se selecciona la cantidad de dispositivos, que se planea administrar, en el caso de la institución, existen 926 equipos, por tal motivo, se selecciona de 101 a 1000 dispositivos.

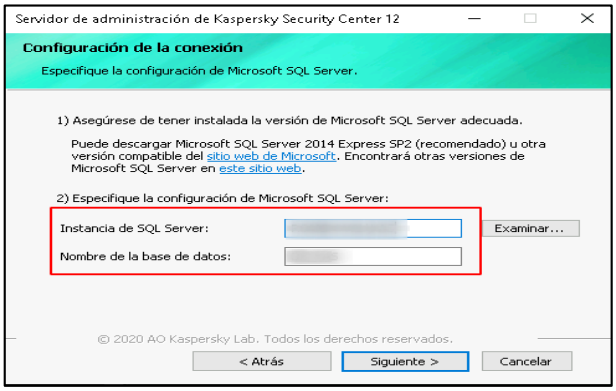
Figura 21. Selección de cantidad de dispositivos



Fuente: Elaboración propia

- Seleccionamos la instancia creada en el servidor SQL y, se le asigna un nombre a la base de datos

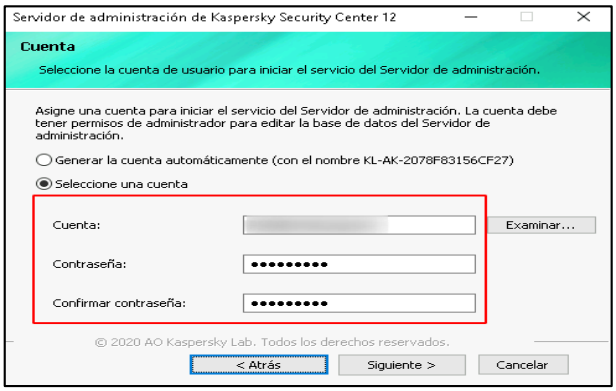
Figura 22. Selección de instancia de la base de datos



Fuente: Elaboración propia

- Se agregan los usuarios maestros que ingresarán a la consola para la administración y control.

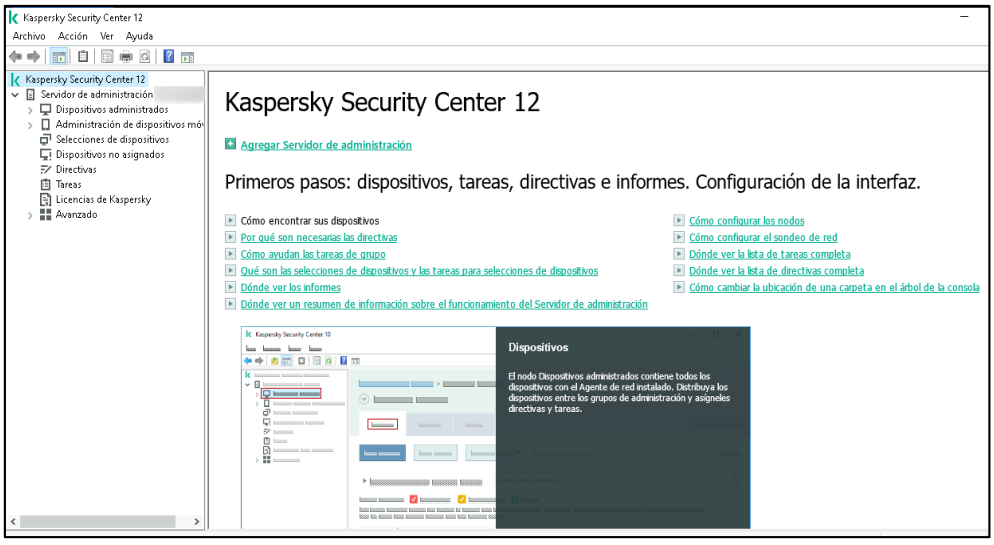
Figura 23. Cuanta de administrador de la consola del antivirus



Fuente: Elaboración propia

- EL software de instalación configura automáticamente los puertos y la longitud de la clave de cifrado para la conexión con el servidor de administración.
- Una vez finalizada la instalación del software, se puede observar la consola de administración.

Figura 24. Consola de administración Kaspersky

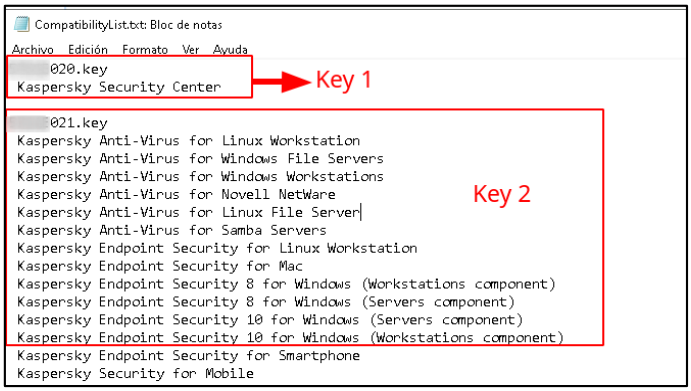


Fuente: Elaboración propia

Activación de licencias

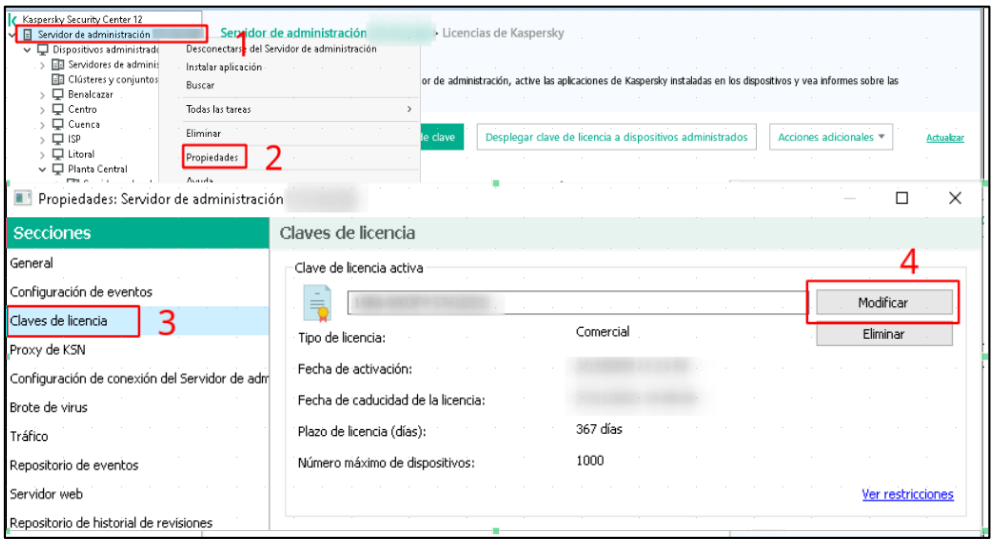
Luego de la instalación del aplicativo, se procede con la activa, la institución cuenta con una licencia tipo *Advanced* para 1000 dispositivos, la misma, consta de dos archivos que son cargados en la consola de administración, el primer archivo es utilizado para activar Kaspersky Security Center (consola de administración) y utilizar todas sus funciones; el segundo archivo, se lo carga en la consola para desplegarlo remotamente a los dispositivos administrados.

Figura 25. Archivos de licencia



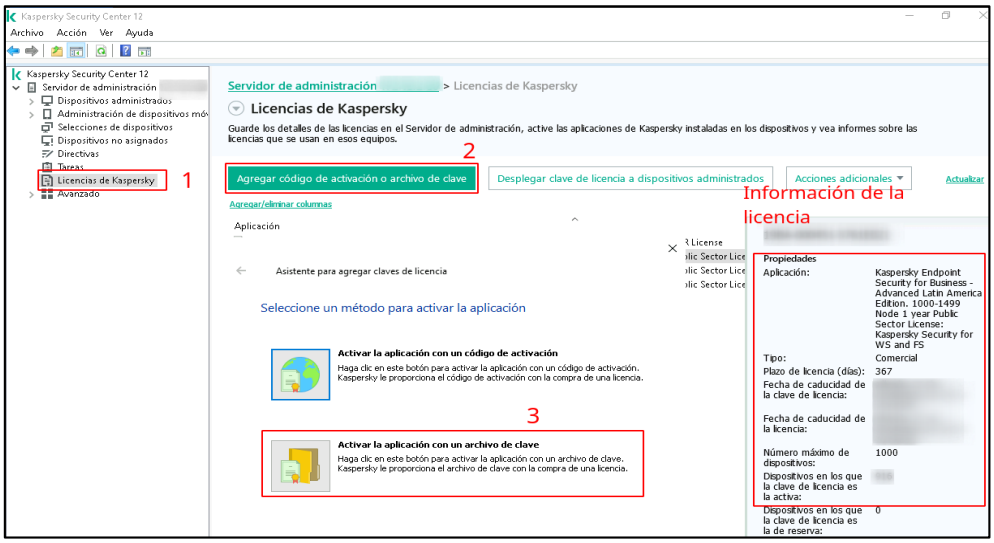
Fuente: Elaboración propia

Figura 26. Activación de Kaspersky Security Center



Fuente: Elaboración propia

Figura 27. Activación Kaspersky Security Endpoint

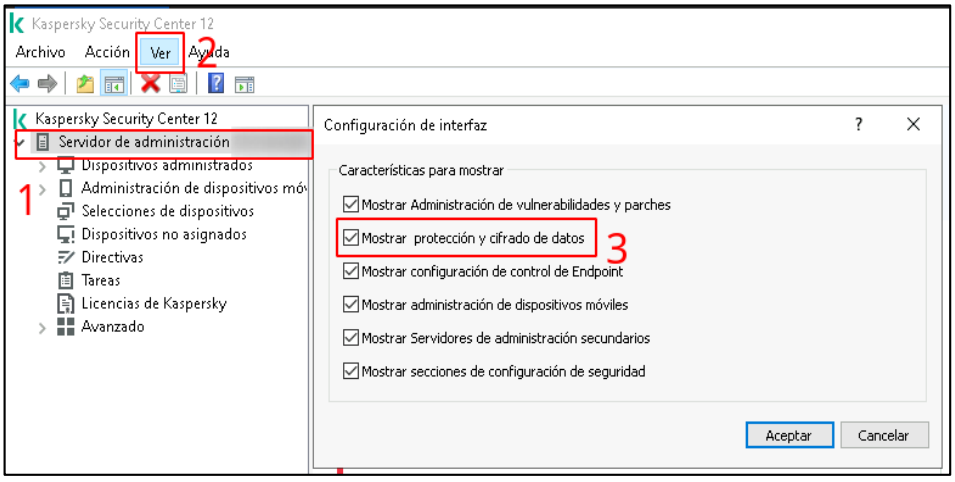


Fuente: Elaboración propia

Configuración de la consola para el proceso de cifrado

- Para el cifrado y protección de datos, se activan los componentes correspondientes necesarios, como se muestra, a continuación.

Figura 28.Activación de funciones de cifrado



Fuente: Elaboración propia

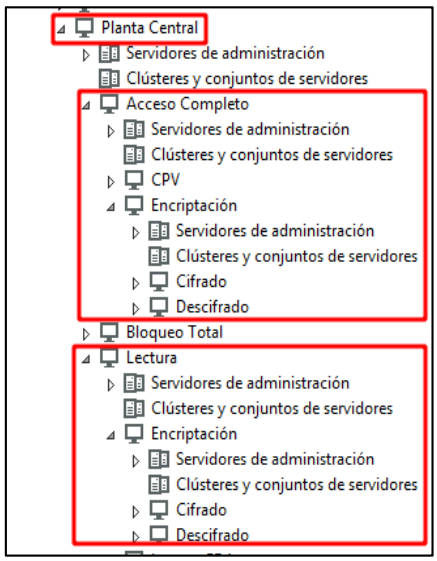
- Se crean los respectivos grupos para la aplicación de directivas de cifrado, para el presente caso de estudio, se crea el grupo PCENTRAL, su organización y grupos que lo integran, se muestran a continuación.

Tabla 23. Directivas de grupo

GRUPO PRINCIPAL	GRUPOS SECUNDADIOS		
PCENTRAL	ACCESO COMPLETO	ENCRIPTACION	CIFRADO
			DESCIFRADO
	BLOQUEO COMPLETO	ENCRIPTACION	CIFRADO
			DESCIFRADO
	LECTURA	ENCRIPTACION	CIFRADO
			DESCIFRADO

Fuente: Elaboración propia

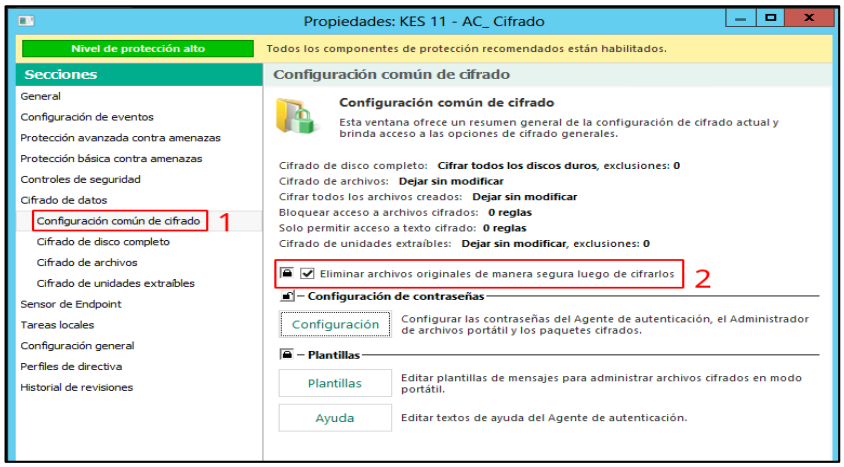
Figura 29. Grupos creados



Fuente: Elaboración propia

- El grupo ENCRIPTACION contiene las directivas de Cifrado y Descifrado de equipos, en la directiva, se ingresan las características de cifrado, en el presente caso de estudio, se configura la directiva global de cifrado de disco completo, la cual, nos indica, que se cifraran todos los discos duros del equipo, no se modificaran los archivos y los archivos originales, se eliminan luego de ser cifrados.

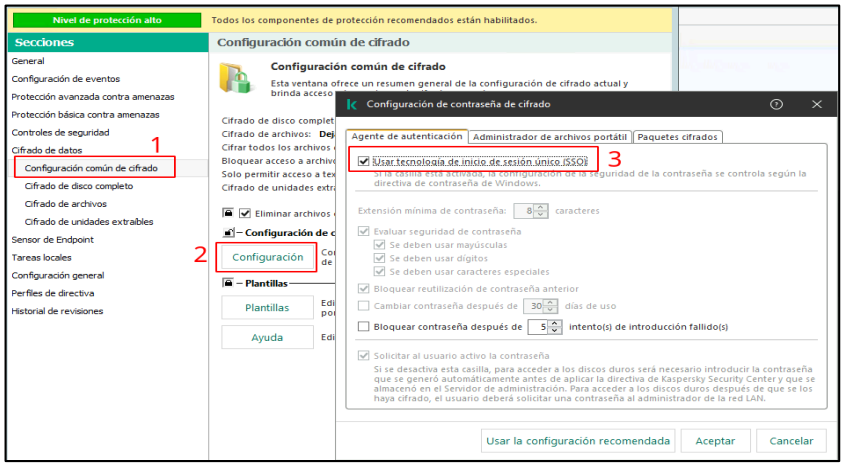
Figura 30. Configuración de directivas de cifrado



Fuente: Elaboración propia

- Para la autenticación de los usuarios, se utiliza la opción “Tecnología de inicio de sesión único SSO” para la autenticación por medio del usuario y contraseña creados por el administrador de la red en el Active Directory.

Figura 31. Configuración de acceso de usuario

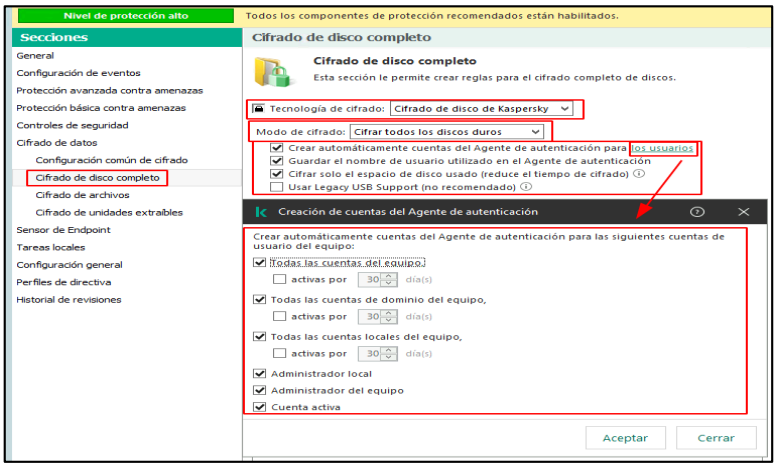


Fuente: Elaboración propia

- Para el cifrado de disco completo, se utiliza la “Tecnología de cifrado de disco Kaspersky”, esta tecnología, cifra el disco sector por sector, y al mismo tiempo todas las particiones lógicas del disco. Una vez cifrados los discos duros, al

próximo inicio de sesión la autenticación se realiza por medio del “Agente de Autenticación”, para esto, es necesario conocer el nombre de usuario y contraseña de la cuenta de usuario creada por el administrador de red.

Figura 32. Selección de tecnología de cifrado



Fuente: Elaboración propia

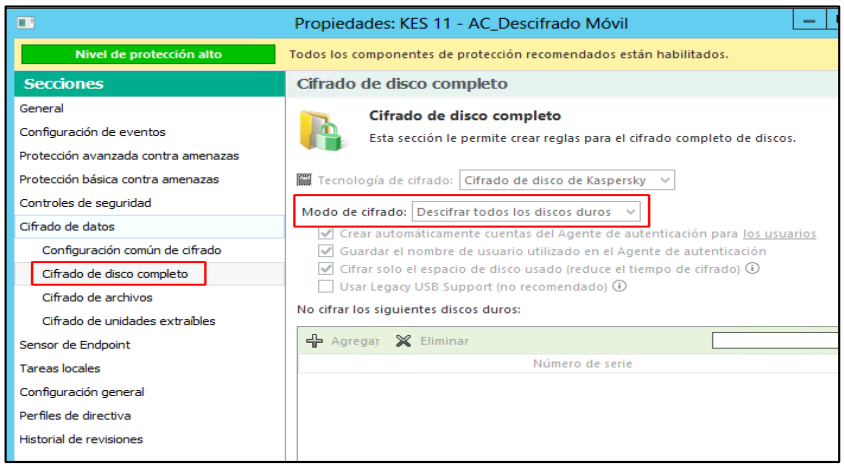
- Una vez realizada las configuraciones, la directiva queda activa para el grupo CIFRADO, esta, es aplicada a los dispositivos que lo integran. Para iniciar el proceso de cifrado de disco completo, se desplazan los dispositivos desde “Dispositivos Administrados” hacia el grupo correspondiente. Finalmente, se aplica el estado Directiva fuera de la oficina, en el caso de que un dispositivo abandone el perímetro de la red de la institución.

Figura 33. Directiva de cifrado creada

Fuente: Elaboración propia

- Para el grupo DESCIFRADO, se crea una directiva para descifrar todos los discos.

Figura 34.Directiva de descifrado creada

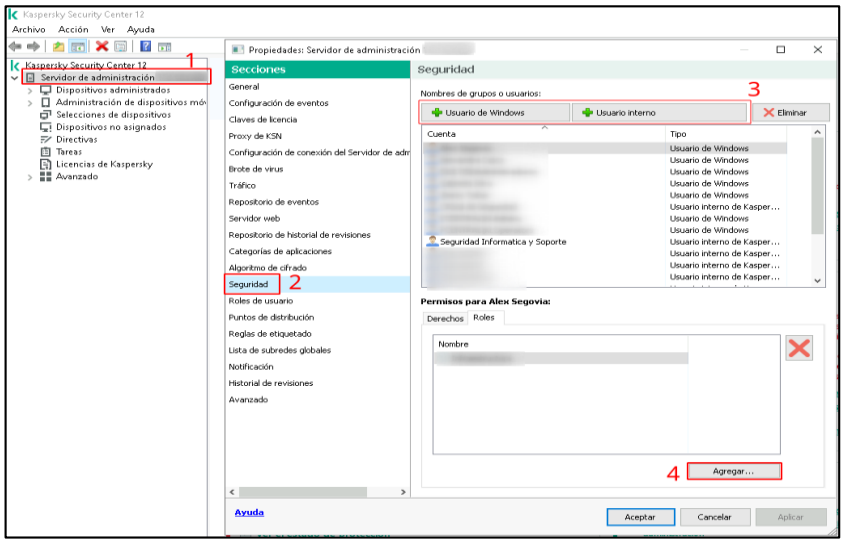


Fuente: Elaboración propia

Creación de perfiles de usuario

- En este apartado del documento se crean los perfiles y cuentas de usuario, para el uso adecuado de la consola de administración de la herramienta de cifrado. En primer lugar, se crean las cuentas de usuario, las cuentas de “Consulta, Supervisión e Infraestructura”, se usan los usuarios y contraseñas de Windows para el acceso a la consola de administración, razón por, la cual, se selecciona “Usuario de Windows”, los usuarios SuperAdmin y Operador, estos son creados directamente en la consola de administración por seguridad e integridad de la institución, en este caso, se selecciona “Usuario Interno”.

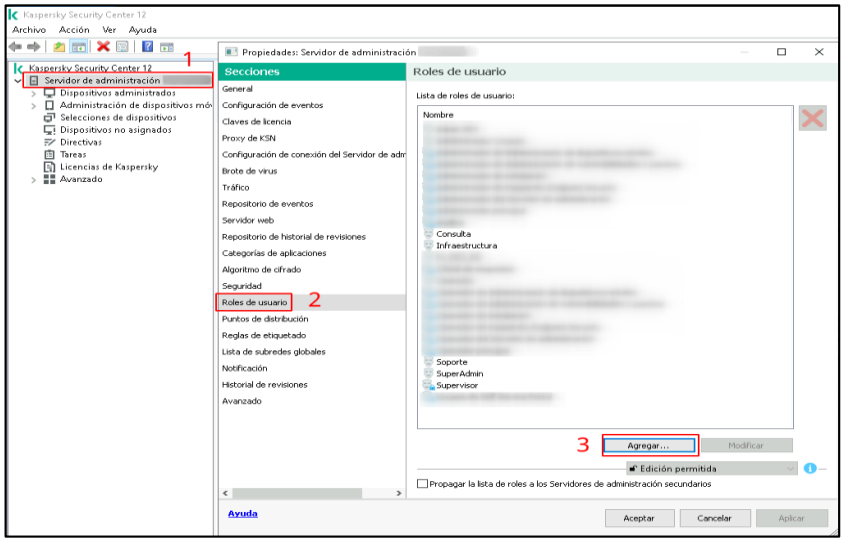
Figura 35. Creación de usuarios



Fuente: Elaboración propia

- En segundo lugar, se crean perfiles, que son asignados a las cuentas de usuario según los permisos correspondientes.

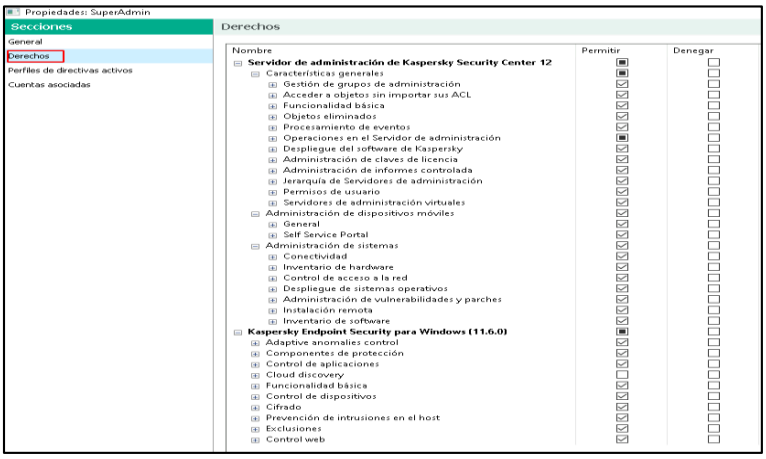
Figura 36. Creación de perfiles de usuario



Fuente: Elaboración propia

- **Perfil SuperAdmin:** usuario con permisos totales, este perfil, es asignado al administrador de la consola, este, realiza cambios globales a nivel consola, crea, modifica y elimina cuentas de usuario y sus respectivos perfiles.

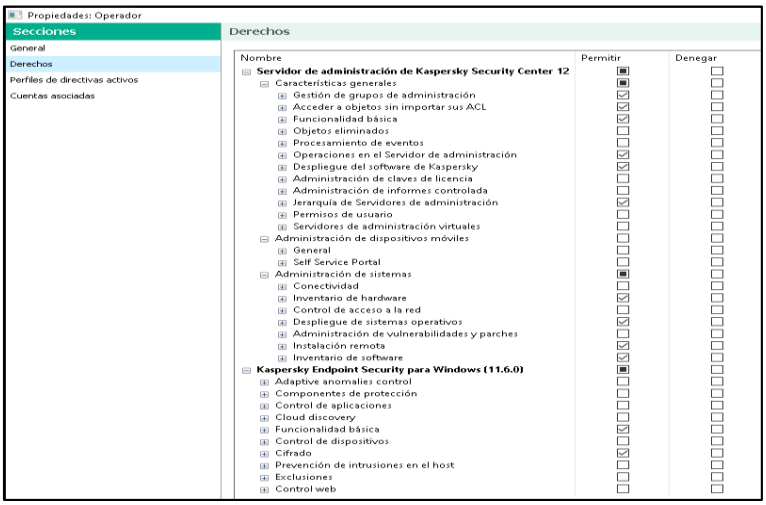
Figura 37. Permisos perfil SuperAdmin



Fuente: Elaboración propia

- **Perfil Operador:** asignado a los analistas de soporte técnicos de las sucursales de la institución para que continúen con el proceso de cifrado de equipos, a continuación, se muestran los permisos asignados.

Figura 38. Permisos perfil operador



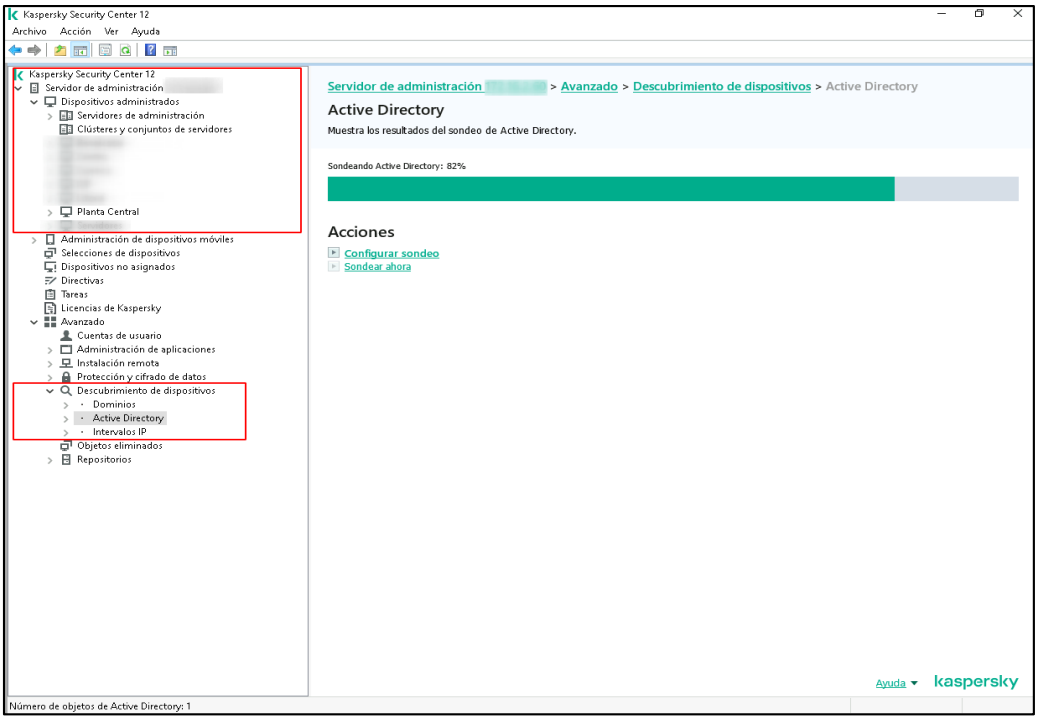
Fuente: Elaboración propia

- **Perfil Consulta:** este perfil tiene permisos de lectura de informes generados por la consola de administración y consulta de objetos eliminados (tareas, directivas, aplicaciones).
- **Perfil Supervisor:** este perfil tiene acceso de lectura y modificación a los informes generados por la consola de administración.
- **Perfil Infraestructura:** este perfil tiene acceso a la lectura y administración de puntos de distribución creados por la consola automáticamente dentro de la red la institución.

Pruebas de funcionamiento de la herramienta

Una vez implementada la herramienta, se procede a validar su funcionamiento, para esto, ingresamos a la consola de administración donde apreciamos los grupos creados, además, se realiza un escaneo de red para descubrir los equipos del Active Directory.

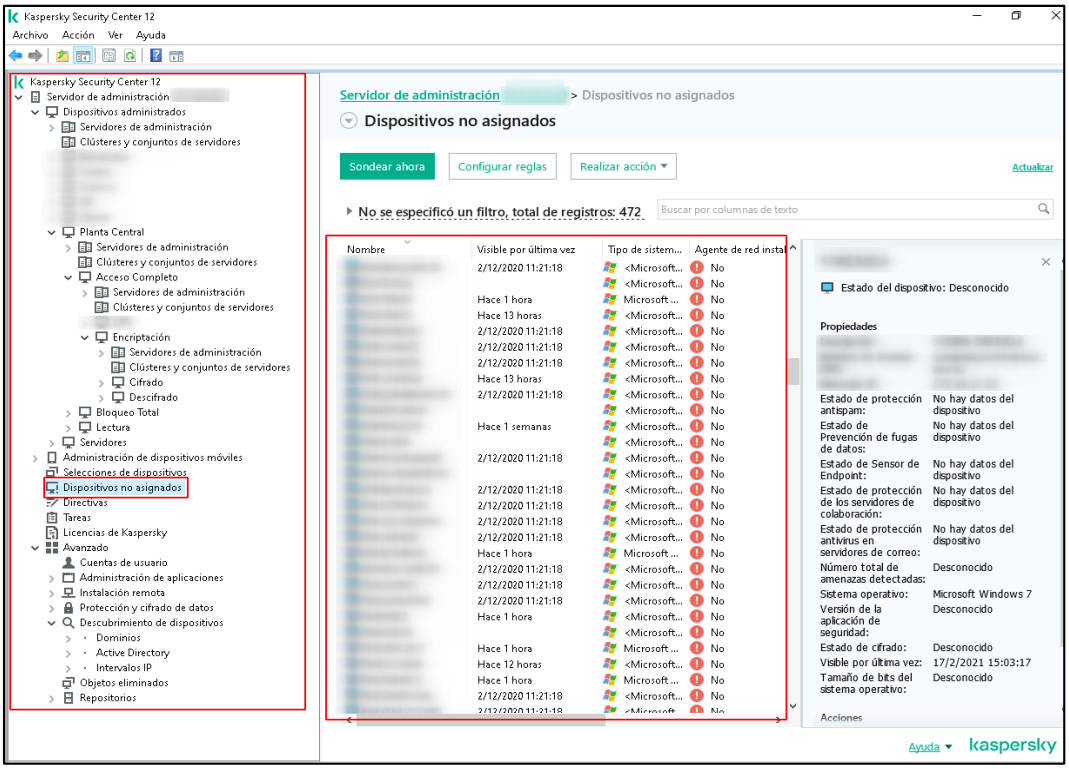
Figura 39. Sondeo de red



Fuente: Elaboración propia

Después del sondeo de red, apreciamos los equipos descubiertos por la consola de administración, donde nos muestra el nombre el equipo, sistema operativo, aplicación instalada y el tiempo de su última conexión. Los equipos descubiertos, se encuentran como no asignados, no tienen grupos ni directivas aplicadas.

Figura 40. Equipos descubiertos



Fuente: Elaboración propia

CAPÍTULO III. ANÁLISIS DE LOS RESULTADOS DE LA INVESTIGACIÓN

En este capítulo, se analizan los resultados obtenidos de la investigación realizada para la implementación del proyecto, para esto, se realizan pruebas de validación de funcionamiento con la finalidad de determinar el grado de confiabilidad del sistema. Las pruebas realizadas, se detallan, a continuación.

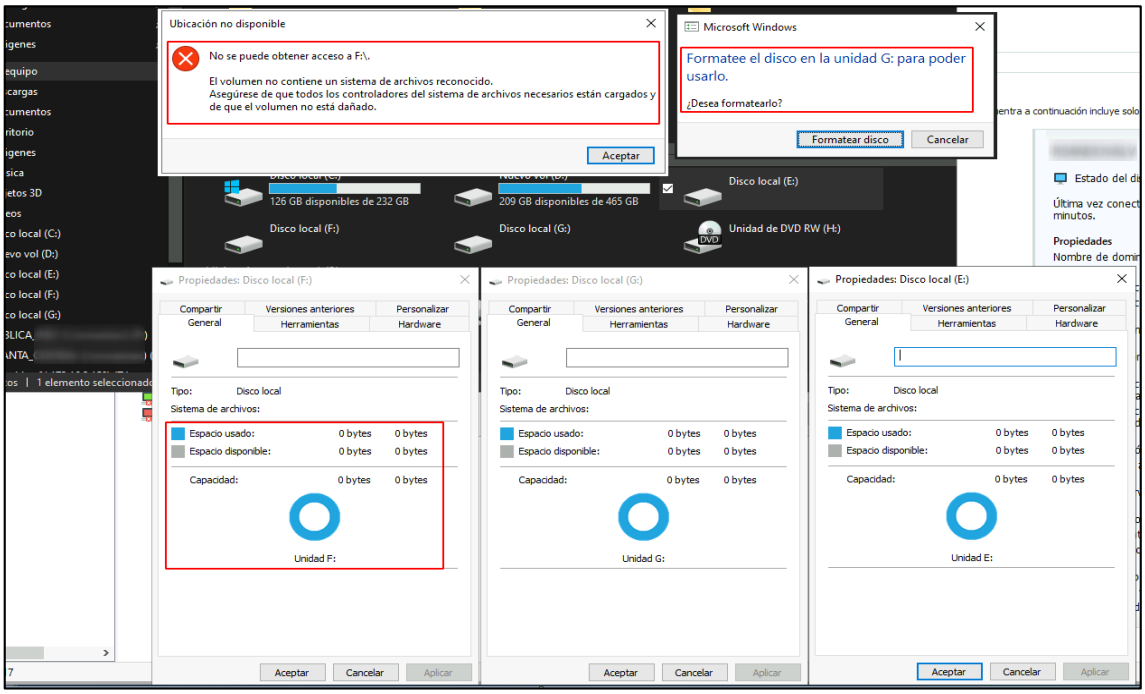
- **Conexión enclosure de disco duro:** para verificar el acceso al disco duro.
- **Ataque al disco duro:** para el ataque al disco duro, se crea una imagen del mismo con la ayuda del software FTK Imager.
- **Recuperación de la información:** para recuperación de información del disco cifrado, se utiliza el software Testdisk y Photorec.

3.1 Validación del sistema de cifrado

- **Conexión enclosure de disco duro**

Para verificar que el disco cifrado, se encuentre con un formato ilegible, se lo retira del computador portátil y con la ayuda de un enclosure lo conectamos en un equipo anfitrión, este, reconoce los discos montados como unidades E, F, G, dichas unidades de disco tienen un sistema de archivos desconocido, para utilizarlo, el equipo solicita el formateo del mismo, además, al ingresar a las propiedades, se observa que no tienen información almacenada, los resultados obtenidos, se muestran, a continuación.

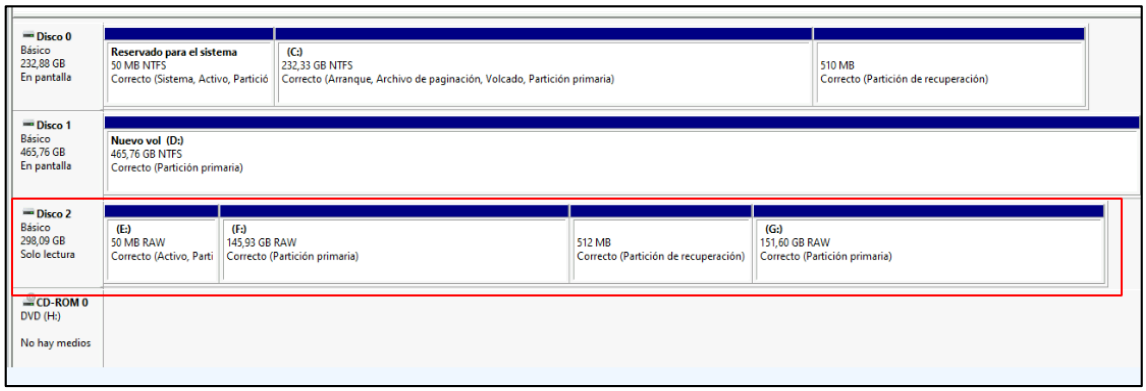
Figura 41. Discos ilegibles



Fuente: Elaboración propia

Otra forma de verificar el estado de los discos duros, es ingresar al administrador de discos de Windows donde, se aprecia que estos, se encuentran con formato RAW, lo que quiere decir que perdieron su sistema de archivos NTFS o FAT 32 y el sistema operativo no permite el acceso a ellos, lo que hace imposible recuperar los datos almacenados.

Figura 42. Discos en formato RAW



Fuente: Elaboración propia

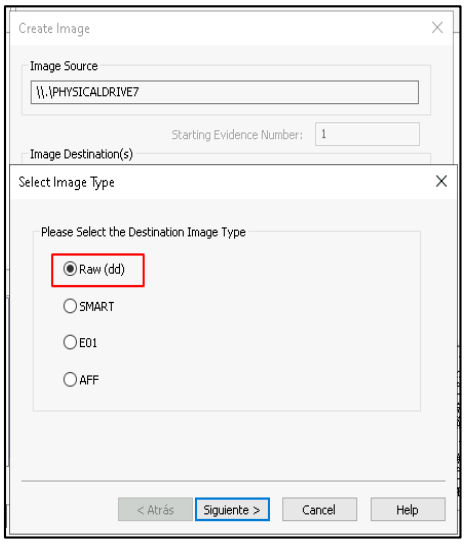
Como, se aprecia en la figura anterior, el disco completo, se encuentra cifrado, este tiene un formato ilegible y el formateo, es la única opción para acceder al dispositivo, esto ocasiona la pérdida total de la información contenida, y garantiza que personal no autorizado acceda a la misma; la confidencialidad e integridad de la información, no se ven afectadas.

- **Ataque al disco duro**

Para realizar esta prueba, se utiliza la herramienta FTK Imager, desarrollado por la empresa AccesData. Explica Granda (2015), es una herramienta forense que nos permite crear copiar perfectas del disco duro (imágenes forenses) sin realizar cambios en la evidencia original, con esto, se recupera usuarios, contraseñas, datos, entre otros, para luego ser analizados de forma hexadecimal.

Con la ayuda de FTK Imager, se procede a sacar una imagen del disco cifrado, seleccionamos entre varios formatos para la creación de la imagen bit a bit, se recomienda utilizar el formato RAW, es un formato de imagen sin particiones y, es estándar, por esta razón, la mayoría de herramientas de análisis forense lo reconoce. El tamaño de la imagen es igual al tamaño del disco origen.

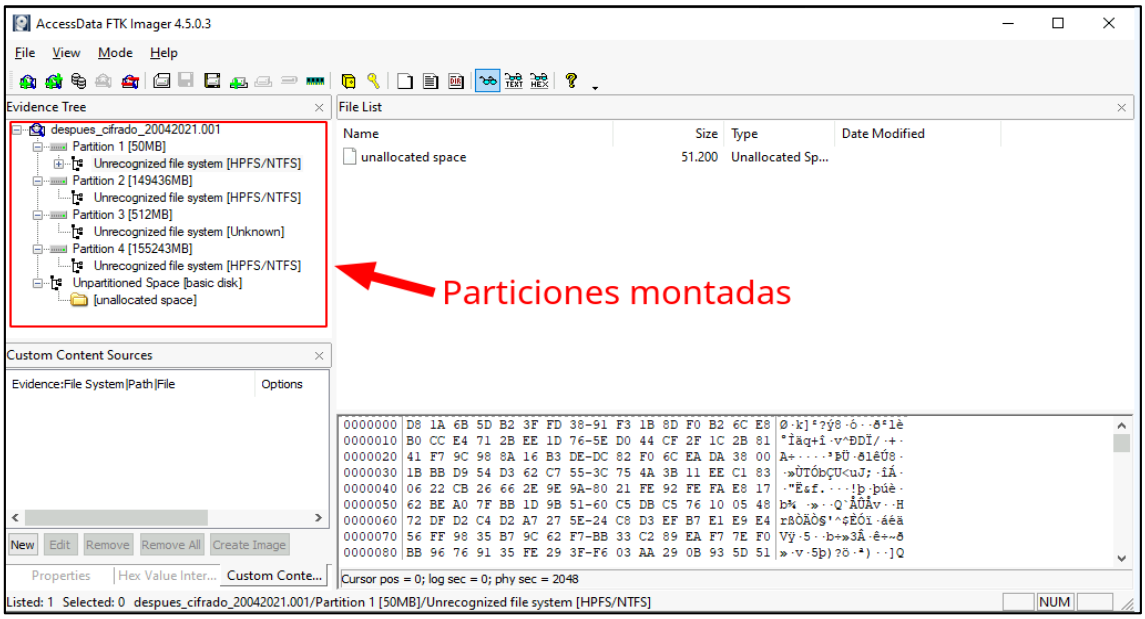
Figura 43. Clonación de disco duro con FTK Imager



Fuente: Elaboración propia

Una vez realizada la imagen procedemos a analizarla con la misma herramienta, para esto, cargamos la imagen antes creada con la opción "*Add Evidence Item*", luego de esto, apreciamos las particiones del disco cifrado montadas.

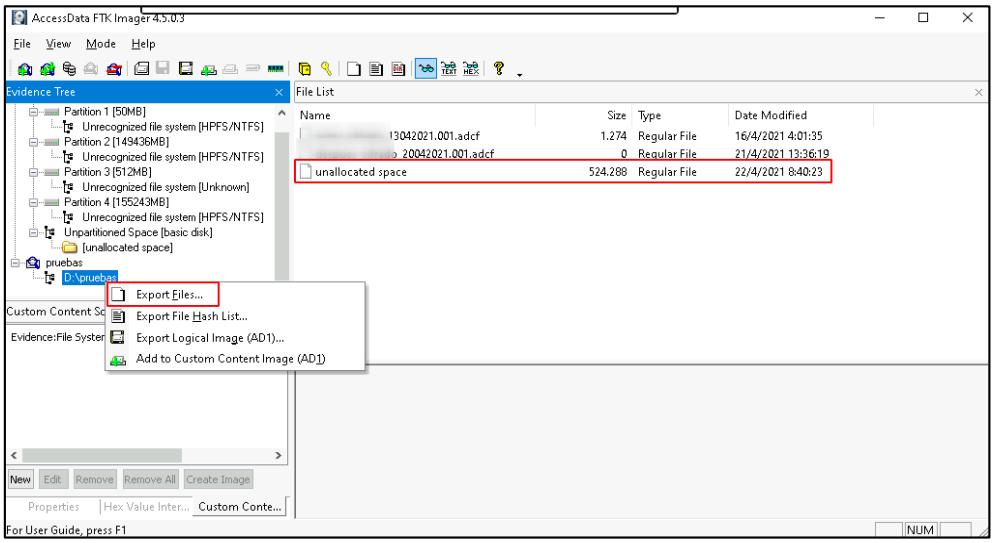
Figura 44.Análisis de la imagen de disco con FTK Imager



Fuente: Elaboración propia

Como observamos en la figura anterior, las particiones montadas en la herramienta, se encuentran con el mensaje de "*Unrecognized file system*" (sistema de archivos no reconocido), y no es posible acceder a la información contenida en el disco duro. La herramienta nos brinda la opción de extraer los archivos contenidos en las particiones para analizarlos, de igual manera, es imposible examinar los datos, tienen un formato desconocido.

Figura 45. Exportación de archivos

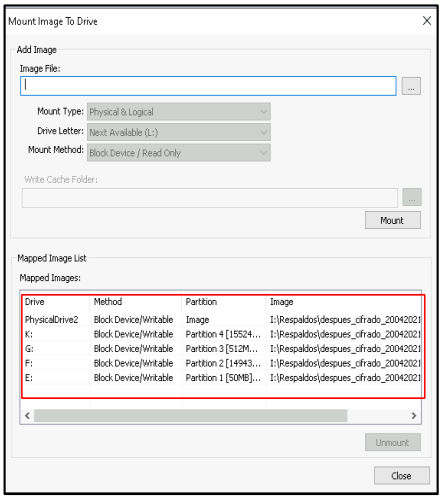


Fuente: Elaboración propia

- **Recuperación de la información**

Para esta prueba, se utiliza la imagen creada con FTK Imager, por motivos de seguridad y para no causar daños al disco físico de la computadora portátil. La recuperación de información, se realiza con las herramientas Testdisk y Photorec.

Figura 46. Imagen de disco montado con FTK Imager

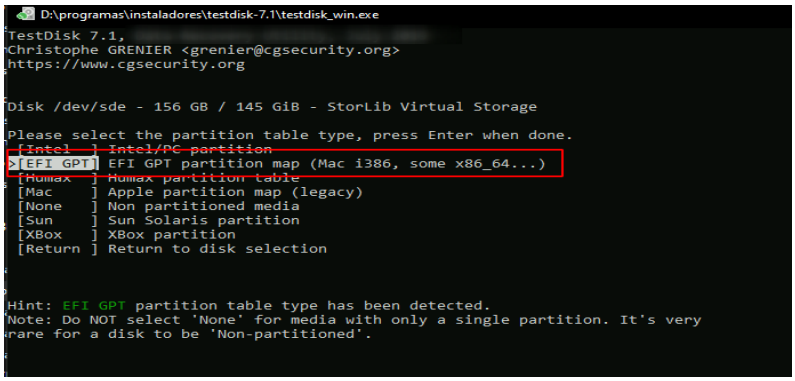


Fuente: Elaboración propia

- **Testdisk**

Explica Pérez García (2011), Testdisk, es una potente herramienta para la recuperación de información, es capaz de reconstruir sectores de arranque con los valores mínimos para que la unidad lógica sea accesible aunque no *booteable*.
Una vez montadas las particiones lógicas de la imagen de disco, se procede a ejecutar Testdisk para analizarlas y tratar de recuperar particiones y tener acceso a las mismas.

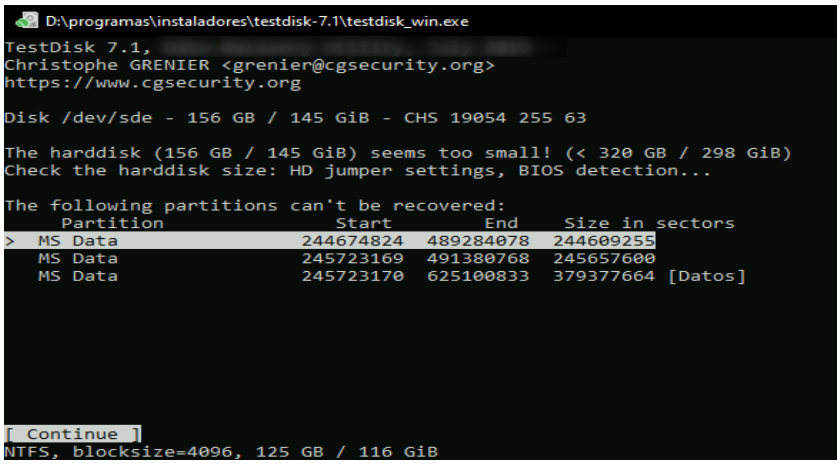
Figura 47. Análisis de disco con Testdisk



Fuente: Elaboración propia

Después de este proceso, la herramienta de análisis encuentra varias particiones en la imagen, estas, se muestran, a continuación.

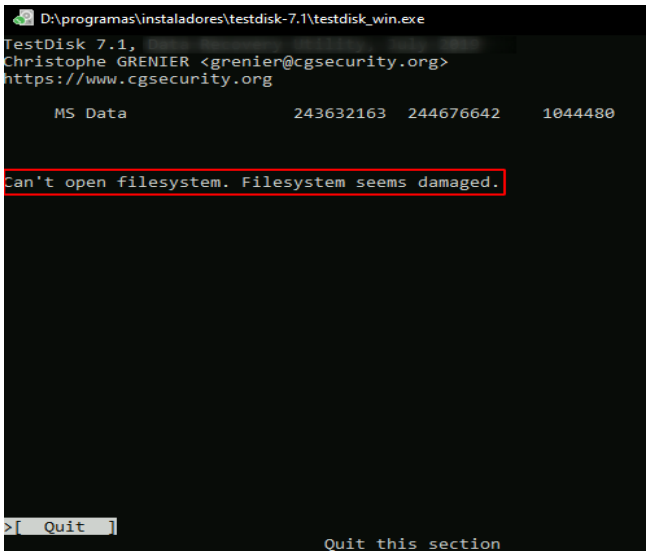
Figura 48. Particiones encontradas



Fuente: Elaboración propia

Ingresamos a la partición “Datos” recuperada por el software Testdisk para listar los archivos que contiene, observamos que la partición, se encuentra dañada y, no se tiene acceso a la misma.

Figura 49. Archivos inaccesibles

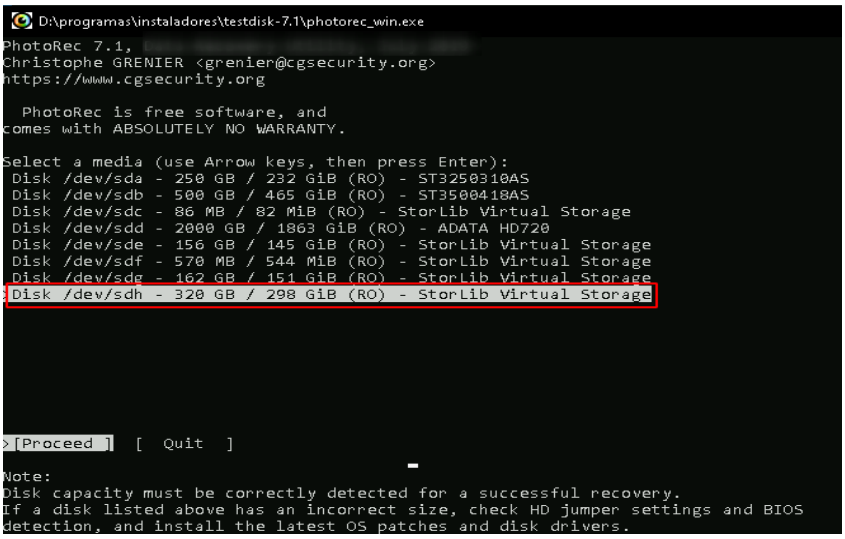


Fuente: Elaboración propia

- **Photorec**

En su trabajo de investigación Granda (2015) explica, Photorec, es un software de licencia GNU (Licencia Pública General), *open source*, especializado en la recuperación de imágenes, videos y documentos que han sido eliminados o perdidos, y cumple con los requisitos para mantener la integridad de la evidencia. Nos brinda la oportunidad de seleccionar el tipo de archivos a recuperar, lo que la hace una herramienta muy flexible.

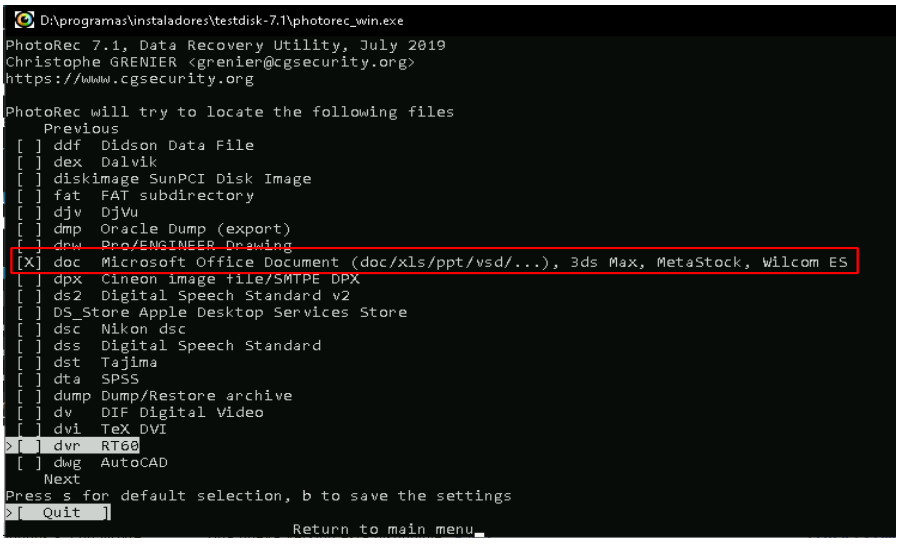
Figura 50. Análisis de disco con Photorec



Fuente: Elaboración propia

Para la recuperación de información del disco de prueba, se configura el software Photorec para que busque y recupere archivos de Microsoft Office (Word, Excel, Power Point).

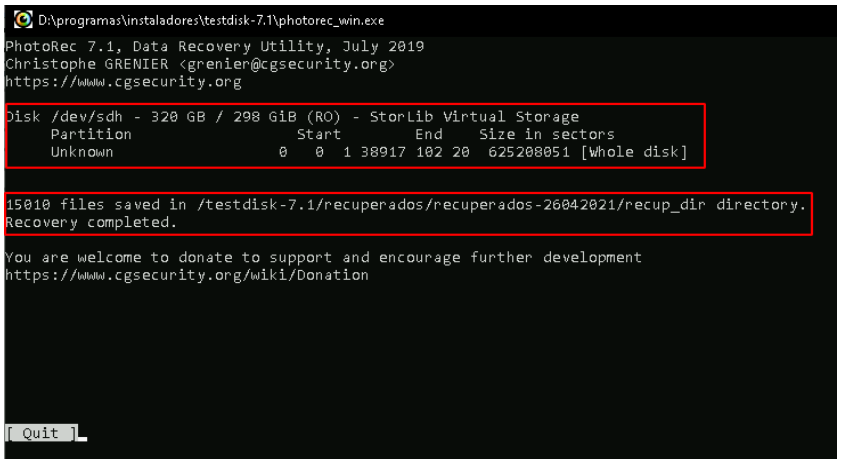
Figura 51. Configuración de software Photorec



Fuente: Elaboración propia

El tiempo de recuperación de información varía según la capacidad del disco, esta herramienta realiza un análisis sector por sector y recupera los archivos con las extensiones indicadas en su configuración.

Figura 52. Resultados Photorec



Fuente: Elaboración propia

El software Photorec recuperó 15010 archivos de diferentes extensiones después de analizar el disco completo. La información recuperada corresponde a la parte del disco, que se encuentra libre o no utilizada, los datos del usuario actual del equipo, se encuentran encriptados y el software no tiene acceso a estos, y no son manipulables por parte de terceras personas.

Resumen de los resultados de las pruebas realizadas

A continuación, se muestra un resumen de los resultados de las pruebas realizadas, a los discos cifrados.

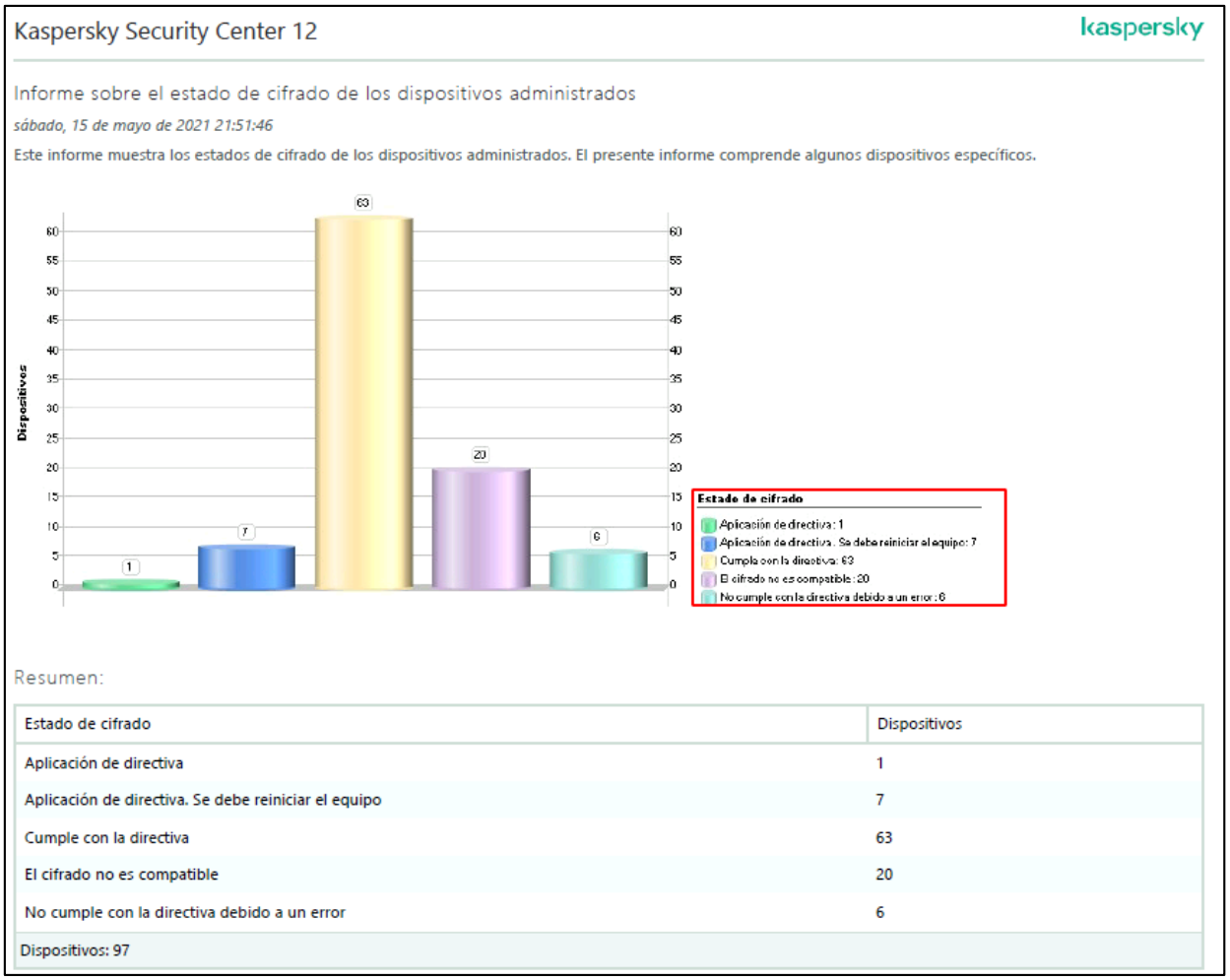
Tabla 24. Resultados de pruebas realizadas

Prueba realizada	Herramienta	Observaciones	Acceso a la información
Conexión del disco cifrado en otro equipo	Enclosure	• El disco cifrado se encuentra en formato desconocido, se debe formatear para poder utilizarlo.	No
Ataque al disco duro	FTK Imager	• Con la ayuda del software se crea una bit a bit, se analiza la imagen creada, las particiones del disco cifrado se muestran como extensiones desconocidas.	No
Recuperación de las particiones	Testdisk	• Se analiza la imagen del disco cifrado, después de este proceso no se puede restaurar las particiones, estas aparecen como desconocidas.	No
Recuperación de información	Photorec	• Se analiza la imagen del disco cifrado, se recupera información de la parte del disco no utilizado, los datos recuperados corresponden a sectores formateados disco.	Se recupera información de la parte no utilizada del disco, los datos del usuario actual del equipo se mantienen cifrados y no son accesibles

Fuente: Elaboración propia

Una vez realizada la validación de funcionamiento del sistema de cifrado, se procede con la implementación del cifrado de disco completo en los equipos que integran de la población del presente proyecto, a continuación, se muestra un informe de los equipos encriptados.

Figura 53. Informe de equipos cifrados



Kaspersky Security Center 12

kaspersky

Informe sobre el estado de cifrado de los dispositivos administrados

sábado, 15 de mayo de 2021 21:51:46

Este informe muestra los estados de cifrado de los dispositivos administrados. El presente informe comprende algunos dispositivos específicos.

Resumen:

Estado de cifrado	Dispositivos
Aplicación de directiva	1
Aplicación de directiva. Se debe reiniciar el equipo	7
Cumple con la directiva	63
El cifrado no es compatible	20
No cumple con la directiva debido a un error	6
Dispositivos: 97	

Fuente: Elaboración propia

CONCLUSIONES

- La fundamentación teórica de los sistemas de cifrado, evidencia los riesgos de fuga de información en instituciones públicas y privadas, donde, los dispositivos portátiles son los más difíciles de proteger por su alta movilidad fuera de las instalaciones, para esto, los sistemas de cifrado brindan la oportunidad de salvaguardar la información contenida en este tipo de dispositivos.

- El diagnóstico del estado actual de la información y del hardware de los computadores portátiles de la institución expone las vulnerabilidades de los mismos debido a sus deficientes características técnicas y software desactualizado, se encontró que la información de los discos de los equipos estaba completamente libre para el acceso a cualquier usuario, además, se realizó una prueba PreCheck, para determinar que los equipos dentro de la organización son óptimos para la implementación del sistema de cifrado.

- La implementación del sistema de cifrado de información demuestra la factibilidad de uso del software antivirus de la institución para el desarrollo del proyecto en estudio debido a sus altas prestaciones técnicas y gran cantidad documentación existente en el internet. Para este proceso de implementación, se propone en este trabajo una metodología de trabajo de tres pasos – Revisión – Directrices – Implementación) Ver figura 13. En el proceso de revisión los equipos cumplen los requerimientos técnicos de implementación y control basado en los datos recopilados por el *Active Directory*, en el estudio de directrices, se analizan tanto las opciones de cifrado, se encuentra como la mejor opción para este trabajo el cifrado AES con una llave de longitud de 256 bits, en cuanto a las directrices institucionales, se opta por el diseño de cinco perfiles de usuario para los equipos los mismos que muestran resumidos en la tabla 19, luego del estudios correspondiente, se selecciona como herramienta de cifrado a la provista por la empresa Kaspersky.

- La documentación generada con este trabajo de titulación, proporciona las pautas necesarias para la réplica del sistema de cifrado, en otras instituciones púbicas del Ecuador con condiciones de trabajo similares al ambiente de estudio, además, de presentar opciones técnica de metodología practica que muestra lineamientos herramientas y técnicas que serán fácilmente adoptadas por cualquier organización, además, es un punto de partida en entidades públicas o privadas, que se encuentren en desarrollo de este tipo de proyectos, puesto que cuenta con un análisis enmarcado en las políticas públicas actuales.

- La validación del funcionamiento del sistema de cifrado, confirma que solo personal autorizado accede al dispositivo portátil cifrado. En caso de pérdida o robo del equipo, la información, se mantiene ilegible y para utilizar el disco duro es necesario formateado. En caso de daño completo del equipo o fallas del sistema operativo, es posible recuperar la información cifrada mediante un procedimiento detallado en la documentación operativa del presente documento.

RECOMENDACIONES

- Se recomienda mantener un estudio del estado del arte actualizado de forma que este mismo plan, se mantenga actualizado en función del tiempo. Se agrega a la propuesta nuevas herramientas nuevas técnicas o normativas internas de las organizaciones que le den vigencia a la propuesta en el tiempo. Como los dispositivos tecnológicos son por naturaleza de entre los equipos con mayor crecimiento tecnológico cada vez, se presentan nuevas tendencias por lo que es importante mantener una vigilancia tecnológica.

- Se recomienda establecer procedimientos de diagnóstico de equipos computacionales al interior de la institución de forma, que se apliquen criterios unificados, que faciliten el proceso de adquisición y potenciamiento de los equipos tecnológicos sin afectar las capacidades de encriptación propuesta en este trabajo.

- Capacitar constantemente al personal encargado de la administración de la herramienta de cifrado, para la solución de problemas presentados y solicitar soporte técnico al fabricante solamente cuando sea necesario.

- Se recomienda mantener vigente el proceso planteado en el cifrado de equipos, se ajusta al proceso metodológico planteado, que si bien, es cierto, es sencillo, pero ha demostrado efectivo en el logro de los objetivos de mejora de la seguridad de los datos de los equipos con mayor movilidad dentro de la organización como son los equipos portátiles.

- Mantener actualizada la documentación operativa del sistema de cifrado y difundirla adecuadamente dentro de la organización de forma que tanto el personal técnico como el operativo comprenda el alcance y beneficios que este proceso aporta a la organización. No cabe duda que buena parte de la efectividad de este proceso radica en la capacidad de uso del personal

operativo, quien comprende los beneficios individuales e institucionales que la propuesta aporta para la organización.

- Realizar mantenimientos periódicos a la consola de administración del sistema de cifrado, para la liberación de licencias no utilizadas y que estas sean asignadas a otros equipos.

- Garantizar el soporte técnico por parte del fabricante o proveedor del software antivirus, vía remota o en sitio cuando la situación lo requiera.

BIBLIOGRAFÍA

Asamblea Nacional del Ecuador. (2015). Constitución del Ecuador. *Registro Oficial*. https://www.asambleanacional.gob.ec/sites/default/files/constituciondelarepublicadelecuador-incluyereformas-consultapopular7demayo.pdf

Cáceres Tarco, C. E., & Mena González, C. E. (2015). *Elaboración de la guía de implantación de las normas prioritarias del esquema gubernamental de seguridad de la información EGSI en las entidades de la administración pública central*. http://bibdigital.epn.edu.ec/handle/15000/11234

Chala, Y. F. (2019). *Importancia de la aplicación del mecanismo de cifrado de información en las empresas para la prevención de riesgos como ataques, plagio y pérdida de la confidencialidad*. https://repository.unad.edu.co/handle/10596/30745

Congreso Nacional del Ecuador. (2004). Ley Organica de Transparencia y Acceso a la Informacion Pública. *Lotaip*, 1–10. https://www.oas.org/juridico/PDFs/mesicic5_ecu_ane_cpccs_22_ley_org_tran_acc_inf_pub.pdf.

Corrales Sanchez, H. (2012). *Criptografía y Métodos de Cifrado*. https://es.calameo.com/read/0054906781e7d9236ba1a

Diaz Bravo, L., Torruco Garcia, U., Mildred, M. H., & Margarita, V. R. (2013). La Entrevista, recurso flexible y dinámico. *Investigación En Educación Médica*, *2*(7), 162–167. http://www.scielo.org.mx/scielo.php?pid=S2007-50572013000300009&script=sci_arttext

ESET. (2014). Cifrado de la información. *Enjoy Safer Technology*, 26. https://www.welivesecurity.com/wp-content/uploads/2014/02/guia_cifrado_corporativo_2014.pdf

Gómez Rivadeneira, M. B. (2013). Cifrado de datos transmitidos a través de redes inalámbricas. In *Pontificia Universidad Católica del Ecuador*. http://repositorio.puce.edu.ec/handle/22000/6242

Granda, G. E. (2015). *Metodología para el análisis forense de datos e imágenes de acuerdo a las leyes del Ecuador*. https://dspace.ups.edu.ec/handle/123456789/8943

INCIBE. (2013). Protección de la información. *INCIBE*, 18–22. https://www.incibe.es/sites/default/files/contenidos/dosieres/metad_proteccion-de-la-informacion.pdf

INCIBE. (2015). *Ciberespionaje, criptografía y criptobulos*. https://www.incibe-cert.es/blog/ciberespionaje-criptografia

INEC. (2020). *Organigrama*. https://www.ecuadorencifras.gob.ec/organigrama-1/

INEN. (2015). NTE INEN ISO/IEC 27001 - Tecnologías de la información —Técnicas de seguridad — Sistemas de gestión de seguridad de la información – Requisitos. *INEN*, 1–5. https://www.normalizacion.gob.ec/buzon/normas/nte_inen_iso_iec_27001.pdf

INEN. (2017). *NTE INEN ISO/IEC 27002 - Tecnologías de la información — Técnicas de seguridad — Código de práctica para los controles de seguridad de la información*. 1–5. https://www.normalizacion.gob.ec/buzon/normas/nte_inen_iso_iec_27001.pdf

Ledezma Espín, D. N. (2015). *Desarrollo de políticas de seguridad de la información basadas en las Normas ISO 27002 para una Coordinación Zonal del INEC*. 112. http://repositorio.pucesa.edu.ec/handle/123456789/1555

Manosalvas García, C. E. (2015). *Análisis e investigación de la seguridad de la información en la Autoridad Portuaria de Manta y como el esquema*

gubernamental de seguridad de la información, apoyo a fortalecer la infraestructura tecnológica y seguridad de la institución. http://repositorio.ug.edu.ec/handle/redug/43915

Medina Vargas, Y., & Miranda Mendez, H. (2015). Comparación de algoritmos basados en la criptografía simétrica DES, AES y 3DES. *Mundo FESC*, *1*(9), 14–21. https://dialnet.unirioja.es/servlet/articulo?codigo=5286657

MINTEL. (2013). *Esquema Gubernamental de Seguridad de la Información EGSI*. 1–47. https://www.gobiernoelectronico.gob.ec/wp-content/uploads/2020/01/Registro-Oficial-Acuerdo-Ministerial-No.-025-2019-EGSI-version-2.0.pdf

MINTEL. (2020a). *Esquema Gubernamental de Seguridad de la Información V2*. https://www.gobiernoelectronico.gob.ec/wp-content/uploads/2020/01/Registro-Oficial-Acuerdo-Ministerial-No.-025-2019-EGSI-version-2.0.pdf

MINTEL. (2020b). *Ranking de evaluación a las entidades gubernamental de seguridad de la información V1*. https://www.gobiernoelectronico.gob.ec/wp-content/uploads/2020/11/Ranking_Evaluacion_EGSI-15_1.pdf

Pérez García, M. (2011). *Recuperación de información en discos duros electromecánicos a nivel físico y lógico para su análisis forense informático*. http://www.repositoriodigital.ipn.mx/handle/123456789/12669

Perugachi Betancourt, M. L. (2020). *Diseño de una política de seguridad de la información para la dirección de gestión económica de la Arcotel, basada en las normas ISO 27002:2013 Y EGSI*. http://repositorio.uisek.edu.ec/handle/123456789/3797

Presidencia del Ecuador. (2011). *Estatuto Regimen Juridico Administrativo*. *338*, 1–64. https://www.defensa.gob.ec/wp-content/uploads/downloads/2018/05/ERJAFE_abr18.pdf

Roca Busó, L. (2015). *Seguridad Informática: Criptografía*. Minubeinformatica.Com. http://minubeinformatica.com/cursos/seguridad-informatica/criptografia

Serrano Losada, H. D. (2019). Comparación de métodos criptográficos para la seguridad informática. *Universidad Nacional Abierta y a Distancia UNAD*, *May*, 1–9. https://repository.unad.edu.co/handle/10596/30318

Vanegas Lopez, R. M. (2018). *Implementación de un sistema de protección de la información confidencial en dispositivos portátiles de universidad central de Nicaragua, empleando técnicas de cifrado con gestión centralizada*. http://ribuni.uni.edu.ni/id/eprint/2548

ANEXOS

ANEXO 1. Documentación Normativa

Resolución No. 030

CONSIDERANDO

Que, la constitución de la República del Ecuador el artículo 227 de la Constitución de la República del Ecuador dispone que la administración pública constituye un servicio a la colectividad, que se rige por los principios de eficiencia, calidad, jerarquía, desconcentración, descentralización, coordinación, partición, planificación, transparencia y evaluación;

Que, mediante Acuerdo Ministerial No. 166 de 19 de septiembre de 2013, publicado en el Suplemento del Registro Oficial No. 88 de 25 de septiembre de 2013, el Secretario Nacional de la Administración Pública, dispuso a las entidades de la Administración Pública Central, Institucional y que dependen de la Función Ejecutiva el Uso obligatorio de las Noemas Técnicas Ecuatorianas NTE INEN-ISO/IEC 27000 para la Gestión de la Seguridad de la Información;

Que, el artículo 6 del citado Acuerdo No. 166, dispone: "*Es responsabilidad de la máxima autoridad de cada entidad mantener la documentación de la implementación del EGSI debidamente organizada y registrada de acuerdo al procedimiento específico que para estos efectos establezca la Secretaría Nacional de la Administración Pública*";

Que, a través de la Resolución No. 019 de 19 de marzo del 2014, la institución resuelve la implementación del EGSI y conforma la Comisión de Gestión de Seguridad de Información;

Que, mediante Resolución No. 011 de20 de febrero de 2015, publicado en la edición especial del Registro Oficial No. 325 de11 de junio del 201, se expide el Estatuto Orgánico de Gestión Organizacional de por procesos de la institución;

Que, mediante Acuerdo Ministerial No. 0001606 de 17 de mayo del 2016, la Secretaria Nacional de la Administración Pública, con el fin de simplificar los controles creados en las instituciones de la Función Ejecutiva y mejorar su gestión institucional dispones en su artículo 11 y siguientes la supresión del Comité de Seguridad de la Información;

En uso de las facultades que le confiere la ley:

RESUELVE

Artículo 1: La implementación del Esquema Gubernamental de Seguridad de la Información (EGSI) en la institución de conformidad con lo establecido en el Acuerdo Ministerial No. 166 de 119 de septiembre de 2013, publicado en el suplemento del Registro Oficial No. 88 de 25 de septiembre de 2013.

Artículo 2: Dejar sin efecto a la Comisión de Gestión de Seguridad de Información de la institución, por lo que, las funciones previstas en el Esquema Gubernamental de seguridad de la Información para el Comité de Gestión de Seguridad de la Información pasan a ser competencia de la Dirección de Planificación y Gestión Estratégica que, además, de las atribuciones establecidas en el mencionado Acuerdo Ministerial y en el Estatuto Orgánico de Gestión Organizacional por Procesos deberá:

1. Presentar conjuntamente con el Oficial de Seguridad de la Información un informe de gestión al Director Ejecutivo precisa las acciones para impulsar y mejorar el Esquema Gubernamental de Seguridad de la Información en la institución.
2. Implementar campañas internas con la finalidad de difundir el EGSI con ayuda de las áreas competentes de la institución.
3. Cumplir con las disposiciones que sobre la materia expida la Secretaría Nacional de la Administración Pública.

Artículo 3: El Oficial de Seguridad de la Información tiene las responsabilidades establecidas en el Esquema Gubernamental de Seguridad de la Información, e impulsa su implementación en la institución, coordina sus acciones con la Dirección de Planificación y Gestión Estratégica y, además, actúa como contraparte de la Secretaría

Nacional de la Administración Pública para la institucionalización de EGSI y en la gestión de incidentes de seguridad de la información.

DISPOSICIONES GENERALES. -

Primera: De la correcta aplicación de la presente Resolución encárguese a la Dirección de Planificación y Gestión Estratégica y al Oficial de Seguridad de la Información de la institución.

Segunda: Deróguese la Resolución No. 019 de 19 de marzo del 2014 y todas las disposiciones de igual o menor jerarquía, que se contrapongan con la presente resolución.

Tercera: La presente resolución entra en vigencia a partir de su suscripción, sin perjuicio de su publicación en el Registro Oficial.

COMUNIQUESE. –

Dado en Quito, Distrito Metropolitano, a 05 de julio del 2016.

ANEXO 2. Documentación operativa

Manual de Usuario para el proceso de cifrado de discos duros de computadores portátiles

- **Glosario de términos**

Cifrado: Procedimiento que utiliza un algoritmo de cifrado con una llave secreta para transformar un mensaje en texto ilegible, de tal manera que sea incompresible o de difícil acceso para personal no autorizado.

Descifrado: Proceso de convertir el texto cifrado en el texto en claro por medio de un algoritmo criptográfico.

Disco Duro: Dispositivo de hardware usado para almacenamiento datos informáticos, todas las computadoras tienen un disco duro interno.

BIOS: Sistema básico de entrada-salida del inglés *Basic Input/Output System,* es un software instalado en una memoria no volátil (ROM) de un ordenador, es fundamental para el arranque del computador, es el puente o interfaz de comunicación entre el hardware y el software.

Consola de administración de Kaspersky: Software de gestión centralizada que permite administrar de forma remota, la herramienta Kaspersky Endpoint Security.

Cuenta de administrador de dominio: Cuenta de usuario con roles administrativos dentro de un dominio de Directorio Activo.

Agente de Red de Kaspersky Security Center: Software de interacción entre el servidor de administración y los dispositivos conectados a este.

- **Responsabilidades**

Tabla 25. Responsabilidades proceso de cifrado

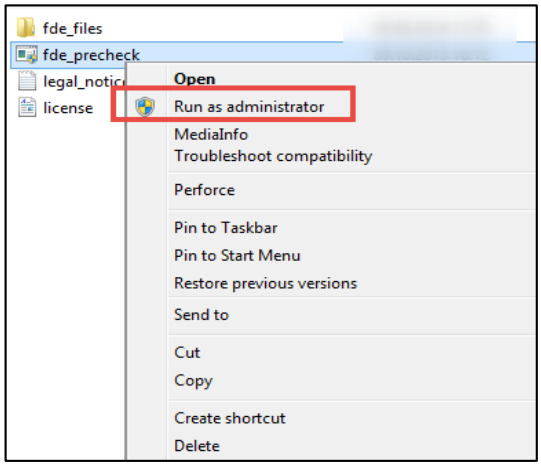
Cargo	Responsabilidad
Administrador de Consola Kaspersky	Crea directivas de cifrado y descifrado de disco completo en la consola de administración.
Técnico Soporte al Usuario	Prepara el equipo portátil para el cifrado de disco completo.

Fuente: Elaboración propia

- **Cifrado**
  - **Preparación del equipo**

Ejecutar con permisos administrativos el aplicativo *FDE PreCheck*, provista en la herramienta de cifrado *Kaspersky Endpoint Security Center.*

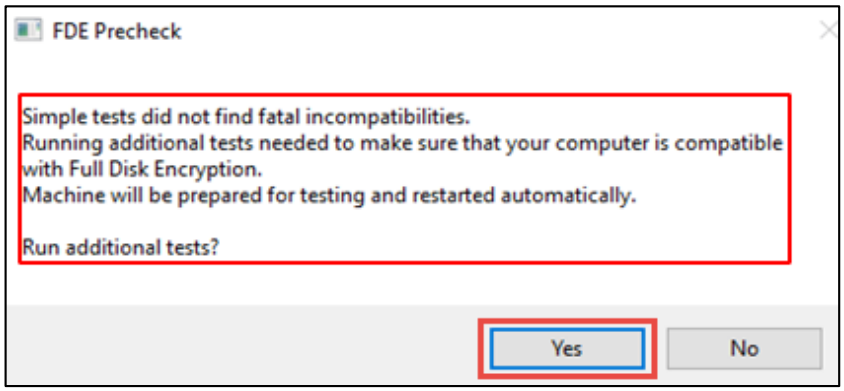
Figura 54. Aplicativo PreCheck



Fuente: Elaboración propia

Una vez ejecutado el aplicativo, el equipo, se reinicia automáticamente para realizar los test adicionales, seguir los pasos indicados en el test.

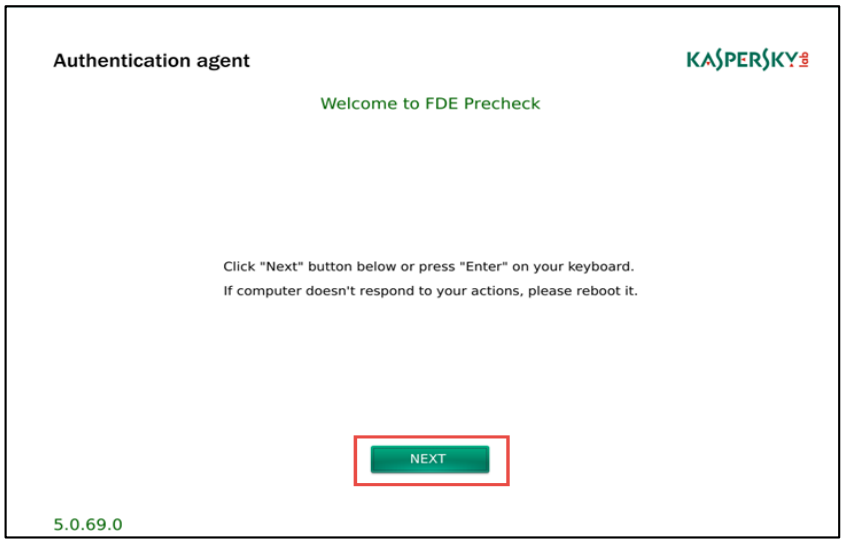
Figura 55. Pruebas adicionales



Fuente: Elaboración propia

Las pruebas que realiza la herramienta son comprobaciones interactivas para comprobar el correcto funcionamiento del teclado, dispositivos apuntadores y tokens.

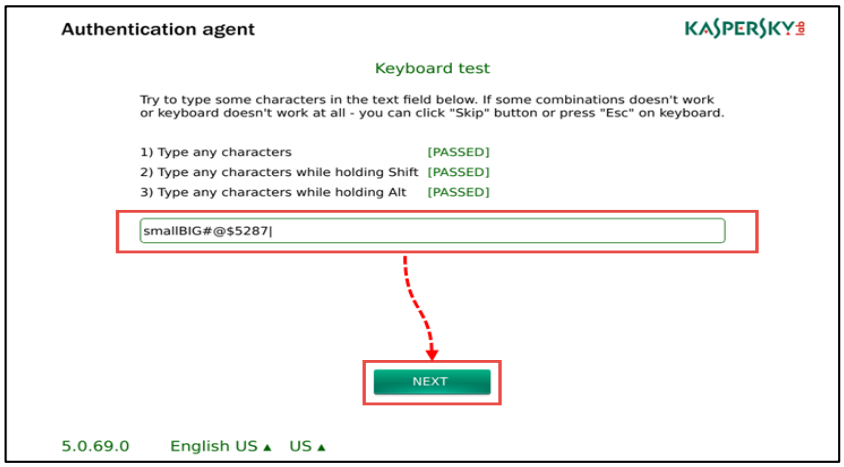
Figura 56. Inicio test



Fuente: Elaboración propia

La finalidad de esta prueba es comprobar, que se ingresen todos los caracteres del teclado incluidas las combinaciones de SHIFT y ALT.

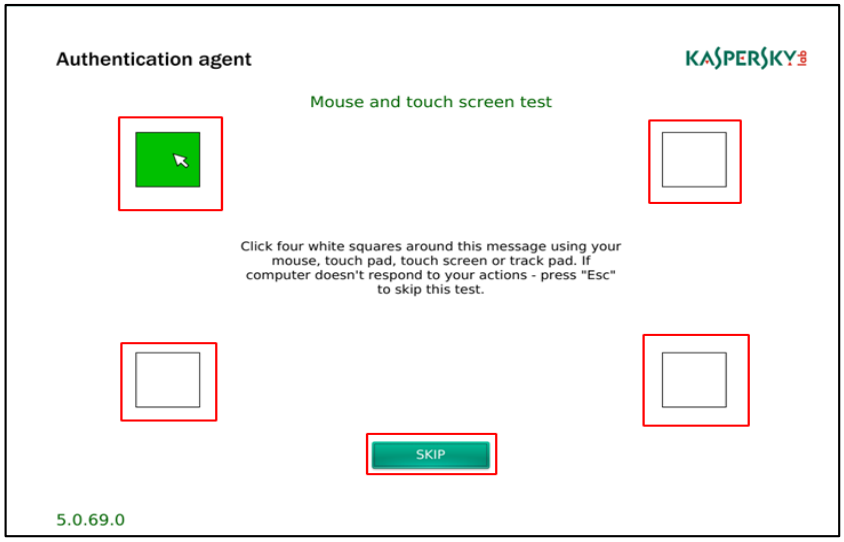
Figura 57. Test teclado



Fuente: Elaboración propia

La finalidad de esta prueba, es comprobar los dispositivos como mouse, pantalla táctil o panel táctil funcionan correctamente.

Figura 58. Test dispositivos apuntadores



Fuente: Elaboración propia

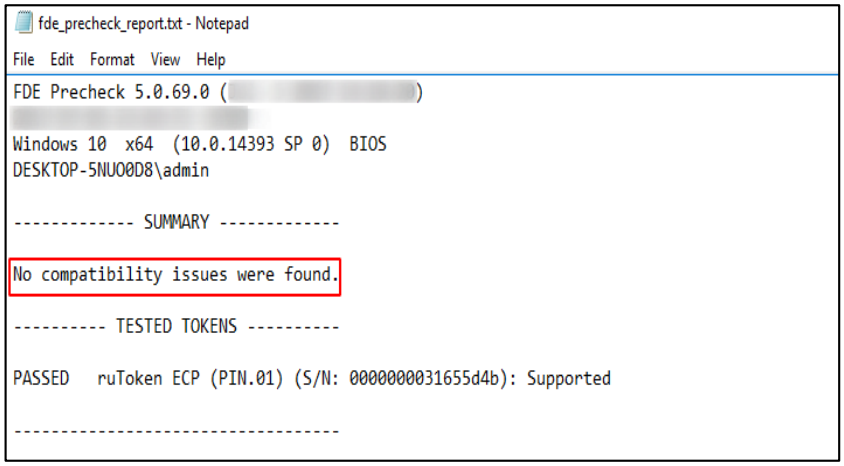
La finalidad de esta prueba, es probar la compatibilidad del sistema operativo, una vez que termine el proceso, el sistema operativo arrancará.

Figura 59. Test sistema operativo

Fuente: Elaboración propia

Finalmente, la herramienta genera el informe de que, no se presentaron errores en el test y, se continua con el proceso de cifrado.

Figura 60. Sin problemas de compatibilidad



Fuente: Elaboración propia

- **Configuraciones iniciales del equipo**

Se asigna un nombre del equipo, como recomendación, se configura el nombre del usuario creado en el Directorio Activo como nombre de equipo, por ejemplo:

- Nombre de usuario: José Pérez
- Usuario creado en el AD: JPEREZ
- Nombre de equipo: JPEREZ

Se une el equipo al dominio institucional, queda de la siguiente manera:

- JPEREZ.institucion.gob.ec.

Después, se cargan los usuarios que utilizarán el equipo, con los perfiles asignados a cada uno.

Tabla 26. Usuarios configurados en los equipos cifrados

Usuario	Perfil	Observaciones
Usuario de dominio	Estándar	JPEREZ
Usuario local	Administrador local	Control administrativo cuando el equipo está fuera de dominio
Usuario de dominio	Administrador de dominio	Control administrativo cuando el equipo está dentro de dominio
usuario de dominio	Administrador Kaspersky	Usuario administrador de Kaspersky, controla el cifrado de disco y acceso al computador en caso de fallas

Fuente: Elaboración propia

NOTA: Los usuarios listados en la tabla anterior cumplen un rol primordial en el proceso de cifrado y estos serán cargados obligatoriamente en el equipo a ser cifrado.

- **Instalación de la herramienta de cifrado**

Se procede con la instalación del software del cifrado, conformado por dos aplicativos:

a) Agente de red de Kaspersky security center
b) Kaspersky Endpoint security para Windows

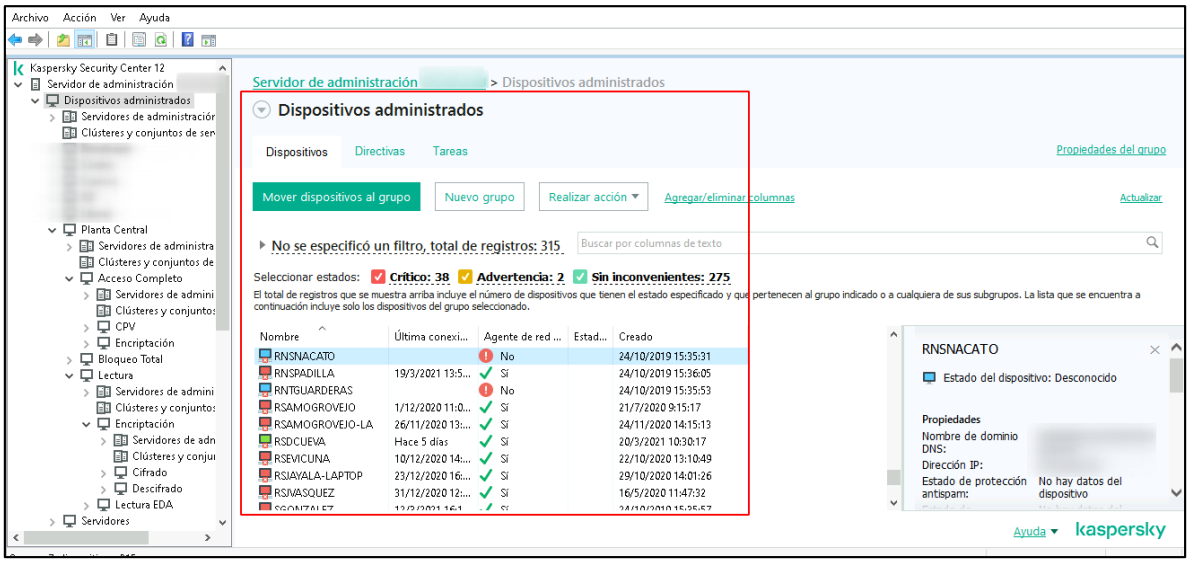
Por recomendaciones del fabricante la instalación, se realiza en secuencia, primero a y después b, para no tener problemas al momento de sincronizar el equipo con el servidor de administración.

Figura 61. Aplicativo de cifrado de disco completo instalado

Fuente: Elaboración propia

Una vez instalado el software de cifrado, el equipo o dispositivo, se sincroniza con el servidor de administración, después, es visible en la consola de administración de Kaspersky en la sección Dispositivos Administrados.

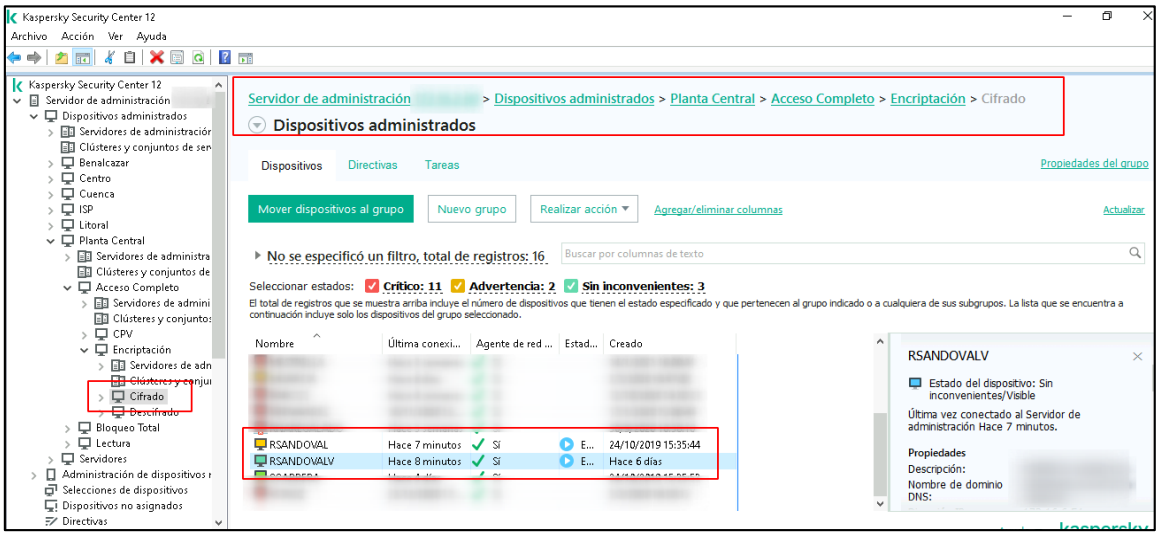
Figura 62. Dispositivos administrados



Fuente: Elaboración propia

Realizamos una búsqueda por nombre de equipo, y lo movemos al grupo CIFRADO para la aplicación de la directiva de cifrado.

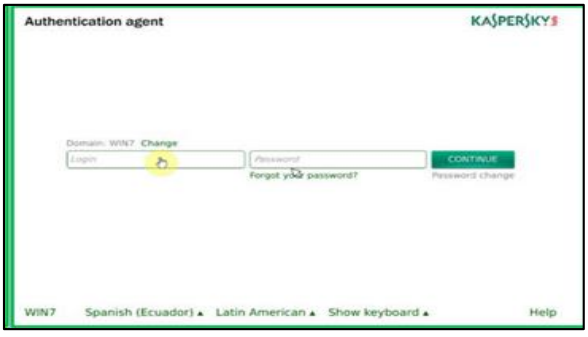
Figura 63. Dispositivos en el grupo cifrado



Fuente: Elaboración propia

Una vez transferido el equipo al grupo CIFRADO, la aplicación, solicita reiniciar el equipo por el cambio de componentes en la herramienta; una vez aplicada la directiva de cifrado, la aplicación solicita reiniciar el equipo por nuevamente, finalmente, al terminar el proceso de cifrado se realiza un tercer y último reinicio, donde, observamos la interfaz de ingreso al equipo de la herramienta de cifrado. Para el tercer reinicio es necesario consultar el estado de cifrado de disco al administrador de la consola.

Figura 64. Equipo cifrado. Agente de autenticación Kaspersky

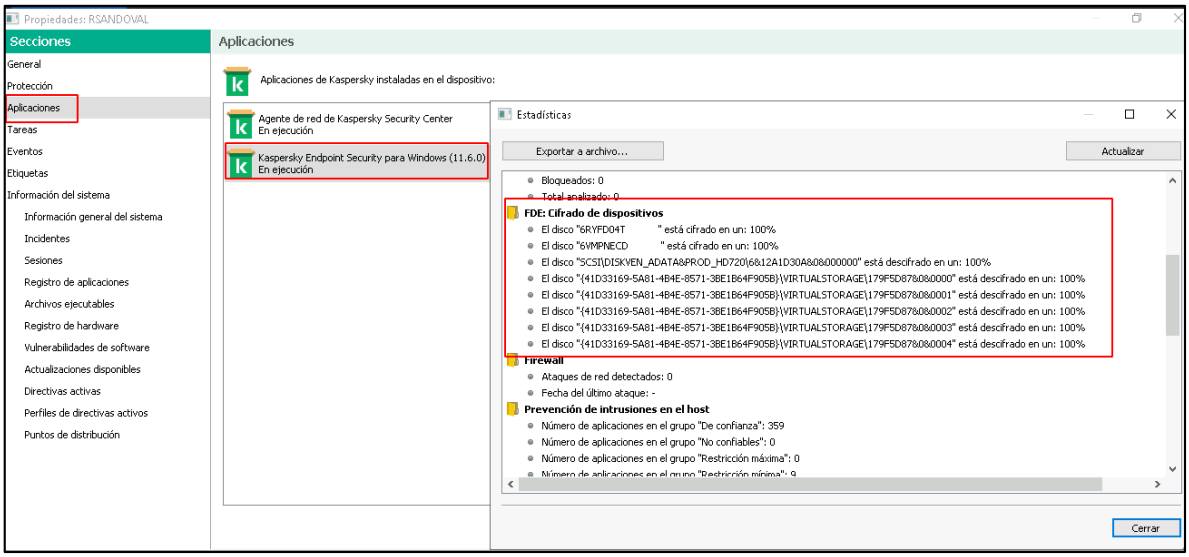


Fuente: Elaboración propia

NOTA: En el caso de no reiniciar el equipo, el proceso de cifrado queda suspendido hasta el próximo reinicio realizado por el usuario.

El proceso de cifrado lo verificamos en la consola de administración, en el nombre del equipo damos clic derecho, propiedades, en la nueva ventana vamos a aplicaciones, seleccionamos Kaspersky Endpoint Security para Windows, finalmente, damos clic en Estadísticas.

Figura 65. Proceso de cifrado de discos



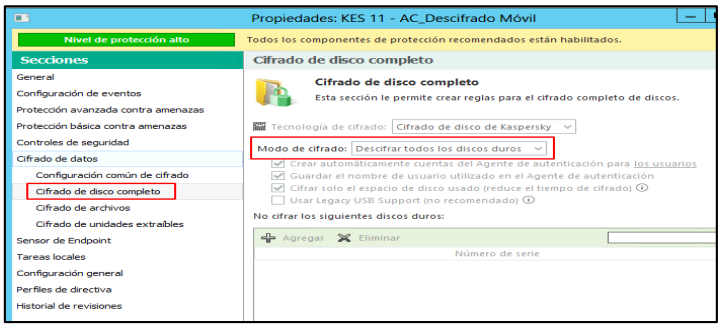
Fuente: Elaboración propia

NOTA: El tiempo de cifrado de discos duros depende de: tamaño del disco, tipo de disco: SSD (disco sólido) o HDD (disco mecánico), y cantidad de información que estos contengan; se recomienda realizar este proceso con discos duros formateados. El tiempo estimado del proceso de cifrado esta entre 30 minutos y 5 horas.

- **Descifrado**

Para el proceso de descifrado es necesario crear la directiva de descifrado y aplicarla al grupo con el mismo nombre. Una vez creada la directriz basta con mover el equipo al grupo indicado.

Figura 66. Directiva de grupo Descifrado



Fuente: Elaboración propia

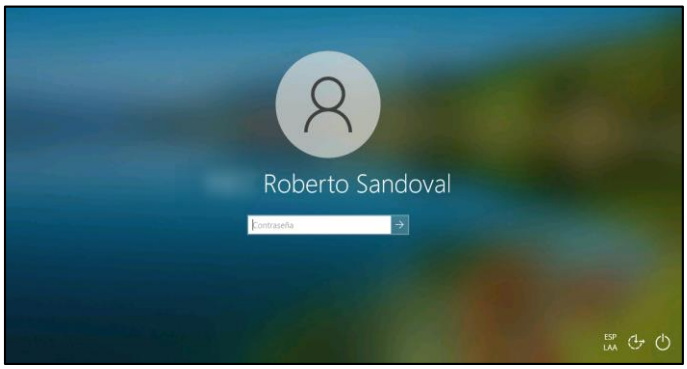
NOTA: Un equipo, no se descifra si el proceso de cifrado no ha culminado.

El tiempo de descifrado de un equipo depende de la cantidad de información contenida en su disco duro, debido a que los equipos en esta etapa cuentan con una considerable cantidad de información, este proceso toma entre 5 horas a 8 horas.

El proceso de descifrado es verificado por medio de la consola de administración.

Una vez culminado el proceso, el equipo no muestra el agente de autenticación de Kaspersky al inicio del sistema operativo, se muestra el acceso normal al equipo, la información contenida en el disco duro es respaldada en un disco externo, también, es posible extraer el dispositivo de almacenamiento y con la ayuda de un enclosure conectarlo a otro computador para realizar los respaldos respectivos.

Figura 67. Equipo descifrado



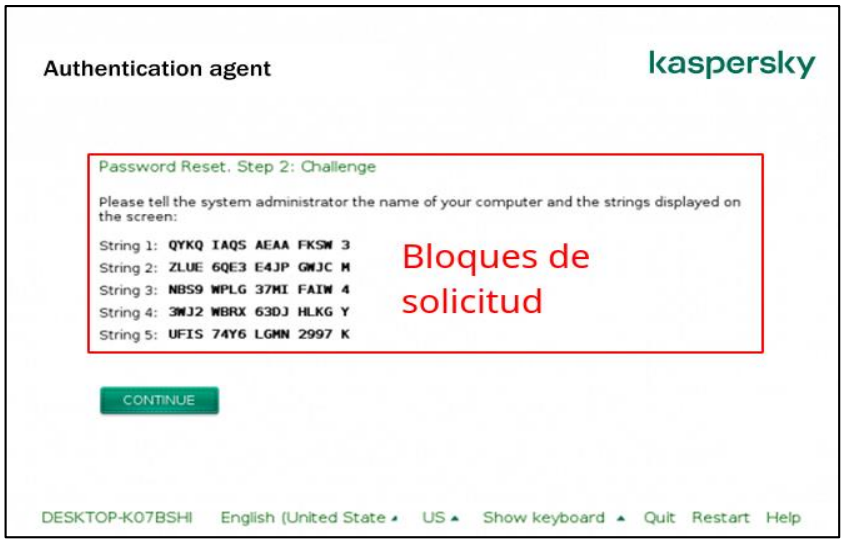
Fuente: Elaboración propia

- **Acceso a la información**
  - **Reseteo de contraseña**

En el caso de olvidar la contraseña para acceder al equipo cifrado, bloque de acceso al equipo por ingresos fallidos de contraseña, la herramienta de cifrado nos permite recuperar la contraseña con un procedimiento de solicitud y respuesta.

Una vez restringido el acceso al disco cifrado, seleccionamos “Olvide mi contraseña”, paso siguiente, el agente de autenticación nos muestra los bloques de solicitud, como, se muestra, a continuación.

Figura 68. Bloques de solicitud

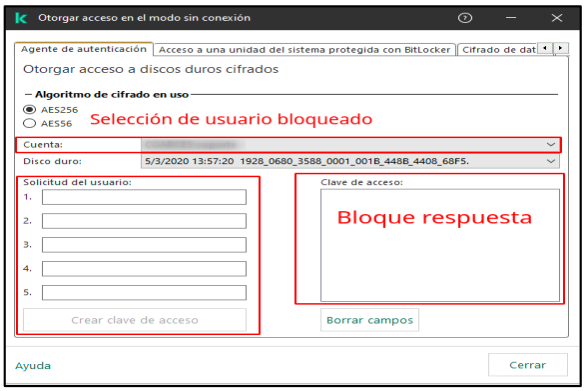


Fuente: Elaboración propia

El administrador de la consola ingresa los bloques de solicitud en Kaspersky security center para obtener los bloques de respuesta y comunicarlos al usuario.

En la consola de administración, se realiza una búsqueda por nombre de equipo, en propiedades del equipo seleccionamos “Otorgar acceso en el modo sin conexión”.

Figura 69. Bloques de respuesta



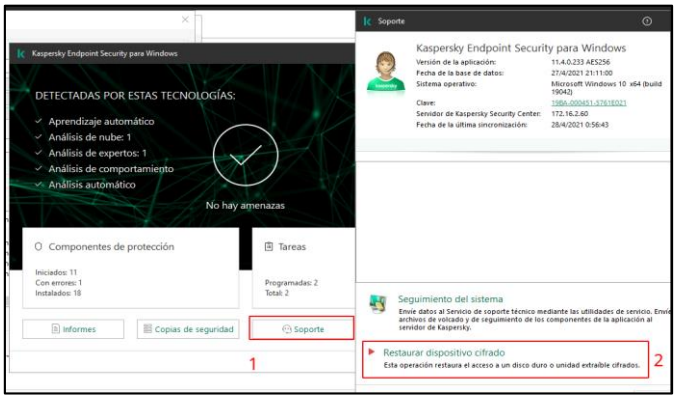
Fuente: Elaboración propia

El bloque respuesta, es ingresado por el usuario en el agente de autenticación, esto permite resetear la contraseña para el acceso al disco duro.

- **Acceso a un disco cifrado con problemas del sistema operativo**

Para un disco duro cifrado que tenga problemas en su sistema de archivos y no permita el acceso al sistema operativo, con la ayuda de un enclosure, se lo conecta a otro equipo cifrado, abrimos la interfaz de usuario de Kaspersky, para este proceso necesitamos de la ayuda del administrador de consola, es necesario ingresar usuario y contraseña en la opción de “Restaurar dispositivo cifrado”, como, se muestra, a continuación.

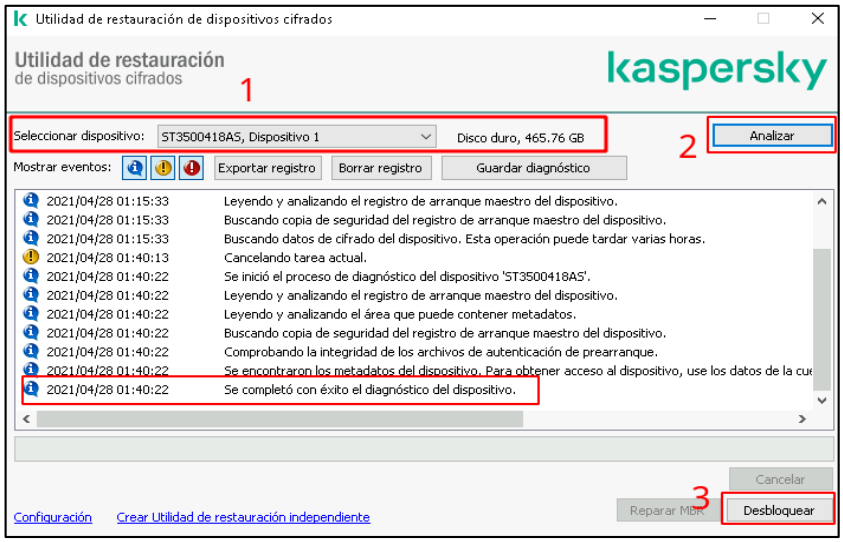
Figura 70. Interfaz de usuario



Fuente: Elaboración propia

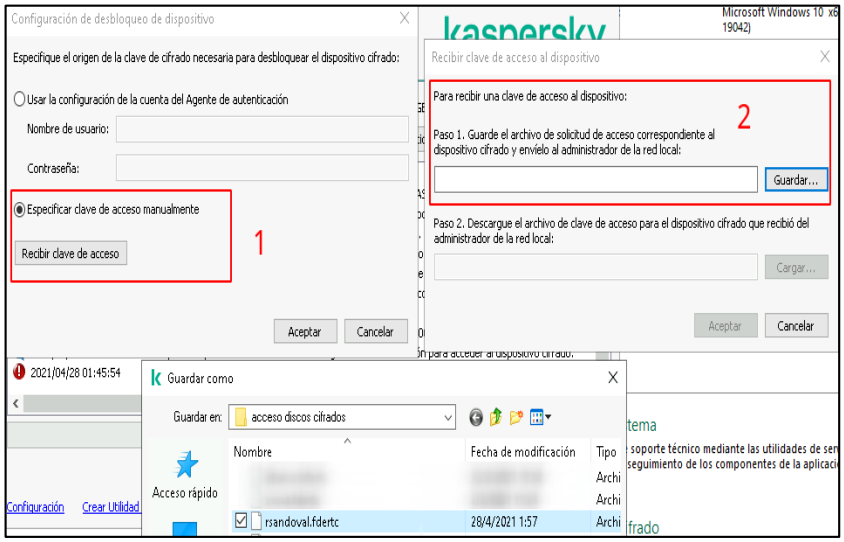
Luego de esto, se procede a analizar el disco duro al, que se requiere acceder, una vez finalizado el análisis, se genera la solicitud de acceso, esta, se guarda y envía al administrador de la consola para la generación de la solicitud de respuesta, y esta sea cargada por parte del usuario y, se conceda acceso al disco.

Figura 71. Análisis de disco cifrado



Fuente: Elaboración propia

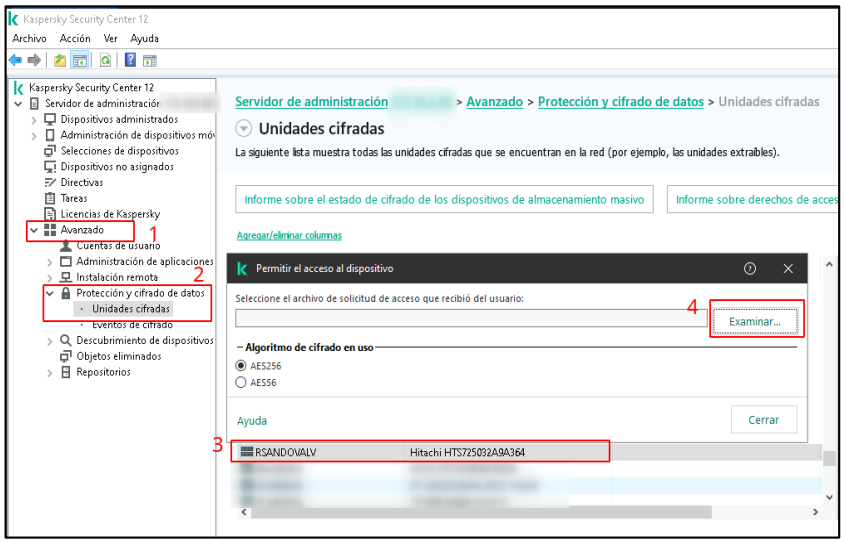
Figura 72. Generación de solicitud de acceso



Fuente: Elaboración propia

En la consola de administración, buscamos el dispositivo para conceder el acceso y generar la solicitud de respuesta.

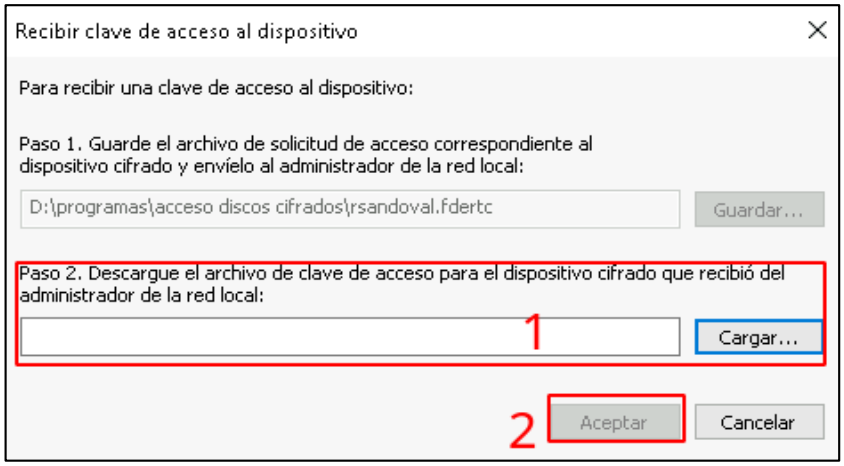
Figura 73. Solicitud de respuesta



Fuente: Elaboración propia

Finalmente, se carga el archivo de respuesta generado en la consola de administración para el acceso al dispositivo cifrado

Figura 74. Acceso a disco cifrado



Fuente: Elaboración propia

- **Configuraciones adicionales**

Cambios en la configuración de equipos cifrados

Para el cambio de custodio de un equipo cifrado, se realizan configuraciones adicionales como, cambio de nombre de equipo y agregar el nuevo usuario, dichos procesos, se detallan, a continuación.

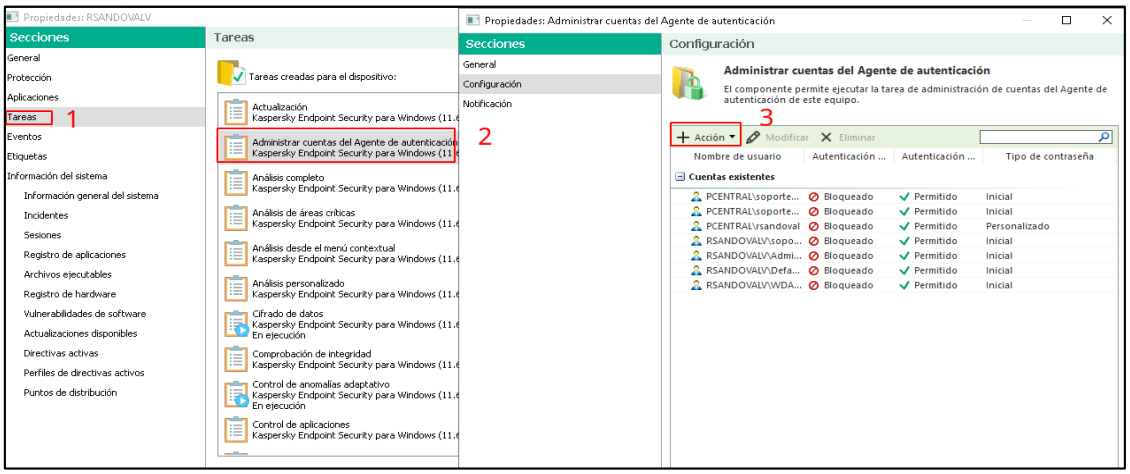
➢ **Cambio de nombre de equipo**

Este proceso, se lo realiza con la ayuda del usuario administrador local del equipo; en el agente de autenticación de Kaspersky en lugar del dominio, ingresamos el nombre del equipo, el nombre del usuario y la contraseña, una vez dentro del dispositivo, procedemos a bajar del dominio y al cambio de nombre para posteriormente subir el equipo al dominio nuevamente, realizada esta configuración, es necesario agregar los nuevos usuarios que utilizarán el computador en la consola de administración.

➢ **Agregar un nuevo usuario**

Para agregar un nuevo usuario, realizamos una búsqueda por nombre de equipo en la consola de administración, una vez localizado el dispositivo vamos a propiedades y realizamos la acción mostrada, a continuación.

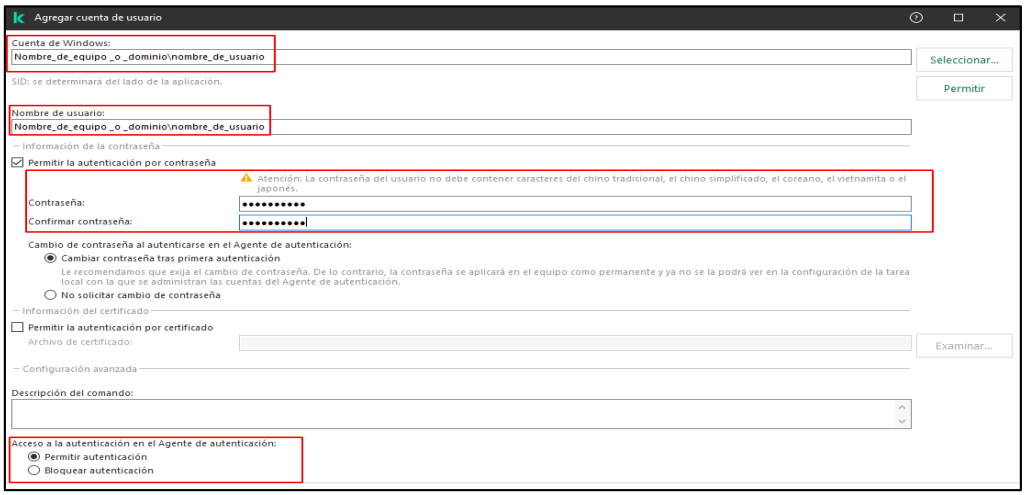
Figura 75. Agregar un nuevo usuario en un equipo cifrado



Fuente: Elaboración propia

En la opción “Acción” agregamos el nuevo usuario y el nuevo nombre del equipo o dominio.

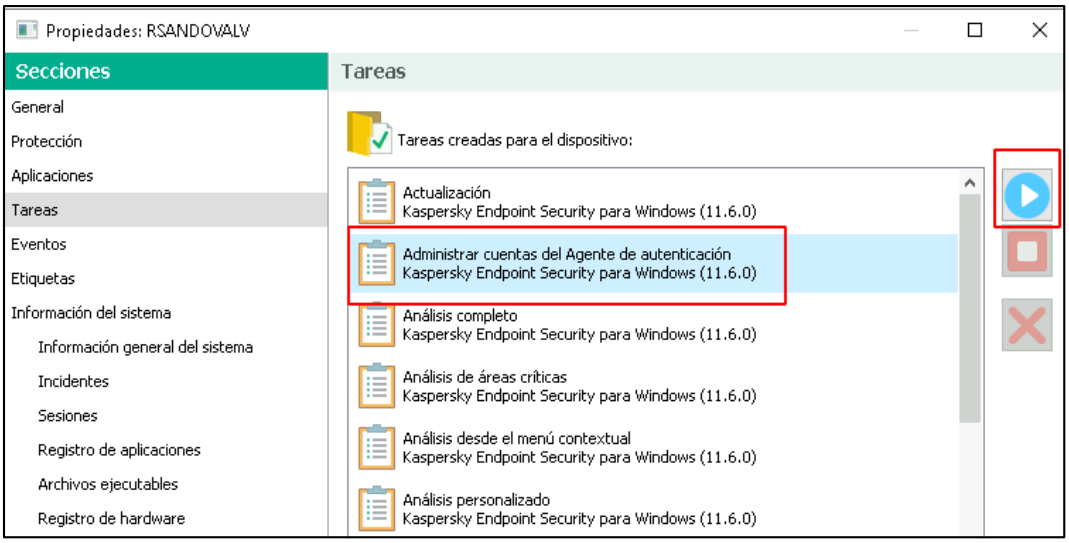
Figura 76. Configuración de un nuevo usuario



Fuente: Elaboración propia

Luego de configurada la tarea, se procede a iniciar la misma, una vez concluida, el nuevo usuario ingresa con sus credenciales.

Figura 77. Tarea de autenticación



Fuente: Elaboración propia

- **Solución de problemas**

Problemas de compatibilidad del aplicativo FDE PreCheck

- Descargar la versión más actual desde la página oficial de Kaspersky *security center*.
- Activar y desactivar el sistema de cifrado Bitlocker de Windows.
- Desactivar la opción de seguridad TMP en el BIOS del computador.

El aplicativo de Kaspersky con los componentes de cifrado, no se instalan

- Desinstalar versiones anteriores del aplicativo, instalar nuevamente.
- Descargar el aplicativo más actual desde la página oficial de Kaspersky security center.
- Desinstalar otros aplicativos antivirus instalados en el computador.

El dispositivo, no se sincroniza con la consola de administración

- Verificar que el agente de red se encuentre instalado.
- Verificar que el equipo se encuentre conectado a la red institucional.

El proceso de cifrado de disco completo no inicia

- Verificar que la licencia del aplicativo se encuentre activa, caso contrario adquiera una nueva licencia, el proceso de cifrado funciona solamente con una licencia activa.
- El sistema de cifrado no es compatible con el sistema operativo, actualice su sistema operativo.
- No se han realizado los reinicios del sistema necesario para que el proceso inicie, reinicie su equipo las veces necesarias.

No se permite el acceso los usuarios configurados en el equipo

- Los usuarios fueron creados después del proceso de cifrado, solicitar al administrador de consola que agregue los usuarios al equipo.

- Ingresar al equipo con el usuario administrador de Kaspersky (usuario maestro) para logear a los demás usuarios.
- El usuario se encuentra bloqueado por ingreso fallido de la contraseña, solicitar al administrador de consola el *reset* de contraseña.

ANEXO 3. Entrevista dirigida al personal del Departamento de DITIC de la Institución

Esta entrevista forma parte de un proyecto de investigación previa la obtención del título de Máster en Ciberseguridad de la Pontificia Universidad Católica del Ecuador Sede Ambato, los datos recolectaos con este instrumento son tratados de forma impersonal y tienen una intencionalidad académica.

1. ¿Usted conoce cuantos computadores portátiles tiene la institución en su inventario, de estos, que porcentaje sale de las instalaciones para teletrabajo?
2. ¿Qué características técnicas tienen los equipos portátiles, que se encuentran en teletrabajo, los sistemas de protección de datos instalados son fiables, usted considera que estos sistemas de protección protegen la confidencialidad de la información?
3. ¿De los equipos portátiles, que se encuentran actualmente en el inventario de la institución, ¿cuáles cree usted que son los más importantes a ser considerados para la implementación del sistema de cifrado de datos?
4. ¿El sistema de protección de datos instalado en los computadores portátiles de la institución brinda la opción de cifrado de datos, considera que la encriptación del disco duro mejora la seguridad de los equipos portátiles?
5. ¿Cuáles son las ventajas que brindaría el sistema de cifrado implementado en los computadores portátiles de la institución?