II CONVENCIÓN CIENTÍFICA INTERNACIONAL
"II CCI UCLV 2019"

XVIII SIMPOSIO INTERNACIONAL DE INGENIERÍA ELÉCTRICA. "SIE 2019"
TELECOMUNICACIONES Y ELECTRONICA

HERRAMIENTA PARA LA PREVENCIÓN DE FUGAS DE INFORMACIÓN EN LA RED CORPORATIVA DE ETECSA.

TOOL FOR THE PREVENTION OF INFORMATION LEAKS IN THE CORPORATE NETWORK OF ETECSA.

Ing. Dennis Meriño Menadier

Dr.C Félix Florentino Álvarez Paliza

1-Dennis Meriño Menadier.ETECSA,Cuba.dennis.merino@etecsa.cu

2-Felix Florentino Álvarez Paliza, UCLV, Cuba. fapaliza@uclv.edu.cu

Resumen

La información se ha convertido en uno de los activos más importantes de una organización, es utilizada como arma de desprestigio, herramienta de presión y valor que se comercializa y vende a escala global en todo tipo de ámbitos y sectores. Todo ello ha convertido la fuga de información entre las mayores amenazas existentes en la actualidad.

La Empresa de Telecomunicaciones de Cuba, ETECSA a fin mantener una alta reputación y entorno seguro, en que sus proveedores y clientes confíen en la habilidad que tiene de proteger los datos de su negocio. Cuenta con un nivel de gestión de seguridad, para minimizar los riesgos, protegerse contra violaciones de datos, y prevenir otros eventos que afectan sus finanzas, relaciones públicas, y su reputación.

Debido a la problemática existente en la empresa en relación al almacenamiento, transporte, acceso y procesado de la información en los diferentes medios y tecnologías de la información con que se dispone, en el presente trabajo se analizan, propone y evalúa, la implementación de una herramienta para la detección y prevención de fugas de información (DLP), haciendo uso de los métodos científicos, las buenas prácticas internacionales y la Norma ISO 27000, así como investigaciones relacionadas sobre las tecnologías líder en sistemas de prevención de fuga de información y gestión de incidentes de seguridad.

La implementación de la solución propuesta en la red corporativa de ETECSA, hace más efectivo y ágil la gestión de seguridad de la información, se garantizan los principios de confidencialidad, integridad y disponibilidad y el cumplimiento de lo normado en materia de seguridad de la información en Cuba.

Palabras Claves: Ciberseguridad; Seguridad de la Información; Detección de Fugas de Información, DLP

Abstract:

Information has become one of the most important assets of an organization, it is used as a weapon of discrediting, a tool of pressure and value that is marketed and sold on a global scale in all types of fields and sectors. All this has turned the leakage of information among the biggest threats that exist today.

The Telecommunications Company of Cuba, ETECSA in order to maintain a high reputation and secure environment, in which its suppliers and clients trust in the ability to protect the data of their business. It has a level of security management, to minimize risks, protect against data breaches, and prevent other events that affect your finances, public relations, and reputation. Due to the existent problematic in the company in relation to the storage, transport, access and processing of the information in the different means and technologies of the information that is available, in the present work, the implementation of an analysis is analyzed, proposed and evaluated. Tool for the detection and prevention of information leaks (DLP), making use of scientific methods, international best practices and the ISO 27000 standard, as well as related research on the leading technologies in information leakage prevention and management systems security incidents.

The implementation of the solution proposed in the corporate network of ETECSA, makes the management of information security more effective and agile, guarantees the principles of confidentiality, integrity and availability and compliance with the regulations on information security in Cuba.

Keywords: *Cybersecurity; Security of the information; Information Leak Detection; DLP*

1. Introducción

Las amenazas a la ciberseguridad crecen rápidamente. Los virus, gusanos, caballos de Troya, ataques de falsificación, robos de identidad, el correo basura y ciberataques están al alza. Es necesario entender lo que es la ciberseguridad para poder sentar los cimientos necesarios a fin de poder proteger las redes del futuro.

Se denomina Ciberseguridad al conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciberentorno. [1]

La ciberseguridad garantiza que se alcancen y mantengan las propiedades de seguridad (Disponibilidad, Integridad y Confidencialidad) de los activos de la organización y los usuarios contra los riesgos de seguridad correspondientes en el ciberentorno.

Se denomina fuga de información a la pérdida de la confidencialidad, de forma que información privilegiada sea accedida por personal no autorizado. La protección de la información se articula en torno a la protección de tres principios básicos: confidencialidad, integridad y disponibilidad[2].

El impacto y las consecuencias posteriores a un incidente de fuga de información, son muy negativos. Por un lado, la filtración de información puede dañar la imagen pública de la empresa y por tanto impactar negativamente en el negocio, generando desconfianza e inseguridad en clientes. Asimismo, la publicación de información puede generar consecuencias a terceros: grupos externos de usuarios y otras organizaciones cuyos datos se hayan hecho públicos. [3]

Para tratar de evitar la pérdida de información sensible, se debe identificar qué información es realmente vital para la empresa, antes de poder protegerla adecuadamente. Evidentemente, esta tarea no es sencilla y requiere un estudio pormenorizado en cada caso, pero siempre existe una base inicial sobre la que empezar a trabajar, como son el cumplimiento del marco regulatorio o la protección de propiedad intelectual y el diseño de soluciones técnicas para minimizar la ocurrencia de este tipo de incidentes. [4]

La prevención de pérdida de datos (DLP) es una estrategia para asegurarse de que los usuarios finales no envían información sensible o crítica fuera de la red corporativa. El término también se utiliza para describir productos de software que ayudan a un administrador de red a controlar qué datos pueden transferir los usuarios finales. [5]

La adopción de DLP, también llamada prevención de fuga de datos, prevención de pérdida de información o prevención de extrusiones, está siendo impulsada por amenazas internas y por leyes

estatales de privacidad cada vez más rigurosas, muchas de las cuales tienen estrictos componentes de protección de datos o de acceso. Los productos de software de DLP utilizan reglas de negocio para examinar el contenido de los archivos y etiquetar la información confidencial y crítica, para que los usuarios no puedan divulgarla.

Una vez que las herramientas de software DLP han sido implementadas, un usuario final que intente, de manera accidental o malintencionada, revelar información confidencial que ha sido etiquetada, será repudiado. Además de ser capaces de monitorear y controlar las actividades de punto final, las herramientas de DLP también pueden ser utilizadas para filtrar flujos de datos en la red corporativa y proteger los datos en reposo.

En general un proyecto de DLP busca la correcta implementación de una plataforma que logre prevenir la fuga de información sensible utilizando herramientas de software perimetral y de cliente final, que permitan atender los requerimientos de seguridad de la organización y los lineamientos de su administración.

Con el fin de subsanar este tipo de vulnerabilidades, es indispensable la implementación de políticas claras en la plataforma de DLP sobre el uso de los dispositivos USB, correo electrónico, archivos y carpetas. Estas políticas definen entre otros esquemas de encriptación, monitoreo y registro. Siempre velando por el cumplimiento de la política de seguridad de la información sectorial, esta consiste en los controles para la protección y manejo de información de los funcionarios pertenecientes a la empresa[6, 7].

Actualmente en ETECSA, la gestión de la información oficial y en particular la información oficial clasificada, se realiza a través de las Oficinas de Control de la Información Clasificadas (OCIC), éstas se encargan de la recepción, tramitación, conservación, destrucción, y control de la información oficial. Para identificar la clasificación de cualquier documento, es requerido consultar las listas internas para la clasificación y desclasificación de la información, establecidas mediante las Resoluciones 163 y 164 del Ministro de las Comunicaciones. [8]

Este proceso suele ser engorroso debido a que es representativo el número de informaciones de la empresa, que teniendo en cuenta las listas internas ameritan de clasificación, por consiguiente el número de medidas a cumplir a partir del marco legal establecido en el país, para el tratamiento de los documentos clasificados, que en su mayoría data de los años 1999, 2000 y 2001, esto en muchos casos provoca atrasos en los flujos informativos, y en otros violaciones de lo establecido al generar los documentos en las PC sin los requisitos establecidos y su tramitación por vías no seguras como el correo electrónico , lo que constituye la situación problemática de este trabajo. Todo lo anterior representa un reto para ETECSA, ante el creciente auge de los ataques cibernéticos y de los casos recientes de fuga de información en las grandes empresas del mundo.

Teniendo en cuenta lo anterior y el desarrollo acelerado de las tecnologías de la información y las comunicaciones, así como de la necesidad de alcanzar niveles superiores de seguridad de la información oficial de la empresa, se plantea el siguiente problema científico. ¿Cómo lograr una gestión más eficiente en la prevención de fugas de información en la Empresa de Telecomunicaciones de Cuba? , para ello es requerido realizar un análisis de cómo se desarrolla la gestión de la seguridad de la información en las operadoras de telecomunicaciones en el mundo. Los resultados de esta investigación tendrán un impacto directo en los procesos de seguridad de la información de la Empresa de Telecomunicaciones de Cuba, lo que constituyen el objeto de estudio y campo de acción de este trabajo.

El presente trabajo propone como objetivo general el empleo de la herramienta SearchInform DLP para la prevención de fugas de información en las redes corporativas de la Empresa de Telecomunicaciones de Cuba.

Se considera que una vez implementada la herramienta propuesta en la empresa, los procesos de gestión de seguridad de la información se realicen de forma más eficiente, y tengan un carácter más preventivo, lo que redundará en mayores beneficios a la entidad, constituyendo ésta la hipótesis del presente trabajo.

Para contribuir a alcanzar el objetivo general propuesto en la presente investigación, se proponen los siguientes objetivos específicos y tareas, cada uno de ellos representa un hito fundamental en el desarrollo de este trabajo.

1. Comparar las herramientas y soluciones de DLP existentes en el mundo.
2. Determinar el marco legal vigente en Cuba para la seguridad de la información oficial.
3. Proponer una arquitectura de implementación en ETECSA para la Herramienta SearchInform DLP.
4. Evaluar los resultados de la aplicación de la herramienta seleccionada.

Tareas de la Investigación:

1. Revisión de la bibliografía existente relacionada al objeto de estudio y campo de acción.
2. Búsqueda de las recomendaciones de los organismos internacionales existentes y buenas practicas sobre el empleo de los sistemas DLP y procesos de gestión de seguridad de la información.
3. Análisis de las normas legales establecidas en Cuba y la empresa sobre Seguridad y Protección de la Información Oficial.
4. Diseño de la arquitectura de implementación de la herramienta DLP seleccionada, a partir de las mejores recomendaciones analizadas.
5. Validación técnica y económica de la solución propuesta.
6. Análisis de los aportes y beneficios de la solución propuesta.

Para poner en marcha un plan de prevención de fuga de información, según [9] es necesario cubrir estos puntos:

- Identificar los activos críticos de información, donde se tiene (físico y cloud) y en qué procesos pueden verse comprometidos.
- Determinar qué personas pueden acceder a ellos y qué uso de los mismos pueden hacer.
- Fijar controles de seguridad para evitar, detectar y responder a posibles vulnerabilidades y ataques.
- Monitorizar continuamente los flujos diseñados y los sistemas implantados para asegurar un nivel de protección óptimo continuo.

La implementación de soluciones DLP debe ser precedida de un estudio centrado en las necesidades del negocio. El resultado de éste deberá mostrar los puntos de vulnerabilidad, posibilitando el establecimiento de un conjunto de soluciones para atender las necesidades evidenciadas. Tener total dominio sobre el ambiente, así como entender los diferentes tipos de DLP y sus aplicaciones, son los primeros pasos en busca de la implementación de solución para evitar la pérdida de datos en ambiente corporativo.

Existen diferentes tipos de soluciones DLP, cada una orientada a un propósito específico, pero con el mismo objetivo: prevenir la pérdida de datos.

DLP de Red**:** Explora todo el contenido que pasa por los puertos y protocolos de la empresa. Proporciona informes importantes que ayudan a garantizar la seguridad de la información en la organización. La información recopilada por el Network DLP se guarda en una base de datos que se puede administrar fácilmente.

DLP de Almacenamiento: Permite ver archivos confidenciales almacenados y compartidos por quienes tienen acceso a la red corporativa. Es una buena solución para controlar datos almacenados en la nube.

DLP usuario final (Endpoint)**:** Estas se instalan en todas las estaciones de trabajo y dispositivos utilizados por los empleados de la empresa para supervisar e impedir la salida de datos sensibles por dispositivos extraíbles, aplicaciones para compartir o áreas de transferencia.

Una vez analizados los aspectos generales descritos anteriormente de las soluciones DLP, corresponde evaluar las herramientas disponibles en el mercado para seleccionar la propuesta a implementar en la Empresa.

McAfee DLP: Utiliza una metodología de control granular, permite controlar la transmisión de datos confidenciales a través de una extensa variedad de canales de pérdida de éstos: aplicaciones como

correo electrónico, webmail, screenscrape, P2P, IM y Skype; redes como HTTP, FTP y Wi-Fi-; y dispositivos físicos como USB, impresoras, fax y almacenamiento portátil.

También posibilita el resguardo de los datos en todos sus formatos, ofreciendo protección con conciencia de contenido y contexto para bloquear la transferencia de información confidencial, incluso si ésta es manipulada, copiada, pegada, comprimida o encriptada desde la fuente original. Esto es posible a través de algoritmos de huella digital y un poderoso motor de expresiones regulares y métodos de clasificación, basados en ubicación y contexto de la marca.

SYMANTEC DLP: Symantec DLP según [10] está configurado para identificar datos confidenciales, incluidos los establecidos en las políticas de protección de datos personales de la unión europea, y utiliza una amplia variedad de técnicas avanzadas de detección de datos para identificarlos en formatos muy diversos.

Symantec DLP puede detectar, supervisar y proteger los datos confidenciales en cualquier ubicación: el lugar de trabajo, durante los desplazamientos físicos o en la nube. Proporciona una visibilidad y un control completos de todos los canales en los que puede producirse la pérdida de datos: aplicaciones en la nube, endpoints, repositorios de datos, correos electrónicos y comunicaciones por Internet.

SEARCHINFORM DLP: El sistema DLP de SearchInform [11] es una herramienta que protege a su negocio en pocos pasos**:**

- Controlará los flujos de información
- Investigará el contenido de toda comunicación escrita y mensajes enviados
- Avisará sobre las violaciones de las políticas de seguridad
- Ayudará a hacer la investigación y prevenir la perdida de información
- Controlará los envíos de correo electrónico
- Controlará los envíos de Mensajes de voz y de texto, y además los archivos transmitidos vía Skype, Viber, ICQ, etc.
- La información enviada o recibida de los servicios de almacenamiento en la nube
- Las publicaciones realizadas en distintos foros y los comentarios en blogs
- Impresiones en papel
- Los archivos que se guardan en dispositivos externos (pendrives, discos duros, CD y DVD)

El sistema funciona en dos niveles: Por un lado controla los datos y el tráfico que va a Internet y por otro, vigila lo que está ocurriendo en la PC de los empleados. Con esta funcionalidad de SearchInform DLP la compañía estará protegida las 24 horas supervisando tanto lo que sucede dentro de la oficina como fuera de ella en viajes de negocios o el trabajo remoto.

A modo de resumen a continuación se muestra la comparación realizada para la selección de la herramienta a implementar en ETECSA, teniendo en cuenta entre los elementos evaluados, la posibilidad de adquirir las licencias y el entrenamiento posterior que se requiere.

HERRAMIENTA	PAÍS-PROVEEDOR	CUMPLE CON LOS REQUERIMIENTOS DE ETECSA	OBSERVACIONES
McAfee DLP Endpoint	EE.UU	Si	No es posible adquirir la licencia directamente por las leyes norteamericanas. Encarece la solución
Symantec Data Loss Prevention	EE.UU	Si	No es posible adquirir la licencia directamente por las leyes norteamericanas. Encarece la solución
SearchInform DLP	RUSIA	Si	Es posible adquirir la licencia y el soporte técnico requerido. Implementado en más de 2000 empresas en todo el mundo y las principales empresas y el gobierno ruso.

Tabla 1. Comparación de las Soluciones Estudiadas.

Teniendo en cuenta los elementos descritos anteriormente sobre las características técnicas de cada solución, las ventajas y desventajas que ofrecen, la posibilidad real de adquirirlos en el mercado, su valor y precio, se determina que la solución a emplear es SEARCHINFORM DLP.

El compendio de normas cubanas para la seguridad y protección de la información data de fines de los años 90 e inicio del 2000, constituye una especialidad reconocida y rectorada por el Ministerio del Interior, teniendo en cuenta que los incidentes asociados a pérdidas, robos, divulgación no autorizada de información, puede entrañar riesgos al país en dependencia del tipo, clasificación y valor de la información, por ende tiene un impacto directo en la seguridad nacional del estado cubano.

El Decreto Ley 199 de Fecha 25 de Noviembre de 1999, del Presidente de los Consejos de Estado y de Ministros de la República de Cuba, [12] reconoce que los servicios especiales enemigos dedican cuantiosos recursos, medios y fuerza cada vez más sofisticados a la obtención de información, por consiguiente se hace necesario fortalecer las medidas establecidas para salvaguardar la información y evitar que esta pudiera ser útil a los planes subversivos de los enemigos de la revolución, entre otras afectaciones a la esfera económica, política y social del país.

El estándar X.1205 de la IUT, recoge una serie de aspectos y recomendaciones generales a tener en cuenta para la adopción de medidas de seguridad del ciberespacio. De igual forma la Norma ISO 27000 y su familia propone una guía metodológica para la implementación de un sistema de gestión

de seguridad de la información, siendo un referente internacional en la materia, por ende constituye una referencia requerida para el desarrollo del presente trabajo de investigación.

2. Metodología

Los métodos de investigación científica empleados fueron los siguientes:

- Métodos Teóricos empelados para la definición de la hipótesis. Específicamente los métodos lógicos hipotético deductivo. Se tiene en cuenta además los procedimientos de análisis, síntesis y abstracción propuestos por este método.
- Métodos Empíricos empleados para la búsqueda de la información primaria a partir de los conocimientos que se tiene del tema, ayuda a comprobar la hipótesis.
- Métodos de observación científica.

3. Resultados y discusión

Para abordar los principales aportes que esta investigación pudiera introducir en ETECSA, se tomarán en cuenta las consecuencias que se derivan de un incidente de fuga de información según [13] :

- Evita daños de imagen, lo que genera un impacto negativo para la entidad y lleva implícita pérdida de confianza de los usuarios.
- Disminuyen o minimizan las afectaciones económicas estrechamente las relacionadas con las pérdidas de contratos o de negocios, o por la filtración de ideas o planes comerciales.
- Se mitigan aquellas afectaciones que suponen un impacto negativo en ámbitos muy diversos, como por ejemplo, el ámbito político, diplomático, institucional, o gubernamental, entre otros.
- Se logra cumplir con las normativas establecidas por el país en esta materia.

De igual forma con la implementación de la solución propuesta, se minimizan los riesgos asociados a la fuga de información en la empresa, se hace más ágil los procesos de gestión de la información oficial, se garantiza los principios básicos de confidencialidad, integridad y disponibilidad de la información. También favorece el cumplimiento de lo normado en materia de seguridad y protección de la información. La arquitectura de despliegue de esta solución, teniendo en consideración los requerimientos de la empresa es la siguiente:

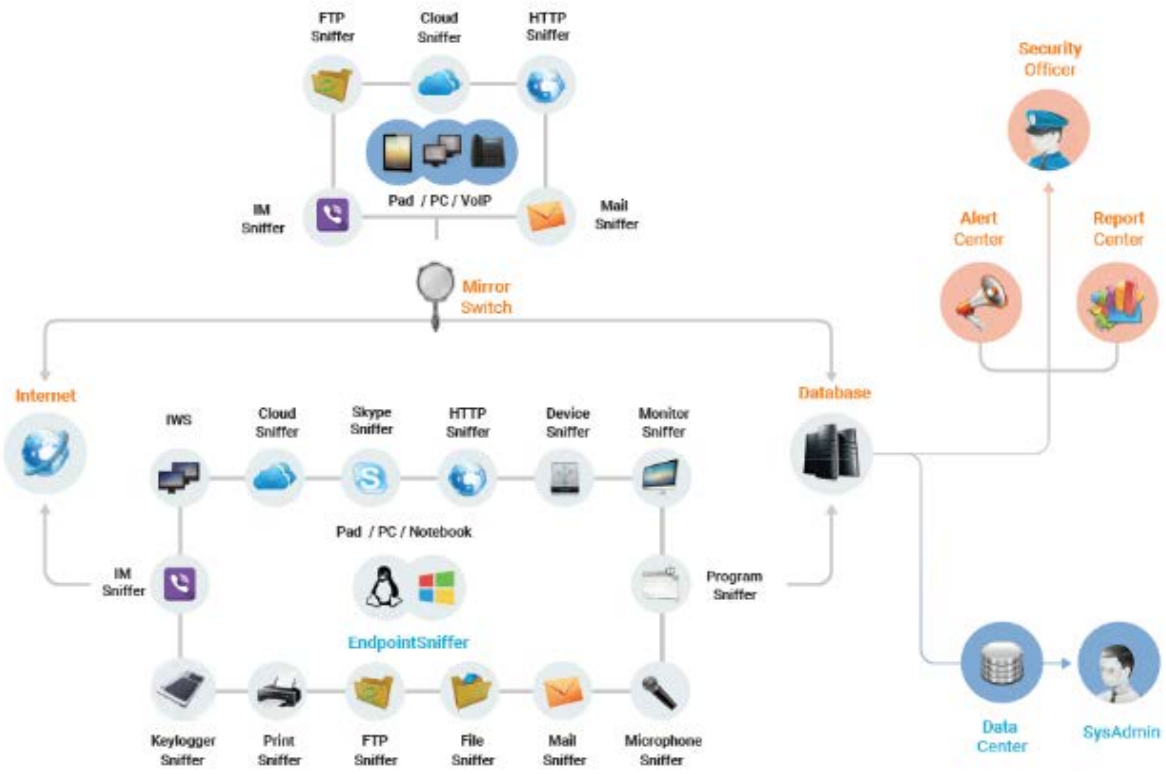

Fig. Arquitectura General de Despliegue de la solución propuesta por el proveedor.

Esta arquitectura permitirá ejercer un control de los principales elementos, escenarios y estados en que se encuentra la información, de esta forma se prevé la mitigación del riesgo de fuga de información unido a la implantación de la política de seguridad y la adopción de otras medidas organizativas y técnicas en la empresa. A continuación se muestra la relación de módulos de la herramienta SearchInform DLP, implementados en ETECSA.

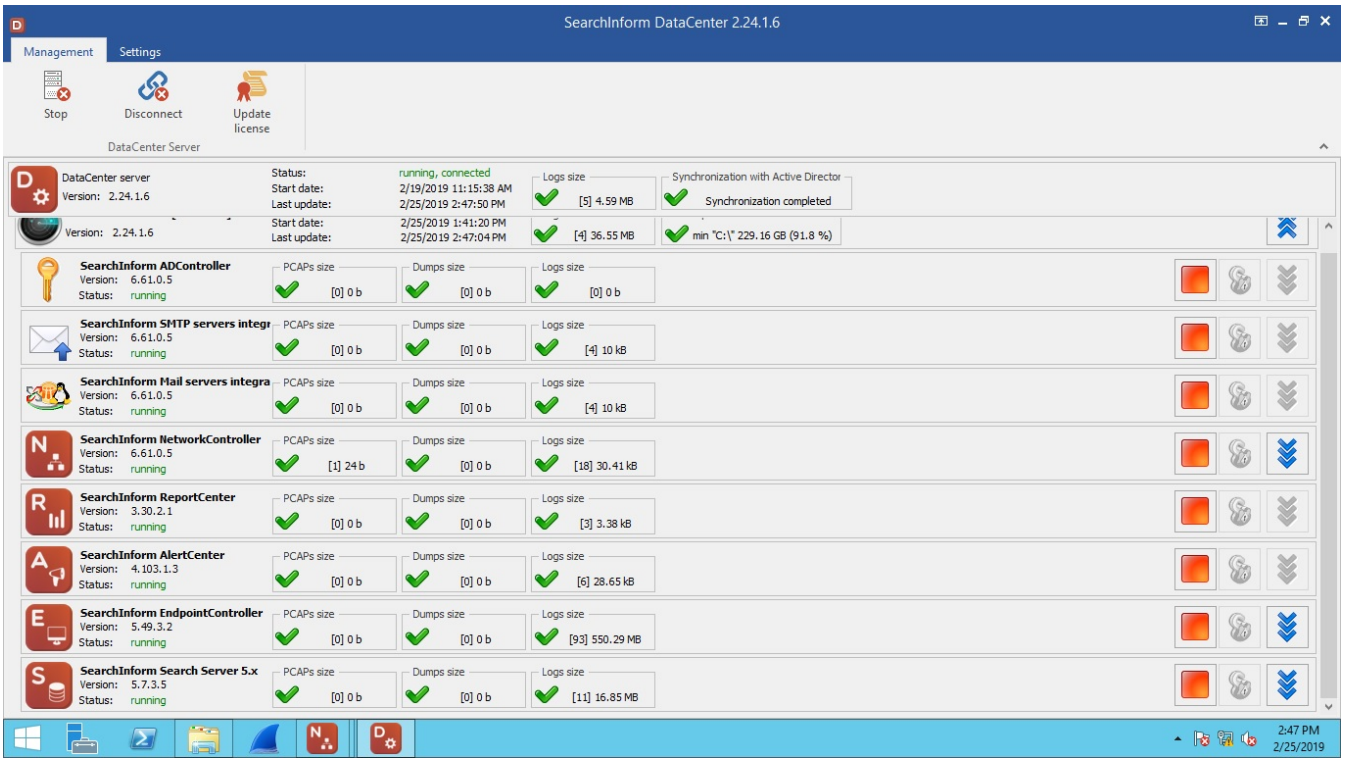

Fig. Módulos instalados de la solución.

La implementación de estos módulos, ha permitido se inicie ETECSA, un proceso de evaluación de las posibles manifestaciones de fuga de información, de forma más eficiente, ya que esta herramienta propicia informes del comportamiento y tendencias del uso de la red corporativa.

De igual forma con la instalación de los agentes en las computadoras seleccionadas, se logra una mayor personalización en la aplicación de las políticas de seguridad de la información establecida, toda vez que puede configurarse en correspondencia al perfil, jerarquía y exposición al riesgo con que cuenta el usuario seleccionado. Esta herramienta además se vincula con facilidad con otras soluciones de seguridad ya implementadas en la empresa.

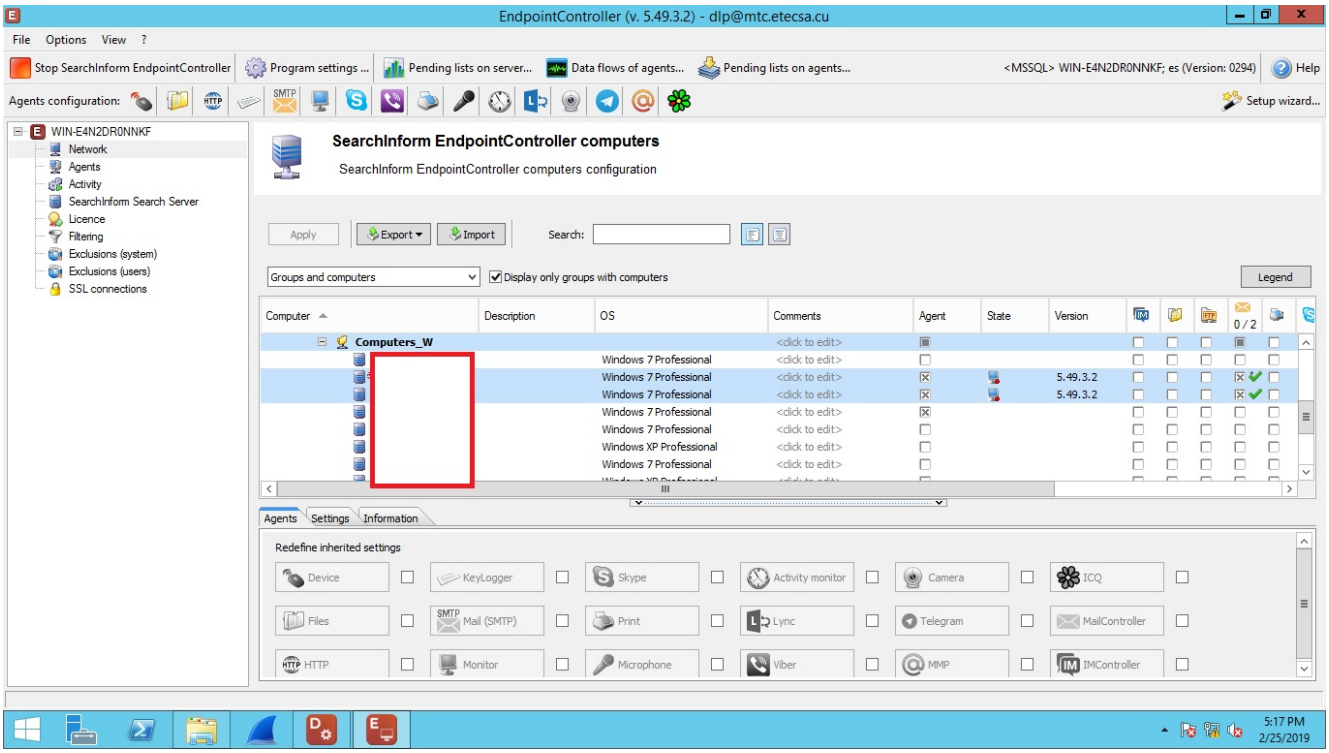

Fig. Relación de usuarios con agentes instalados

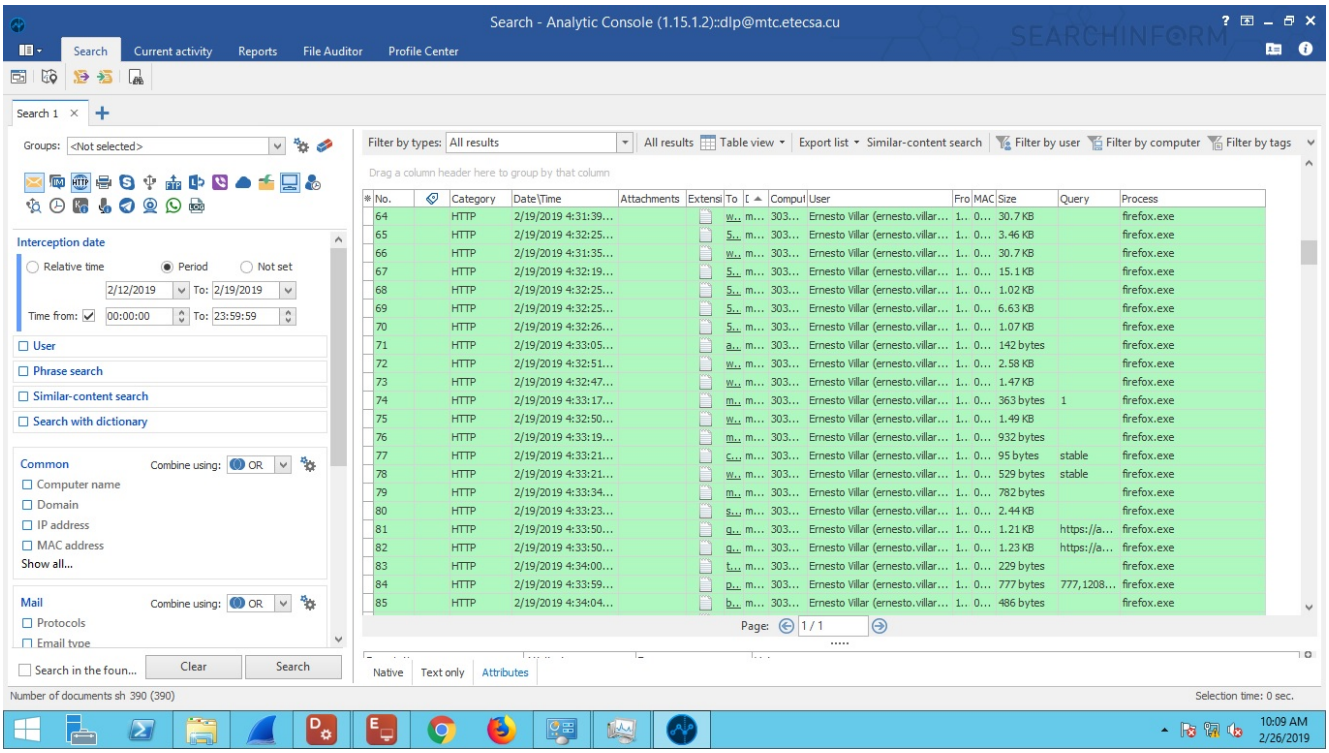

Fig. Reporte de muestra modulo consola analítica.

4. Conclusiones

- Se realizan las pruebas funcionales requeridas, posterior al proceso de instalación y configuración de los aplicativos, obteniendo los resultados previstos y para lo cual se adquiere la solución de DLP.
- En cada unidad organizativa en la cual se aplicó el proyecto de prevención de fuga de información se verificó en cada estación de trabajo la correcta instalación del agente de cliente final.
- Se configuraron las políticas de seguridad a cada dirección, teniendo en cuenta los controles que se querían ejecutar por parte del grupo a cargo de la seguridad de la información.
- Se van afianzando las políticas definidas de acuerdo a los requerimientos expresos de la alta dirección y las normas legales vigentes en el país.
- Se logra un resultado favorable que contribuye a garantizar la confidencialidad, integridad y disponibilidad de la información.

5. Referencias bibliográficas

[1] *X.1205 Seguridad en el ciberespacio – Ciberseguridad*, 2008.
[2] Inteco, "GUÍA GESTIÓN DE FUGA DE INFORMACIÓN," (in ES), *Instituto de Ciberseguridad de España,* 2012.
[3] Incibe, "Como Gestionar una fuga de informacion," *incibe.es,* p. 20, 2016.
[4] I. I. N. d. C. d. España, "Como gestionar una fuga de informacion " 2017.
[5] M. Rouse, 2016.
[6] D. A. A. AVENDAÑO, "DISEÑO E IMPLEMENTACIÓN DEL PROYECTO (DATA LOSS PREVENTION)," Titulo para Ingeniero en Telecomunicaciones FACULTAD DE INGENIERÍA Y CIENCIAS BASICAS, INSTITUCION UNIVERSITARIA POLITÉCNICO GRANCOLOMBIANO, 2016.
[7] *Politicas de Seguridad y Proteccion de la informacion,* ETECSA, 2018.
[8] *Lista de Informacion Oficial Limitada*, 2012.
[9] ORBIT, "Soluciones DLP de prevención de pérdidas de datos y cifrado para GDPR," *orbit.es,* 6 de marzo de 2018 2018.
[10] S. Corporation, "Symantec Data Loss Prevention," *www.symantec.com,* 2018.
[11] S. LTD, "SearchInform DLP," (in ES), 2018.
[12] *Decreto Ley 199.Sobre la seguridad y protección de la infromacion oficial* 1999.
[13] I.-I. N. d. Ciberseguridad, "Cómo gestionar una fuga de información," 20-6-2016 2016.