ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Facultad de Ingeniería en Electricidad y Computación

Maestría en Seguridad Informática Aplicada

"IMPLEMENTACIÓN DE UNA PLATAFORMA TECNOLÓGICA PARA PREVENIR LA FUGA DE DATOS EN LA RED ADMINISTRATIVA DEL SERVICIO INTEGRADO DE SEGURIDAD ZONAL"

EXAMEN DE GRADO (COMPLEXIVO)

Previo a la obtención del título de:

MAGISTER EN SEGURIDAD INFORMÁTICA APLICADA

JOHANNA ROSALYN BACILIO ZAMBRANO

GUAYAQUIL – ECUADOR

AÑO: 2015

AGRADECIMIENTO

A Dios por brindarme la fuerza, fortaleza, sabiduría y apoyo representados en cada una de las personas que me supieron dirigir, con sus consejos y palabras de aliento día a día.

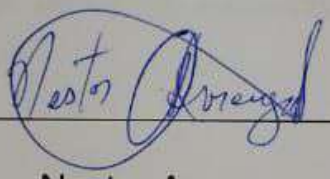
DEDICATORIA

A mi madre que desde lejos me brinda todo el apoyo necesario.

TRIBUNAL DE SUSTENTACIÓN

Ing. Lehin Freire

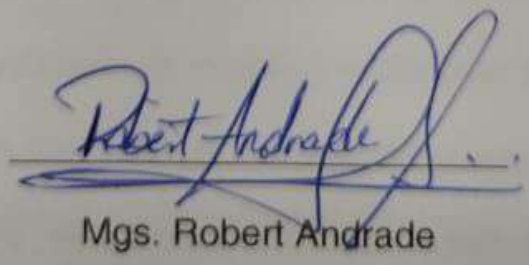
DIRECTOR MSIA



Mgs. Nestor Arreaga

PROFESOR DELEGADO

POR LA UNIDAD ACADÉMICA



Mgs. Robert Andrade

PROFESOR DELEGADO

POR LA UNIDAD ACADÉMICA

RESUMEN

El desarrollo del presente proyecto de “Implementación de una plataforma tecnológica para prevenir la fuga de datos en la red administrativa del Servicio Integrado de Seguridad Zonal”, tiene como objetivo el control y monitoreo de dispositivos y del envío de información dentro y fuera de la institución.

Mediante la implementación de la plataforma CosoSys Endpoint Protector nos permite realizar controles a través de políticas de seguridad de difusión de archivos usando monitoreo, bloqueos y restricción de adjuntos en correos electrónicos, mensajería instantánea, navegadores web, servicios en la nube o dispositivos portátiles de almacenamiento, con el fin de proteger la confidencialidad de la institución.

ÍNDICE GENERAL

ABREVIATURAS Y SIMBOLOGÍA

CTE	Comisión de tránsito del Ecuador
FFAA	Fuerzas Armadas
GPS	Sistema de posicionamiento global (Global Positioning System)
LDP	Prevención de fuga de datos (Data Leak Prevention)

ÍNDICE DE FIGURAS

INTRODUCCIÓN

El Servicio Integrado de Seguridad Ciudadana ha creado y administrado su propia base de datos y a través de su procesamiento se genera información útil, como informes estadísticos, cuyos resultados permiten medir la eficiencia y funcionalidad, el grado de participación de la instituciones de respuesta, además conocer los sectores de toda la provincia con mayor índice delincuencial, es por ello que dicha información es estrictamente confidencial para las instituciones adscritas, la cual no es de conocimiento y dominio público y no puede ser descubierta.

El presente proyecto tiene como finalidad la implementación de una plataforma que permita el control y monitoreo del envío de información dentro y fuera de la institución a través de correos electrónicos, mensajería instantánea, navegadores web, servicios en la nube o dispositivos portátiles de almacenamiento, con el fin de proteger los datos sensibles, imposibilitando a los personas no autorizados acceder a información fuera de la empresa y proteger de la divulgación de datos confidenciales.

Actualmente el crecimiento de la tecnología avanza rápidamente, y la restricción mediante reglas de firewall, bloqueos a sitios o monitorear el historial de páginas web no es suficiente, a simple vista es normal adjuntar un archivo en cualquier correo, lo cual no es prohibido pero podría causar fuga de datos a la institución y atentar contra la confidencialidad si no se implementan políticas que restrinjan la difusión de datos sensibles.

CAPÍTULO 1

GENERALIDADES

1.1 DESCRIPCIÓN DEL PROBLEMA

El Servicio Integral de Seguridad es un ente coordinador de emergencias, en la que están adscritas diferentes instituciones de socorro como son Policía Nacional, Cuerpo de Bomberos, Ministerio de Salud, CTE, FFAA, Ministerio de Gestión de Riesgo, Municipio.

Actualmente posee una innovadora plataforma tecnológica ofreciendo los servicios de recepción de llamadas, video vigilancia, GPS y botones de auxilio.

La red administrativa del servicio integrado, a la que tiene acceso el área de dirección de operaciones, administración, financiero, planificación, jurídico y tecnología, maneja información confidencial la misma que se ve amenazada por el uso constante de la red Internet.

El envío de información en la que intervienen, correos electrónicos, navegadores web, mensajería instantánea, dispositivos USB, da lugar a que la confidencialidad de la información se encuentre amenazada por factores que requieren de un control.

Las instituciones articuladas requieren enviar informes diariamente a correos que pertenecen a su institución, sin embargo el uso de correos personales es un problema por la posible fuga de información, así como el uso de dispositivos de almacenamiento externo y dispositivos portátiles fuera de control.

1.2 SOLUCIÓN PROPUESTA

Para la prevención de fuga de datos detallamos las siguientes soluciones:

- Implementar las políticas de seguridad para restricción de dispositivos de almacenamiento externos no autorizados por la institución y restricción de dispositivos portátiles.

- Implantar la plataforma CosoSys Endpoint Protector para realizar controles mediante políticas de seguridad en: estaciones de trabajo, portátiles, e-mails, navegación web, adjuntos y escaneo de documentos.

- Generación de informes de monitoreo y bloqueos de posible fuga de datos.

CAPÍTULO 2

DESARROLLO DE LA SOLUCIÓN

2.1 SITUACIÓN ACTUAL DE LA INSTITUCIÓN

En la actualidad la provincia cuenta con el Servicio Integral centralizado para la coordinación de llamadas de emergencia en la que participan instituciones de socorro, las mismas que coordinan la atención a la ciudadanía brindando mediante sus recursos el auxilio inmediato, dichas instituciones requieren la comunicación con sus oficinas principales para obtener el apoyo necesario, por lo que se ven en la necesidad de compartir información fuera de la central de emergencias, las instituciones tienen como bien entregar reportes de sus respectivas organismos, por lo que se dificulta el control de fuga de datos.

El área Operativa la constituyen los operadores de llamadas, operadores de video vigilancia, despachadores de las instituciones adscritas, calidad y supervisores de llamadas y despacho, esta área ya cuenta con restricciones al Internet, restricciones en el ingreso a la sala, sin embargo cuenta con un acceso para envío de información hacia fuera de la institución para enviar sus informes diariamente, vía correo electrónico como datos adjunto, la misma que se encuentra propensa a la difusión de datos no autorizados.

El centro cuenta con un aplicativo web de seguridad para compartir reportes e información estadística semanal o mensual con las instituciones adscritas al centro según convenios firmados, Además de la información que se maneja con Fiscalía en la entrega de videos la misma que es controlada y entregada mediante un aplicativo web centralizado en el Servicio Integrado de Seguridad Quito, sin embargo los informes inesperados y comunicación por correo a las instituciones se ve amenazada por la posible fuga de datos por lo que amerita el monitoreo y control, la institución es una empresa joven con una amplia infraestructura la misma que crece día a día en tecnología y calidad de servicio.

La red Administrativa de la central de emergencia la conforma los departamentos, Financiero, Recursos Humanos, Jurídico, Estadística,

Planificación, Dirección de Operaciones, Compras Públicas y Tecnología, las mismas que albergan datos sensible que requiere un seguimiento constante.

El Servicio de Seguridad Integrado cuenta con diferentes salas de acceso a Internet libre como la sala de prensa y la sala de crisis, éstas requieren restricciones de red, además de la prohibición de dispositivos centralizada para un mejor control en las diferentes salas.

2.2 VULNERABILIDADES EN LA ENTREGA DE INFORMACIÓN

La información que manejan las diferentes instituciones adscritas al Centro Zonal es de suma confidencialidad debido a la importancia de los informes que se realizan de manera inesperada según los sucesos ocurridos de las emergencias, robos, asaltos, muertes requiere de un monitoreo constante debido a la fuga que se pueda presentar al enviar este tipo de información confidencial. [1]

En el área Administrativa en los departamento de Estadística y Dirección de Operaciones son los encargados de informar mediante un aplicativo las emergencias recibidas, información estadística de robos, estadísticas de alertas recibidas por categoría, emergencias atendidas por el sistema de gestión sanitaria, Gestión de Riesgos, Gestión de Siniestros, Seguridad Ciudadana, Servicios Municipales, servicio militar, tránsito y movilidad, despachos realizados por consola e institución, etc.

A pesar de realizar el debido control mediante un aplicativo de pertenencia del Servicio Integrado el mismo que se aloja en Quito, la vulnerabilidad se encuentra en otros medios como transferencia de archivos mediante la nube como wetransfer, dropbox, google drive, y demás mensajería instantánea la misma que necesita de su debido control ya que es necesaria la comunicación y transferencia de archivos con otros Servicios Integrados del país y con su central en Quito.

En general los informes de alertas, situación financiera, compras públicas, informes de planificación, actas de jurídico e información sensible de tecnología hacia los proveedores, central Quito y demás empresas que intervienen en la comunicación diaria se ve en la necesidad de llevar un control de bloqueo y monitoreo de toda la información que maneja el área Administrativa en la red.

2.3 IMPLEMENTACIÓN DE PLATAFORMA PARA LA PREVENCIÓN DE FUGA DE DATOS.

Una de las soluciones de hoy en día en el control y monitoreo de fuga de datos es la implantación de la plataforma Endpoint Protector CoSoSys la misma que nos permite monitorear y bloquear el uso de los dispositivos en cada computador, así como el monitoreo de archivos a difundir por la red ya sea en Internet o en la Intranet [2].

La plataforma es de pago la misma que presta las siguientes bondades:

- Monitoreo y control de archivos adjuntos en los diferentes navegadores, así como en mensajería instantánea.

- Bloqueo de envío de información mediante políticas.

- Monitoreo y control en transferencia de archivos en la nube como wetransfer, dropbox, google drive.

- Generación de informes de transferencias y movimientos de archivos por cada área.

- Bloqueo de tipos dispositivos como: memorias USB, unidades de CDS, DVD-RW, cámaras, teléfonos móviles, cámaras web, puertos seriales, lectoras de tarjetas, dispositivos bluetooth y otros dispositivos para compartir archivos en red.

2.3.1 INSTALACIÓN DE PLATAFORMA

Endpoint Protector Virtual Appliance 4.4.0.6 es una plataforma con base en el Sistema Operativo Ubuntu, que viene en dos presentaciones, su versión máquina virtual y dispositivo hardware, para este proyecto usaremos la versión de virtualización para Hiper V Manager 2012 de 64 bits la misma que la instalaremos en un servidor HP Proliant DL360p Gen8.

Al realizar la suscripción la empresa envía los link de descarga con las diferentes versiones.

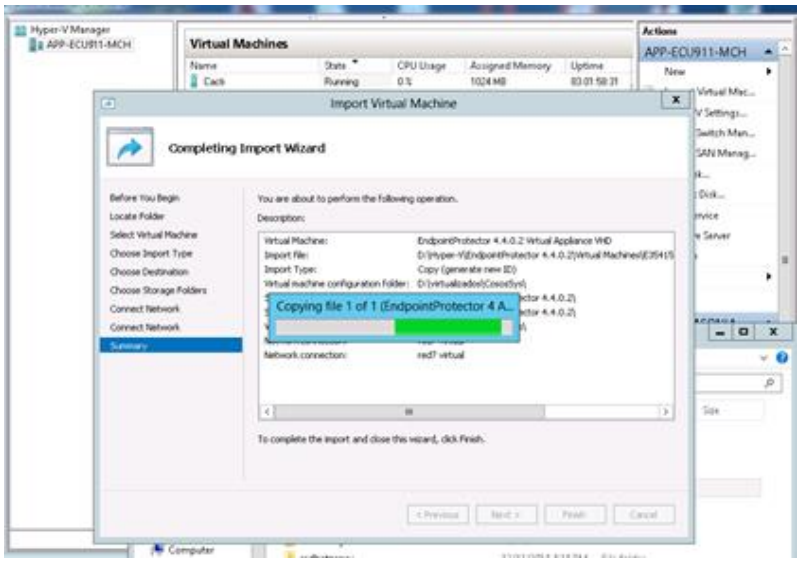


Figura 2.1. Importación de la máquina virtual

La plataforma permite el acceso remoto mediante una interfaz amigable.

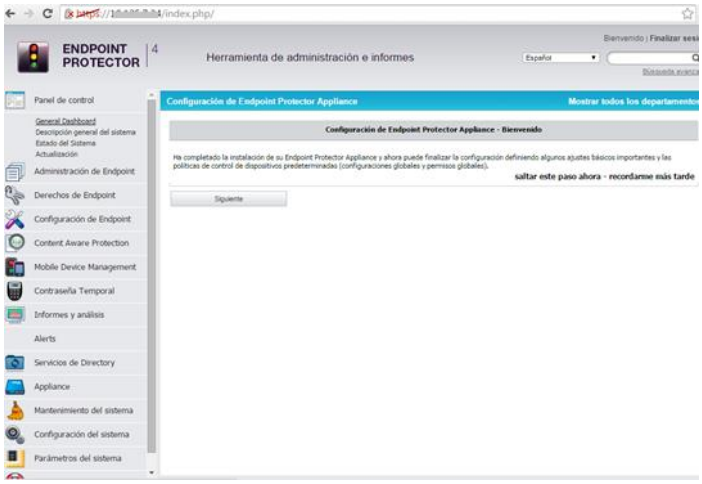


Figura 2.2. Interfaz web de la plataforma Endpoint Protector 4

Para ingresar a la plataforma lo hacemos mediante el protocolo seguro: https://ip_server_endpoint e ingresamos con el usuario y clave por defecto la misma que puede ser modificada desde la herramienta web. En el presente proyecto no mostraremos direcciones ip por lo que usaremos “ip_server_endpoint” para administrar la plataforma.

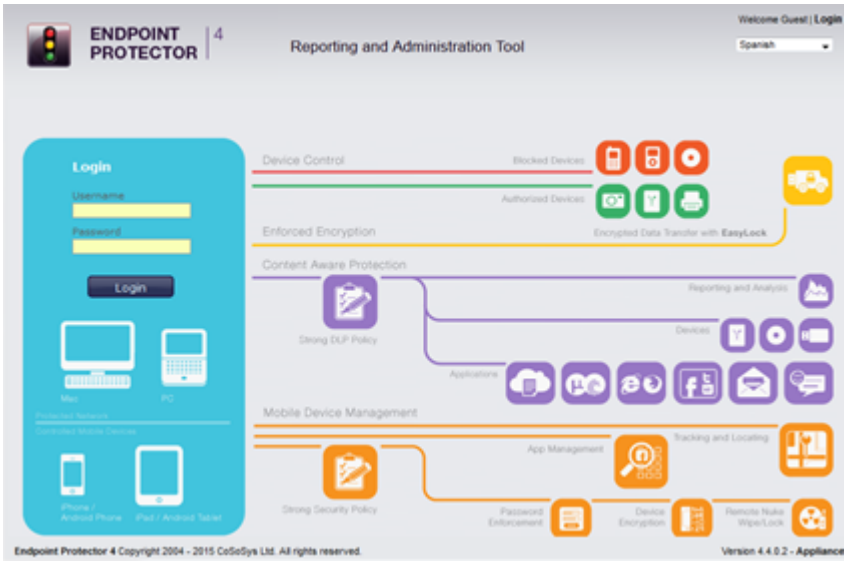


Figura 2.3 Ingreso a la plataforma

Al ingresar a la herramienta nos pide habilitar el modo de prueba o en caso de licencia el archivo requerido.

2.3.2 PUESTA EN MARCHA EN LOS USUARIOS.

Para que cada usuario se conecte a la plataforma se debe ingresar en el web http://ip_server_endpoint para descargar el agente instalador en sus diferentes versiones dependiendo del

sistema operativo. El software se comunica por el puerto 443 a la plataforma o servidor, el agente nos informa sobre los posibles bloqueos y acciones de control y monitoreo dependiendo de la configuración realizada en la plataforma a cada de uno de los equipos clientes.

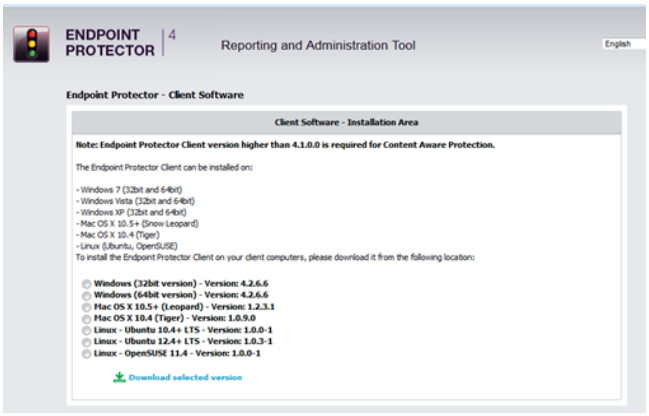


Figura 2.4. Agente para clientes de la plataforma.

Una vez instalado el agente este se colocara en el área de notificaciones de la barra de tareas.

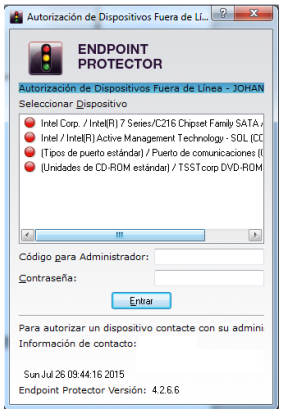


Figura 2.5. Agente instalado en clientes

2.4. DEFINICIÓN DE LA RED ADMINISTRATIVA.

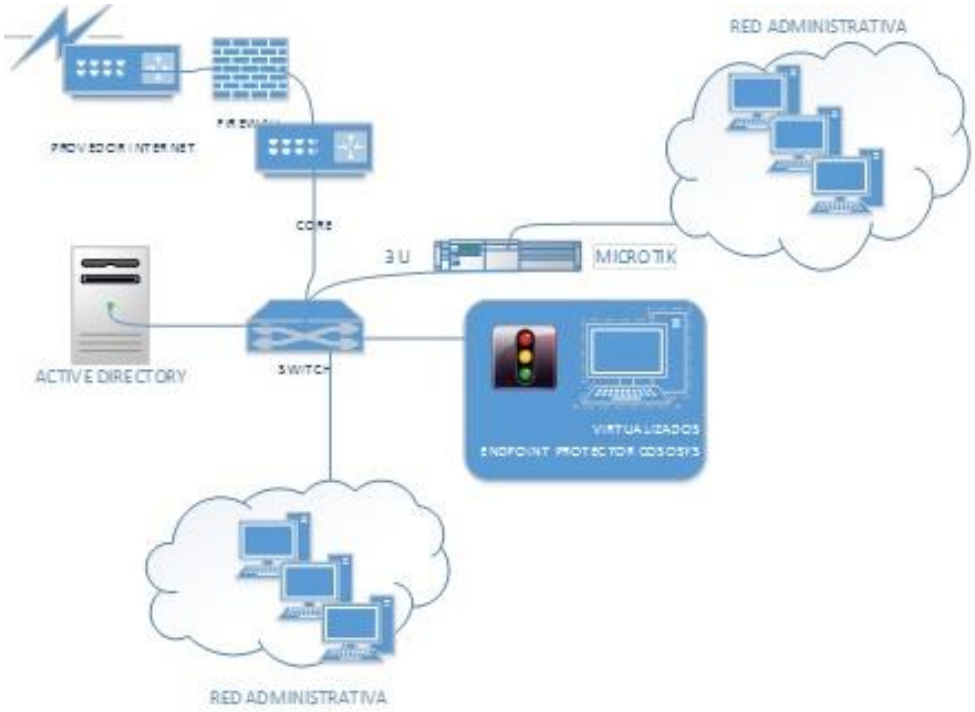


Figura 2.6 Red Administrativa.

Mediante el análisis previo sobre las políticas generadas por el departamento de tecnología nos vemos en la necesidad de implantar la herramienta que nos ayude en el cumplimiento de ellas en cuestión de fuga de datos en la red administrativa con acceso a Internet.

La Red Administrativa la constituyen las siguientes áreas: estadística, jurídico, planificación, compras públicas, financiero, dirección de operaciones, recursos humanos, gerencia, las mismas que cuentan con acceso al Internet a excepción de la red operativa la misma que se encuentra aislada por la sensibilidad de llamadas y video vigilancia.

2.5 CONFIGURACIÓN DE POLÍTICAS PARA ASEGURAR LA INFORMACIÓN

El Servicio Integrado de Seguridad cuenta con algunas políticas para realizar el control en cuanto a la prevención de fuga de datos, entre ellas están las políticas de permanencia en las instalaciones y políticas de difusión de información.

La finalidad de este proyecto es que a través de políticas aplicar restricciones según como sea conveniente, entre las políticas podemos citar las siguientes:

- Está prohibido bajar, obtener, difundir, divulgar, eliminar, quemar y/o guardar información del Servicio Integrado de Seguridad, sin previa autorización de su superior jerárquico o para fines diversos a los establecidos para su cargo.
- Queda prohibido el ingreso a las Salas Operativas de cualquier accesorio tales como carteras, mochilas, teléfonos celulares, computadoras portátiles, laptops, etc, a excepción de los equipos que serán autorizados por el Centro. Estos deberán ser ubicados en el casillero asignado.
- No todos los usuarios pueden visualizar información de carpetas compartidas, por ello se normaliza el acceso a carpetas o archivos

basándose en la categorización de los perfiles de usuarios (Administradores, Usuarios Comunes).

2.5.1 DIFUSIÓN DE LA INFORMACIÓN

La difusión de la información se puede dar a través de dispositivos conectados, por Internet en general, mensajería electrónica, servidores de alojamiento web, redes sociales, etc, para lo cual vamos tratar dos puntos, la gestión de dispositivos y la gestión de archivos adjuntos.

2.5.1.1 CONTROL DE DISPOSITIVOS

Nos permite gestionar el monitoreo y bloqueo a dispositivos como USB, cámaras web, lectoras de tarjetas, cds, etc.

Políticas para control de dispositivos:

- Todo el personal que labora en el Servicio Integrado de Seguridad debe tener acceso sólo a la información necesaria para el desarrollo de sus actividades.
- Está prohibido el uso de dispositivos para extracción de información como discos duros externos, discos ópticos como DVD/RW, o CD/RW, pen drive o

cualquier dispositivo de almacenamiento externo, la única excepción para la extracción de información es emitida por el SubDirector Zonal.

Implementación de política en plataforma:

En la opción Derechos de Endpoint se puede configurar el acceso a los dispositivos mediante: permisos a dispositivos, permisos a equipos, permisos a usuarios, permisos globales.

Para nuestro caso vamos a configurar permisos a equipos, necesitamos bloquear dispositivos como: dispositivos USB, cd, dvd rw, impresoras, conexión a mobiles, etc.

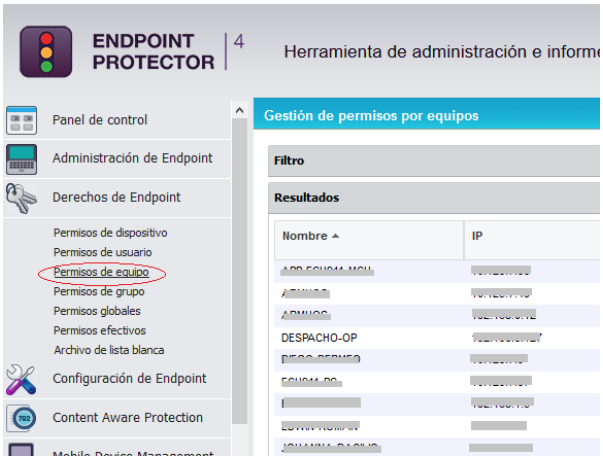


Figura 2.7. Permisos de equipo

En esta opción denegaremos el acceso a cualquier dispositivo para los diferentes equipos según la política.

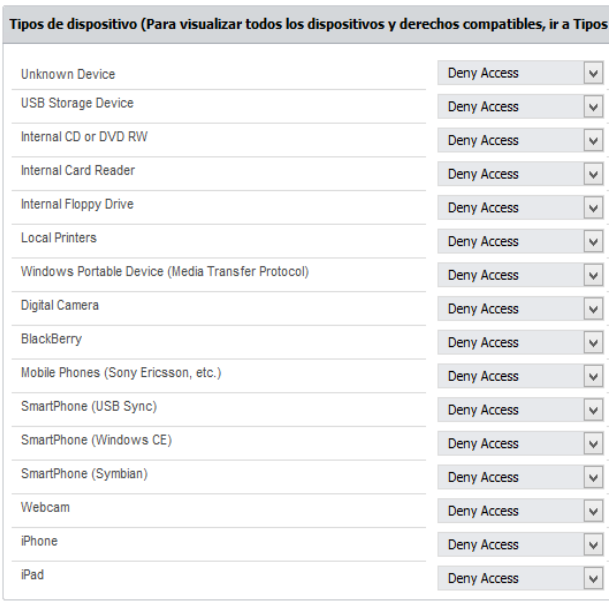


Figura 2.8 Permisos de dispositivos por equipo.

En la opción derechos efectivos podemos realizar la consulta de dispositivos permitidos y denegados por equipo o usuario.

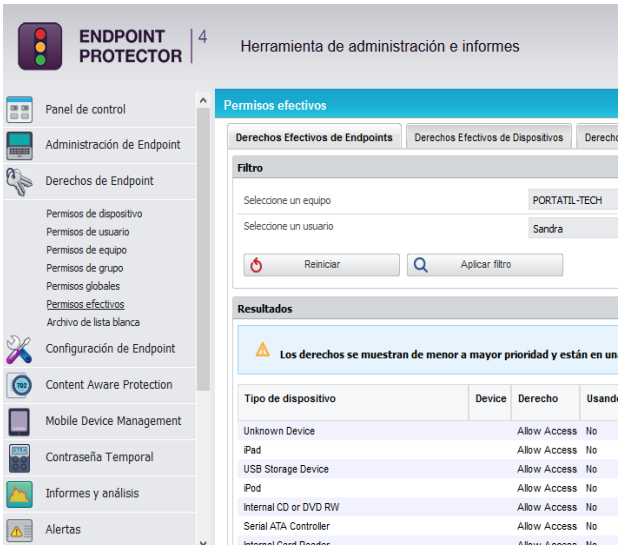


Figura 2.9 Permisos heredados por usuario y equipo.

2.5.1.2 CONTROL DE ARCHIVOS ADJUNTOS.

En la plataforma podemos realizar la creación de políticas de contenido para realizar el debido monitoreo y bloqueo de archivos ya sea por tipo de navegador, mensajería instantánea, redes sociales, servidores de almacenamiento.

Políticas:

- Los usuarios del Servicio Integrado de Seguridad podrán transferir información haciendo uso de la red LAN, por medio de los mails que se han designado para cada uno, en caso de necesitar transferir alguna información, que por su naturaleza o capacidad

exceda los límites de los medios informáticos establecidos, se solicitará el soporte al Departamento Tecnológico.

- En caso de tener restringida la opción de adjuntar algún tipo de archivo no permitido deberá pedir autorización a su jefe inmediato y al área de tecnología el desbloqueo.

Para realizar un control de permisos es necesaria la creación de departamentos.

Creación de Departamentos.

La herramienta nos permite crear departamentos para un mejor control de usuarios o equipos, en la opción configurar el sistema, departamentos del sistema.

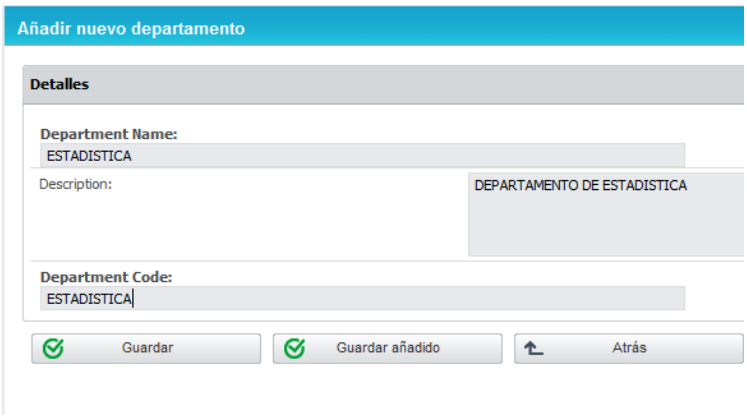


Figura 2.10 Creación de departamentos del sistema

Figura 2.11 Lista de Departamentos.

Monitoreo de Archivos.

En la opción de Protección de Contenido se despliegan algunas opciones como la creación de políticas de contenido de conciencia, como indica en la Figura 2.12, Se creó la política de monitoreo de archivos, esta opción se la ha asignado a todos los departamentos y es de prioridad 1, lo que se pretende es monitorear todo el tráfico de archivos en los usuarios cuyo reporte servirá para mayor control.

Política:

- Los directores de cada departamento tendrán acceso a informes de monitoreo referente a archivos transferidos del área al que pertenece.

Implementación en plataforma:

Nombre de la Política: Monitoreo de Archivos

Acción: Reportar y las notificaciones a los usuarios serán invisibles.

Aplicado a: navegadores web, aplicaciones mail, mensajería instantánea, redes sociales.

Filtro a archivos: gráficos, office, comprimidos, multimedia, etc.

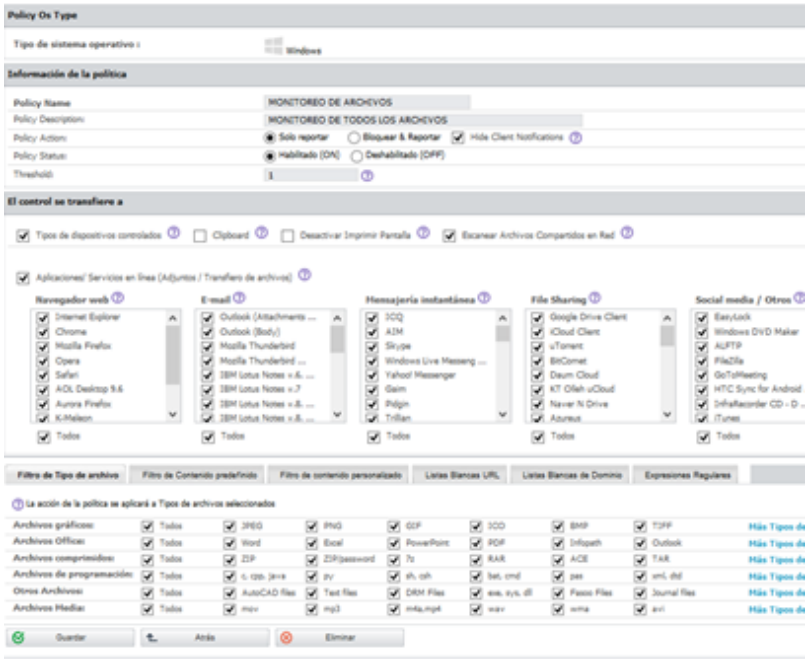


Figura 2.12. Política de monitoreo de archivos

Restricción en tecla Imprimir Pantalla.

Para ciertos departamentos es necesario bloquear la tecla print screen del teclado el computador ya que puede ser causa de fuga de datos en información sensible como la información que maneja distintas áreas.

Política:

Los usuarios tienen prohibido la difusión de capturas de pantalla en departamentos como Financiero, Dirección de Operaciones, Compras Públicas, las mismas que deberán ser autorizadas por la Dirección Administrativa o Gerencia y la Dirección Tecnológica.

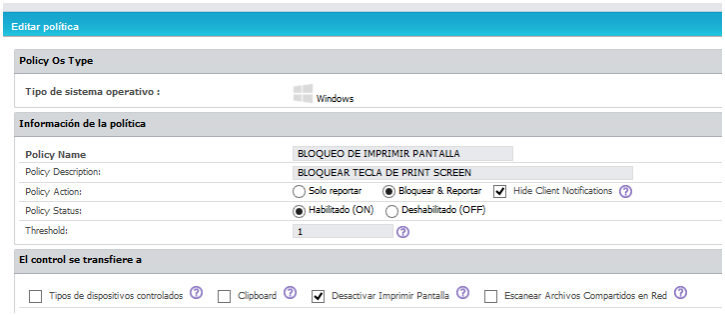


Figura 2.13. Bloqueo de Imprimir Pantalla.

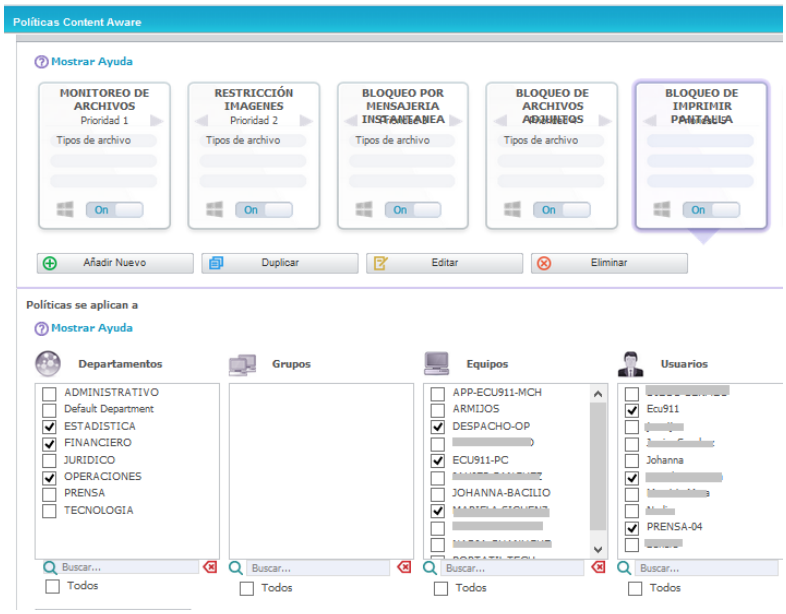


Figura 2.14. Políticas aplicadas a distintos departamentos.

Adjuntos solo por Outlook

La dirección de Operaciones tiene a su cargo equipos en uso estrictamente para envió de correos usada por la coordinación de Instituciones quienes deben presentar información espontanea a sus organismos.

Para lo cual se ha implementado la siguiente política de restricción en la plataforma:

Nombre de la Política: Adjunto solo por Outlook

Acción: Bloquea adjuntos mediante cualquier tipo de aplicativos como navegadores web, aplicaciones mail,

mensajería instantánea, redes sociales permitiendo solo archivos adjuntos mediante Outlook

Filtro a archivos: gráficos, office, comprimidos, multimedia, etc.

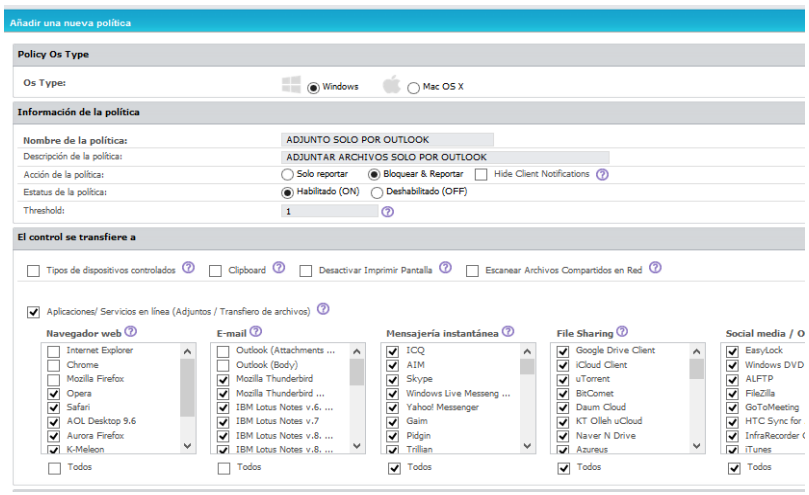


Figura 2.15. Bloqueo de cualquier fuente de transferencia de datos, excepto Outlook.

Restricción de difusión de imágenes.

Los mismos equipos en donde su uso es estrictamente informativo, está prohibido el envío de imágenes, para lo cual se creó la siguiente política.

Nombre de la Política: Restricción de imágenes.

Acción: Bloqueo de adjuntos imágenes.

Filtro a archivos: toda clase de archivos en formato de imágenes.

La política se indica en el siguiente gráfico.

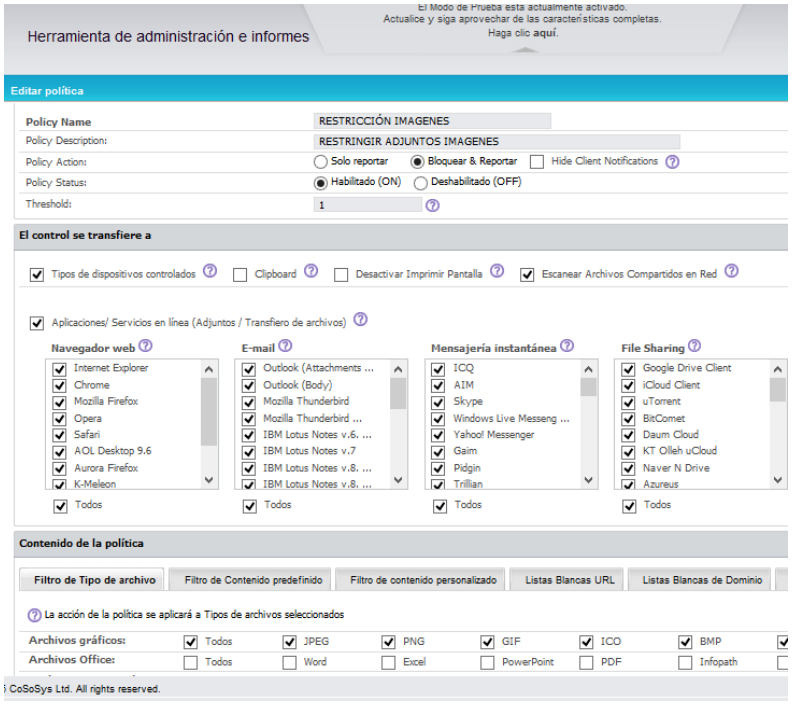


Figura 2.16. Bloqueo de adjuntos imágenes.

Bloqueo de difusión de archivos de mensajería instantánea.

Para la mayoría de departamentos está prohibido el envío de archivos adjuntos de cualquier tipo por mensajería instantánea.

Nombre de la Política: Bloqueo por mensajería instantánea.

Acción: Bloqueo a mensajería instantánea.

Filtro a archivos: toda clase de archivos en cualquier formato.

La política se indica en el siguiente gráfico

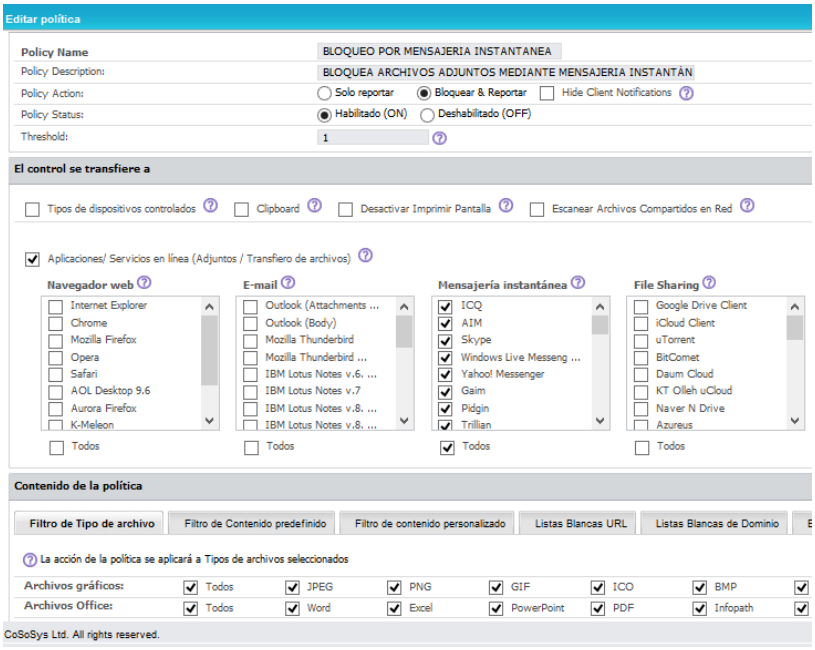


Figura 2.17. Bloqueo de envío de archivos a través de mensajería instantánea.

Desbloqueo de dispositivos mediante contraseña temporal

Los equipos como portátiles de uso de la institución para realizar videoconferencia en reuniones de trabajo con otros Centros de Servicio Integrado del país deberán acogerse a la siguiente política.

Política: Pedir autorización a su jefe inmediato para realizar el uso de cualquier dispositivo que se encuentre bloqueado.

La herramienta nos permite realizar un desbloqueo temporal de dispositivos mediante la generación de una clave, la misma que se entrega al usuario para que tenga uso del mismo como es en el caso de la cámara web.

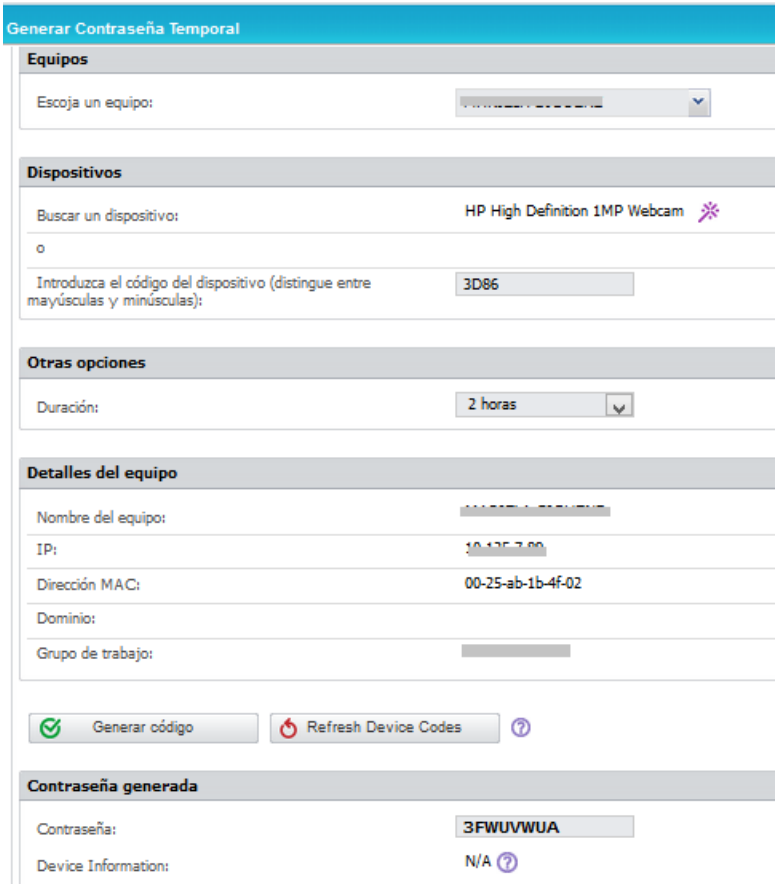


Figura 2.18. Desbloqueo con duración de 2 horas del dispositivo webcam.

El usuario deberá ingresar la clave suministrada por el departamento de tecnología, en el agente instalado en su equipo, para realizar el desbloqueo del dispositivo como se indica en la siguiente figura.

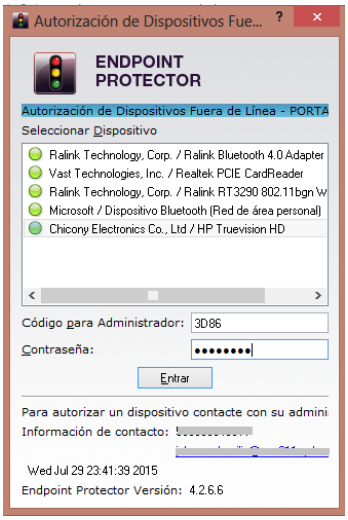


Figura 2.19. Ingreso de clave temporal en el cliente Endpoint.

CAPÍTULO 3

ANÁLISIS DE RESULTADOS

3.1 RESULTADOS OBTENIDOS.

La plataforma nos brinda informes sobre el monitoreo por equipos, usuarios o departamentos, estos reportes pueden clasificarse en: Informes de dispositivos e Informes por políticas de contenido, en el que nos permite visualizar a detalle el seguimiento de la acción realizada ya sea de lectura, escritura o eliminación de archivos.

Además nos permite descargar el archivo físicamente ya que es copiado al servidor para su posterior análisis cuando la herramienta realizo el monitoreo o bloqueo, la figura 3.20 muestra el proceso que realiza la herramienta al ejecutar el bloqueo o monitoreo, copia el archivo en su base de datos, y deniega o permite la copia del archivo a dispositivos, red o herramientas web, según la política dada al equipo, usuario o grupo.

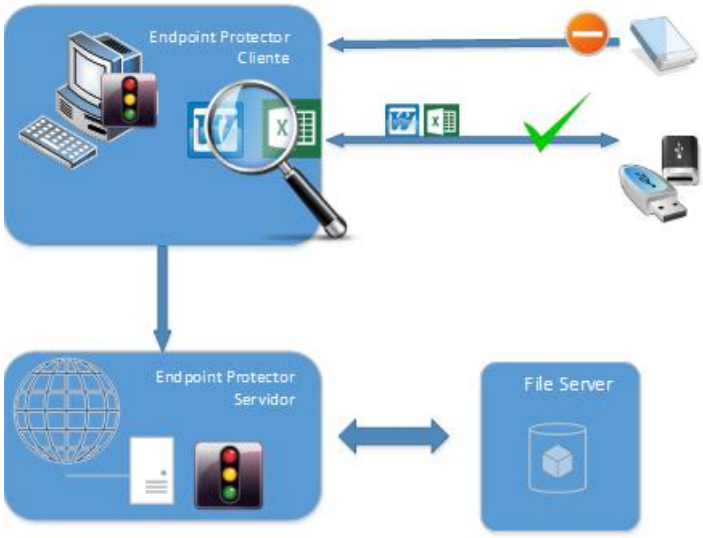


Figura 3.20. Proceso Endpoint Protector server y agente.

3.2 REPORTE DE MONITOREO A DISPOSITIVOS

El Informe de dispositivos ya sea denegado o concedido se revisa en el siguiente listado que muestra la figura 3.21 en la opción Informe de dispositivos del menú de la plataforma en el que detalla el nombre del dispositivo, usuario o equipo y fecha que fue accedido.

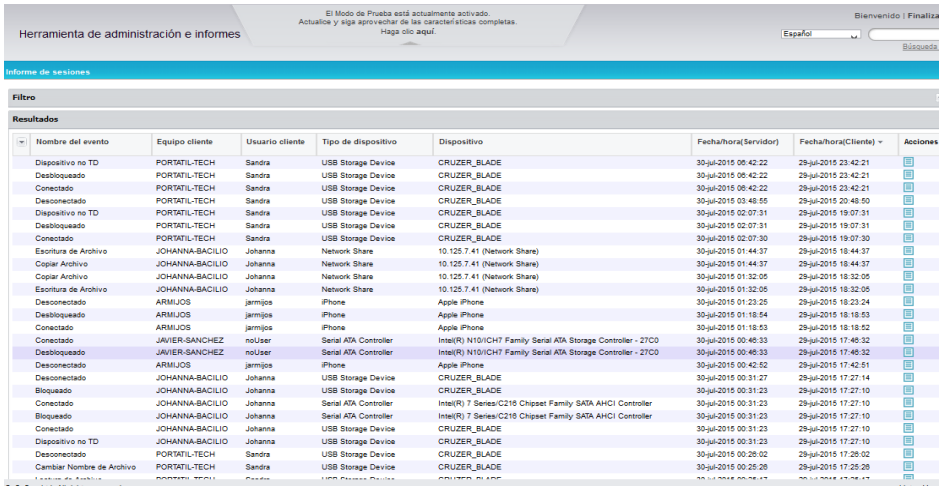


Figura 3.21. Informe de dispositivos conectados.

3.3 REPORTE DE MONITOREO DE ARCHIVOS.

Consulta de rutas de archivos

En el Informe de la figura 3.22 se visualiza el movimiento de archivos por usuarios o equipos donde podemos revisar el evento ya sea copia, eliminación o lectura del archivo, además detalla nombre del archivo, ruta de origen, ruta de destino, fecha, hora y tipo de archivo, dicha opción la encontramos en Informes y Análisis, File Tracing. [3]

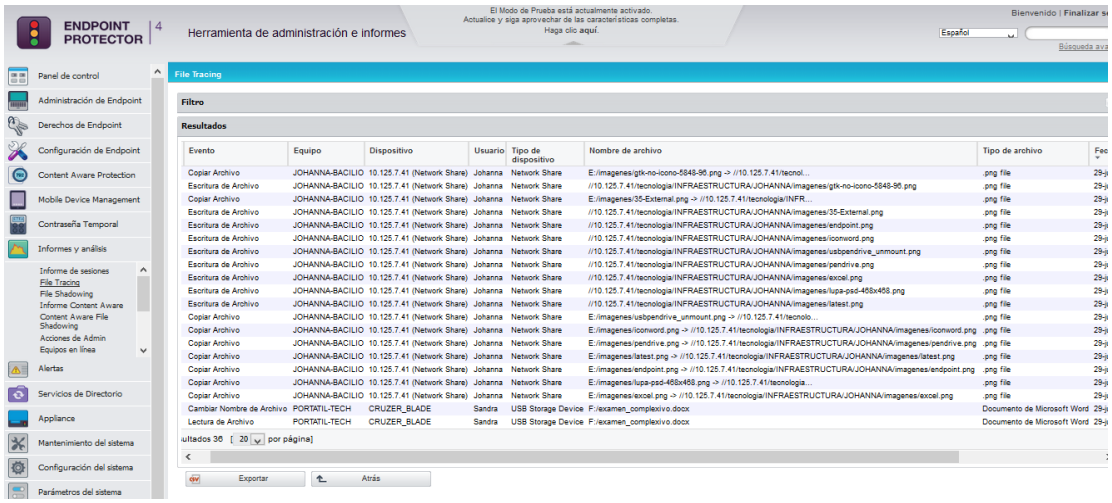


Figura 3.22. Opción File Tracing

3.2.2. DESCARGA DE ARCHIVOS MANIPULADOS.

El siguiente reporte permite mostrar la lista de archivos y obtener una copia que se encuentra alojada en el servidor de Endpoint Protector, la misma que fue copiada al momento que el agente intervino en el monitoreo o bloque según la política definida.

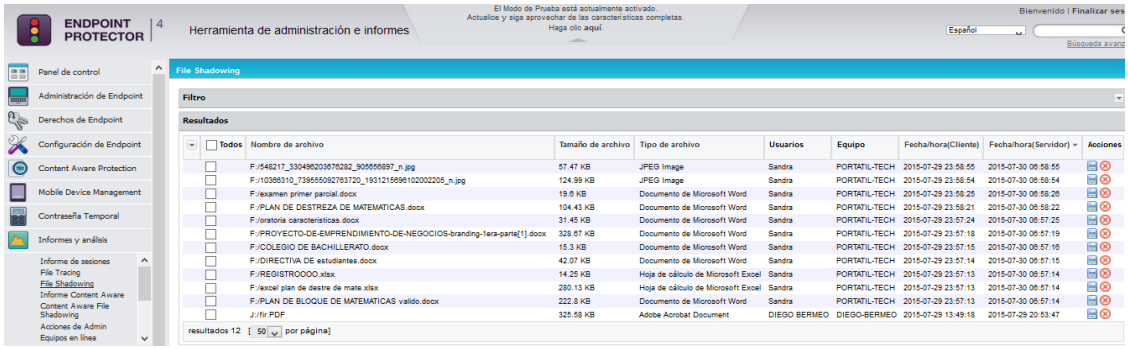


Figura 3.23. Opción File Shadowing

3.2.3. INFORME DE MONITOREO DE ARCHIVOS.

La figura 3.25 nos muestra un Informe sobre la aplicación de las políticas de contenido consiente que fueron detectadas y que se aplicaron con fecha y hora, también contiene el nombre del equipo, usuario, la ruta destino de la transferencia, los informes se pueden exportar en formato csv.

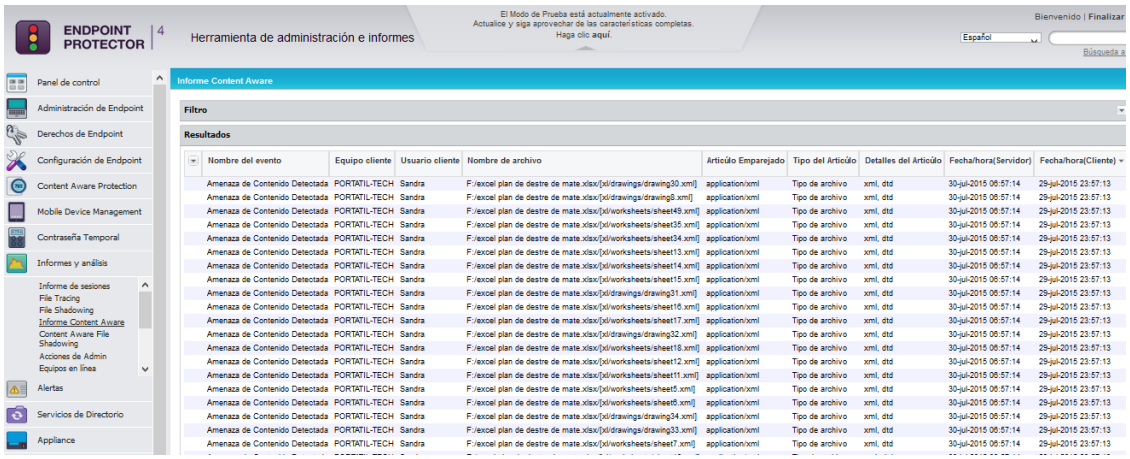


Figura 3.24. Informe de Content Aware.

3.4 ALERTAS

La herramienta Endpoint Protector permite configurar notificaciones o alertas en la transferencia de contenido ya sea por bloqueo o monitoreo, las alertas enviaran un e-mail al administrador del equipo según la configuración del sistema de la plataforma, opción encontrada en ajustes del sistema.

Podemos crear varios tipos de alertas por departamento, equipos, grupos, usuarios.

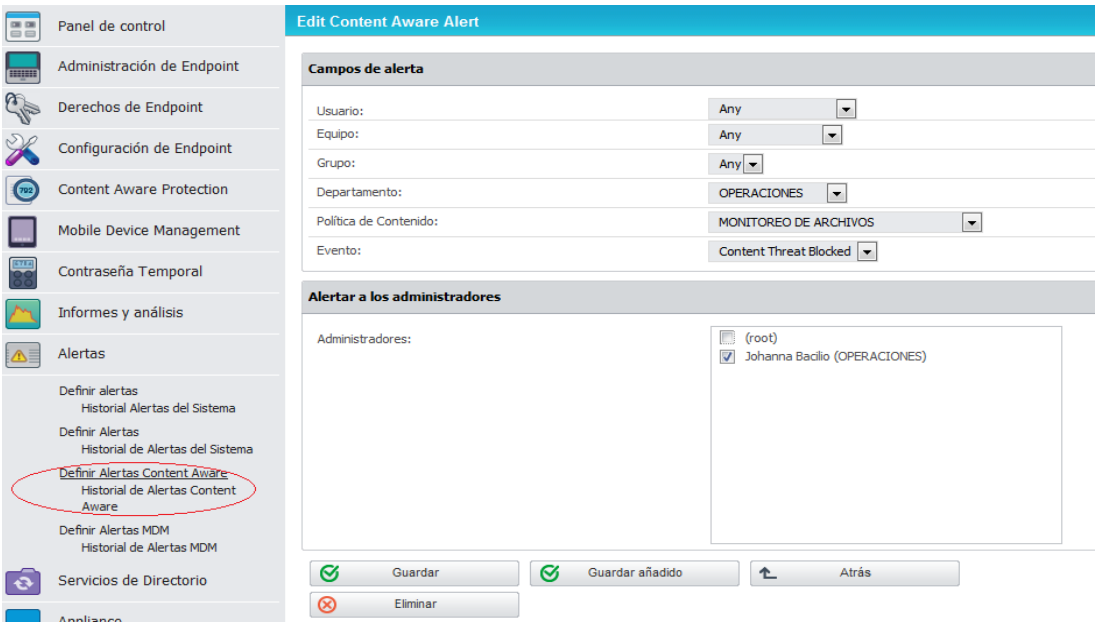


Figura 3.25. Creación de alertas

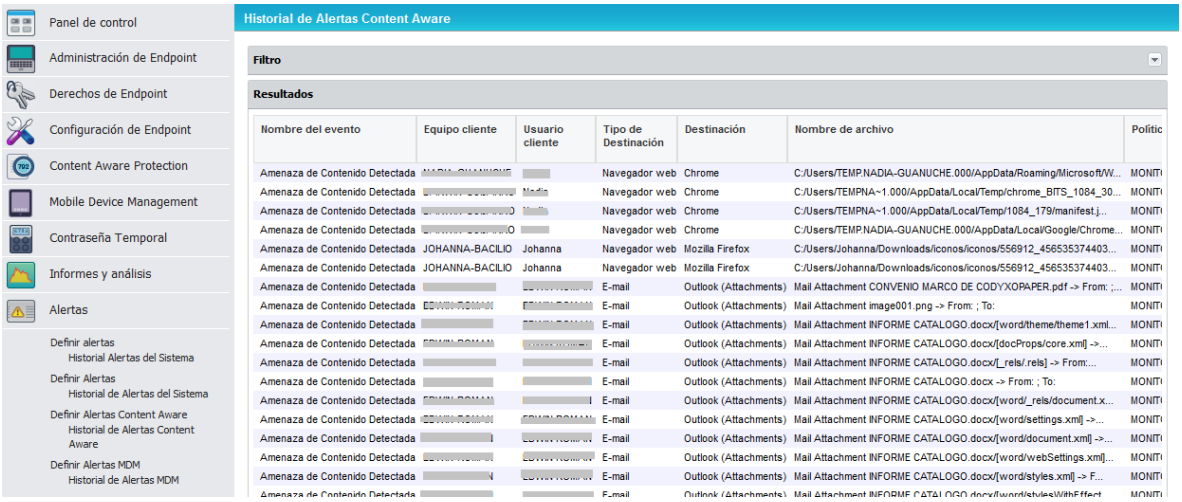


Figura 3.26. Historial de Alertas del sistema

3.5 CONFIDENCIALIDAD EN DOCUMENTOS.

¿Cuál es el costo de la imagen y credibilidad que tendrá que afrontar la institución ante la pérdida o acceso indebido de datos sensibles? [4]

La confidencialidad de los datos con los que cuenta el Servicio de Seguridad Integrado es de suma importancia ya que la pérdida o divulgación de información podría ocasionar muchos factores negativos tanto para la institución y ciudadanía en general, un video, fotos, capturas, informes, serán monitoreados y bloqueados según las reglas ya definidas en la institución.[5]

El departamento de comunicación tiene como bien informar a la ciudadanía de los acontecimientos, fotos, videos que estrictamente son autorizados para su difusión, sin embargo la institución cuenta con mucha información confidencial que necesariamente debe de ser protegida para evitar difusiones no autorizadas.

CONCLUSIONES Y RECOMENDACIONES

CONCLUSIONES

1. La herramienta previene la fuga de datos a través de la aplicación de políticas por departamento, equipos o usuarios, para llevar un mejor control y monitoreo de la información que sale de la institución.

2. La comunicación en red no solo requiere del monitoreo y restricción de páginas web. Claramente se necesita tener controles para la prevención de fuga de datos que protejan la confidencialidad de la información sensible.

RECOMENDACIONES

1. Generar informes periódicamente para realizar el seguimiento de archivos difundidos.

2. Adquirir licencias para obtener las actualizaciones de la plataforma.

3. Implementar nuevas políticas acorde con los bloqueos sugeridos.

BIBLIOGRAFÍA

[1] INFORC, Determinar si los empleados son la preocupación para la seguridad de datos, http://www.inforc.ec/category/dlp/, fecha de consulta julio del 2015.

[2] Hans Steffens, Prevención de fuga de datos (DLP) en cinco pasos, http://liacolombia.com/2010/09/prevencion-de-fuga-de-datos-dlp-en-5-sencillos-pasos/, fecha de publicación septiembre del 2010.

[3] CoSoSys, Data Sheet Endpoint Protector 4 de Cososys en español, http://www.endpointprotector.com/support/pdf/datasheet/Data_Sheet_Endpoint_Protector_4_CoSoSys_ES.pdf, fecha de publicación 12 de junio del 2015.

[4] América Economía, La fuga de información es una razón por las que las empresas pierden dinero, http://www.soluciondlp.com/category/prevencion-de-la-perdida-de-datos/, fecha de publicación el 22 de julio del 2014.

[5] Calvo Moyano Arantxa, Fuga de información, la mayor amenaza para la reputación corporativa, http://www.redseguridad.com/opinion/articulos/fuga-de-informacion-la-mayor-amenaza-para-la-reputacion-corporativa, fecha de consulta julio del 2015.