# Aplicación de una herramienta de seguridad para la prevención de fuga de información

# Application of a security tool for the prevention of leakage of information

GONZÁLEZ-RAMÍREZ, Claudia Teresa†*, GÓMEZ-MARTÍNEZ, Leonardo, COLÍN-MORALES, José Manuel y DELGADO-PICHARDO, Mauricio

*Tecnológico Nacional de México/Instituto Tecnológico de Zitácuaro*

ID 1er Autor: *Claudia Teresa, González-Ramírez* / **ORC ID**: 0000-0002-4106-4583, **Researcher ID Thomson**: G-6313-2019

ID 1er Coautor: *Leonardo, Gómez-Martínez* / **ORC ID**: 0000-0002-5821-3573

ID 2do Coautor: *José Manuel, Colín-Morales* / **ORC ID**: 0000-0002-9438-5217

ID 3er Coautor: *Mauricio, Delgado-Pichardo* / **ORC ID**: 0000-0003-1129-2128

**DOI**: 10.35429/JTEN.2020.13.4.24.33 Recibido 03 de Marzo, 2020; Marzo 30 Junio, 2020

**Resumen**

Considerando que día con día la mayoría de los servicios brindados por cualquier organización, se están migrando a entornos que involucran el uso de equipos de cómputo, servidores y redes de datos, también se deben considerar los múltiples ataques que sufren las empresas, enfocados al robo de información, falsificación, modificación de servicios, suplantaciones, vulnerabilidades en sistemas, entre muchas cosas. A pesar de la gran utilidad y todas las ventajas que ofrecen las redes no se puede dejar a un lado y mucho menos dar por hecho que la seguridad de la organización se encuentra en óptimas condiciones, conceptos como la implementación, administración y seguridad informática. Por ello la empresa debe contar con un esquema de seguridad de Prevención de Fuga de Información, basado en un sistema de seguridad con las herramienta que proporcione éstas ventajas como lo es necesidades y objetivos de la misma.

**Seguridad, Prevención, Información**

**Abstract**

Considering that day by day most of the services provided by any organization are being migrated to environments that involve the use of computer equipment, servers and data networks, the multiple attacks suffered by companies, focused on theft, must also be considered. information, falsification, modification of services, impersonations, vulnerabilities in systems, among many things. Despite the great usefulness and all the advantages that networks offer, it cannot be left aside, much less assume that the security of the organization is in optimal conditions, concepts such as implementation, administration and computer security. Therefore, the company must have an Information Leakage Prevention security scheme, based on a security system with the tools that provide these advantages.

**Security, Prevention, Information**

**Citación**: GONZÁLEZ-RAMÍREZ, Claudia Teresa, GÓMEZ-MARTÍNEZ, Leonardo, COLÍN-MORALES, José Manuel y DELGADO-PICHARDO, Mauricio. Aplicación de una herramienta de seguridad para la prevención de fuga de información Revista de Ingeniería Tecnológica. 2020. 4-13: 24-33

* Correspondencia del Autor (Correo electrónico: claudia.lic@gmail.com)
† Investigador contribuyendo como primer autor.

 

## Introducción

La finalidad del proyecto es el diseño e implementación de un sistema de seguridad de Prevención de Fuga de Información en una organización ya que el crecimiento de las redes locales en los últimos años ha permitido incrementar el flujo de la información a grandes escalas, permitiendo con ello agilizar procesos personales, informativos, comerciales y educativos, pero aunado a ello nuevas amenazas y vulnerabilidades.

En la actualidad es imprescindible la implementación de una red en cualquier sector, debido a la existencia de una empresa que no cuente con una infraestructura de este tipo no le será posible garantizar su productividad y mucho menos su seguridad.

Todas las actividades que involucran el uso de computadoras y telecomunicaciones están relacionadas con información, dado que ésta es un bien al cual es asociado un valor, por lo tanto, están sujetos a riesgos, impactando de esta manera tanto económica como comercial.

Las empresas actualmente están buscando mecanismos que permitan minimizar el riesgo al cual puedan estar expuestos, a causa de que no existe como tal un proceso que se debiera seguir y que con ello garantice o se considere una red cien por ciento segura, pues la práctica demuestra lo contrario, así se implementen mecanismos de control, como lo son el uso de estándares de seguridad, políticas internas, legislación informática, respaldos, planes de contingencia, servicios de seguridad recomendaciones de instituciones como ISO, SANS, NIST, entre otras, todo esto ayuda a reducir riesgos.

## Hipótesis

La fuga de información es la consecuencia de la falta de cultura del personal, ocasionando vulnerabilidad para las empresas, el tener un modelo de prevención de fuga de información en PC’s y Laptops, las empresas minimizarán los riesgos e incidentes de fuga de información.

## Objetivo General

Diseñar e implementar un esquema de seguridad de Prevención de Fuga de Información

## Objetivos Específicos

– Realizar un análisis de riesgos que permita priorizar necesidades de seguridad.

– Estudiar diferentes propuestas para ofrecer seguridad, tanto a nivel red, transporte y aplicación.

– Elaborar un estudio de la infraestructura de red con la que cuenta actualmente la dependencia, para determinar el esquema que permita administrar, auditar e identificar información relevante en los segmentos de red.

– Diseñar un esquema de seguridad para la dependencia, que permita minimizar los riesgos contra la perdida de información (confidencial).

Realizar la implementación, el despliegue de políticas y la puesta en operación del esquema de seguridad propuesto para la dependencia, así como el proceso de concientización de la implementación.

## Caso de Uso

Empresa de servicio, que se denominará Organización**,** dentro de ésta se tiene control de la red como en servicios de control de acceso, monitoreo, implementación de políticas, procedimientos, inventarios de los equipos, prevención, auditorias, detección y respuesta a incidentes que se encuentren en la red.

## Variables

### 1. Independientes

La formación del personal respecto a información confidencial.

### 2. Dependientes

Medidas que se tienen para prevención y corrección de incidentes.

## Problemas a resolver

El área respectiva planteo los siguientes problemas a resolver:

ISSN 2523-6776

– Realización de un primer análisis de riesgos para la dependencia.

– Implementación en su conjunto de reglas de un primer esquema de seguridad para la dependencia.

– Implementación de controles, que permitan identificar y solucionar problemas en la red de manera clara y precisa.

– Desarrollo de políticas de uso de la información para la dependencia.

– Reducir los incidentes de seguridad relacionados con fugas de información lógicas, así como físicas.

Que este estudio sea una base para realizar una implementación de esquema de seguridad para demás organizaciones.

## Fundamento Teórico

### 1. Introducción a la seguridad de la información

La seguridad de TI es un método de defensa de red, que se basa en el establecimiento de recursos de seguridad local de la red y a diferentes niveles, permitiendo definir niveles de confianza, el acceso de usuarios internos o externos a determinados servicios, y denegando cualquier tipo de acceso a otros.

El término Seguridad de la Información cuenta con diversas definiciones, para términos de este proyecto y de forma general, la seguridad de la información, se define como una condición que resulta del establecimiento de medidas técnicas, organizativas y legales para mantener la protección de los activos de información dentro de una organización para continuar con la misión y funciones criticas de su negocio a pesar de los riesgos y vulnerabilidades que se puedan llegar a presentarse por las amenazas. Comúnmente las palabras “vulnerabilidad”, “amenaza”, “exposición” y “riesgo” son usadas de la misma forma, aun sabiendo que tienen significados diferentes. Es importante entender las diferencias de cada concepto, a continuación se presentan las definiciones adoptadas dentro del desarrollo del proyecto.

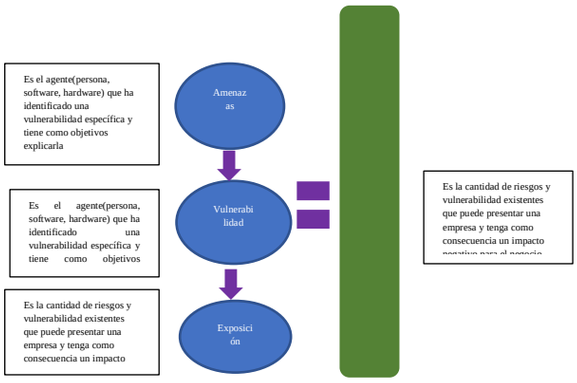


**Figura 1** Definiciones

### 1.1 ¿Qué es DLP?

En los primeros años de la informática, los incidentes de fuga de información solo se relacionaban con el acceso no autorizado provocado por orígenes externos, es decir, personas que no pertenecían, ni formaban parte de una empresa, tenían la intención de ingresar a sistemas no propios, con el objetivo de extraer información para su beneficio, por lo que surge en el mercado por los años 2006 el aplicativo DLP, frente a la necesidad que presentan las organizaciones de proteger la información sensible de fuga de datos.

El termino DLP (Data Loss Prevention), cuyo significado en español es Prevención de perdida de datos, se encarga de identificar y proteger los datos dentro de su red, nos ayuda a comprender como se accede, como se transmiten y si contienen información confidencial.

Es un término que se emplea en el área de seguridad de la información, haciendo referencia a los sistemas que identifican, supervisan y protegen los datos que se procesan, transmiten o almacenan. Los sistemas están diseñados para detectar y prevenir el uso autorizado y la transmisión de información privada, sensible y confidencial, principalmente acorde a la clasificación de la información de cada entidad.

ISSN 2523-6776


**Figura 1** Esquema DLP

## 1.2 Función de DLP

Según el consultor Prathaben Kanagasingham "La función de un DLP es la de identificar, monitorear, detectar e intentar prevenir la fuga de información, considerando como confidencial o sensitiva por la organización. Por lo general esto se lleva a cabo a través de herramientas que cuentan con una gestión centralizada y permiten el monitoreo y control de los datos en el puesto de trabajo" [i].
La función principal de los DLP es proteger los datos de la organización que se pueden encontrar como:

– Datos en Uso: son los datos que se están utilizando en ese momento como, estados financieros, roles de pago, creación de un documento. Las acciones que llevan a cabo los usuarios en los endpoints, tales como copiar datos y archivos en medios extraíbles, imprimir archivos en una impresora local y realizar capturas de pantalla.

– Datos en Movimiento: Son aquellos datos que son transmitidos en una red. Estos datos son particularmente vulnerables, ya que los atacantes no necesitan estar cerca de la computadora donde estos datos están almacenados; solo requieren estar ubicados en algún punto de la ruta de recorrido de los mismos.

– Datos en Reposo: Son los datos que la organización que residen en los repositorios, las bases de datos y los recursos compartidos así como en los discos duros, CD's, memorias USB o cualquier otro medio de almacenamiento.

## 1.3 Características de DLP

Como ya se mencionó anteriormente el DLP ayuda a las organizaciones a que tengan mejor control y manejo de sus datos, además de proteger los datos sensibles. Como nos mencionan el artículo "Understanding and Selecting a DLP (Mogull, 2016)" [ii], describe varían de sus características, de las cuales las más destacadas son:

– Profundo análisis de contenido: DLP tiene la capacidad de analizar a profundidad el contenido empleando diferentes técnicas dependiendo en donde se encuentre la información.

– Gestión de políticas centrales: Las soluciones DLP incluyen un servidor que permite una gestión central y así permite administrar los puntos de detección, creación así como la gestión de las políticas implementadas.

– Amplia cobertura de contenido a través de múltiples plataformas y locaciones.

## 1.4 Prevención de Fuga de Información

Actualmente, llamamos Fuga de Información al incidente en el que un activo de información con valor para una organización, pasa a manos ajenas, perdiendo una de sus cualidades como lo es su confidencialidad. De igual forma puede ser un incidente tanto interno como externo, y a la vez intencional o no.

Debemos de conocer que la fuga de información es una salida no controlada de la información, ocasionando que ésta llegue a mano de personas no autorizadas o que el dueño de la información pierda el control de la misma. En muchos casos ocurre cuando un sistema de información que está diseñado para restringir el acceso solo a personas autorizadas, revela parte de la información debido a errores de los procedimientos del diseño o concepción del sistema.

ISSN 2523-6776

Algunos ejemplos de fuga de información pueden ser desde un empleado vendiendo información confidencial a la competencia (incidente interno o intencional), una secretaria que pierde un documento en un lugar público (incidente interno o intencional) o bajo el mismo entorno la perdida de una laptop o equipo de cómputo, así como también el acceso externo a una base de datos en la organización o un equipo infectado con un software malicioso que envié información a un delincuente.

Cuando nos referimos a incidentes de origen interno, el empleado se ha convertido en uno de los principales factores al cual se debe de enfocar, debido a que el descontento, la venganza, el daño a la imagen, la venta de información altamente valiosa de una empresa para la obtención de un beneficio propio o la creación de una nueva empresa con parte de los activos de información de otra, son algunos de los motivos por los cuales se producen incidentes de fuga de información interna.

Sin embargo, no todos los incidentes de este tipo tienen una motivación específica, en ocasiones, estos incidentes se presentan debido a la falta de conocimiento, formación o simplemente errores humanos en el tratamiento y uso de la información.

## Metodología

"La Prevención de Fuga de Información tiene como objetivo principal: identificar, monitorizar, detectar y prevenir la fuga de información, que es considerada como confidencial por las organizaciones"[iii]. Siendo administrado desde una consola central donde se tiene las capacidades de detectar y prevenir uso no autorizado así como transmisión de información confidencial.

Si observamos lo mencionado anteriormente a través de los datos estadísticos (ilustración 3), podemos decir que de acuerdo a encuestas realizadas por la Agencia NetIQ perteneciente a Micro Focus International, en el año 2016 sobre amenazas internas, un tercio de las organizaciones encuestadas saben que han experimentado ataques internos. De igual forma, tres cuartas partes de los encuestados reconocen estar preocupados por la amenaza que suponen empleados maliciosos o negligentes en lo que respecta a la protección de su información confidencial.

Por otro lado, desde el punto de vista externo, la cantidad de incidentes se ha incrementado de manera exponencial debido a la aparición de: organizaciones criminales, hacktivistas, terroristas, delincuentes cibernéticos, entre otros, los cuales han desarrollado estrategias de ataques avanzadas con el objetivo de obtener un beneficio económico, así como llevar a cabo actividades de sabotaje y provocar daños a la imagen de las organizacionales. De acuerdo a un estudio patrocinado por la firma de McAfee en el año 2015, el impacto económico a nivel mundial provocado por delincuencia cibernética es de aproximadamente 400 millones de dólares al año.

## Causas de Fuga de Información

La naturaleza de los problemas relacionados a fuga de información radica primordialmente en tres aspectos principales relacionados con los ámbitos tecnológicos, personales y organizativos; que al presentarse facilitan y ayudan a la materialización de un incidente de seguridad, esta clasificación obedece a un aspecto fundamental de la información, que es su medio de propagación (sistemas o personas dentro de una organización).

Hoy en día las organizaciones usan dispositivos inalámbricos como: celulares, tabletas, laptops como herramientas de trabajo, los cuales están sincronizados con su correo electrónico, manejan pedidos, poseen cartera de clientes, agenda de contactos, etc. Si bien estas herramientas facilitan a los empleados en sus actividades, representan una gran posibilidad que existan una pérdida de confidencialidad.

Otro factor importante es que con estos dispositivos pueden manejar diferentes conexiones como: Wireless, Bluetooth y si éstas no poseen procedimientos o mecanismos para proteger la información, existe riesgo de que la información que maneje esté comprometida, ya que muchas veces las personas utilizan sus dispositivos en lugares públicos sin considerar que pueden ser víctimas de robo de información. Un artículo de Cardozo González & García Severiche publicado en 2013, menciona que existen diferentes amenazas y vulnerabilidades que pueden llevar a que exista una pérdida de datos, como por ejemplo:

ISSN 2523-6776

– Redes sociales: Representan un riesgo en la confidencialidad de la información, así que las organizaciones deben realizar campañas de sensibilización para que eviten que los empleados publiquen información de la compañía en redes sociales.

– Publicación de videos: Existen actividades que se realizan al interior de las organizaciones que son grabadas, y muchas veces son subidas a páginas sin tener en cuenta la información que en ellas estén, lo que puede poner en evidencia información que solo es relevante para la compañía.

Falta o inadecuada clasificación de archivos de información: La mayoría de las organizaciones no poseen una adecuada clasificación de activos de información, provocando que los empleados no tengan claro el nivel de protección de cada activo, de esta manera dificulta la protección de éstos.

**Controles de seguridad**

Se debe clasificar la información de acuerdo a su importancia para la organización y se deben establecer las medidas de seguridad adecuadas para su tratamiento, a lo largo de su vida útil y en cualquiera de sus formatos, manteniendo los niveles de protección requeridos. La Normativa Global de Seguridad, establece los objetivos de control (OC) necesarios para alcanzar un nivel de seguridad homogéneo y adecuado a las necesidades del negocio.

**Clasificación y Tratamiento de la Información**

La información se clasifica para indicar la necesidad, la prioridad y el grado, de protección aplicable. Se han definido cuatro niveles de clasificación de la información.

– Pública: Información cuya divulgación no afecte a la empresa en términos de pérdida de imagen y/o económica.

– Uso Interno: Información que, sin ser reservada ni restringida, debe mantenerse en el ámbito interno de la empresa y no debe estar disponible externamente, excepto a terceras partes involucradas, previo compromiso de confidencialidad y conocimiento del Propietario de la misma.

– Registrada: Información sensible, interna de áreas de proyectos a los que solo debe tener acceso controlado un departamento, miembros del proyecto, un comité, etc. pero no toda la empresa. Debe ser protegida por su impacto en los intereses de la empresa, de sus clientes o asociados y empleados.

– Reservada: Información de alta sensibilidad que debe ser protegida por su relevancia sobre decisiones estratégicas, impacto financiero, oportunidades de negocio, potencial de fraude o requisitos legales. Su manejo requiere autorización nominativa y su distribución se limitará a un grupo reducido de personas.

Se deben evitar tanto la sobre clasificación como las posibles revelaciones no controladas.

**Etiquetado de la Información**

La aplicación de la clasificación o etiquetado de la información debe realizarse por su propietario, que será el responsable de mantenerla actualizada a lo largo de su ciclo de vida.

Adicionalmente, se considerar como información reservada de cada empleado, sus claves / tokens / identificadores de accesos a los sistemas y los emplazamientos, ya que estos son personales e intransferibles: su información financiera o sobre salud.

**Tratamiento de la Información**

El tratamiento de la información supone que solo esté disponible para aquellos trabajadores que lo necesiten, y que, de ser necesario, tengan autorización para ello.

ISSN 2523-6776

Se definen directrices para el tratamiento de la información según su clasificación en confidencialidad, en lo que respecta a un inventario, etiquetado, acceso, almacenamiento, reproducción, distribución y destrucción. Se debe realiza un checklist para la clasificación de la información tanto para la de carácter pública, exclusiva y almacenada ver tabla 1.

| | |
|---|---|
| **Inventario** | No necesita ser inventariada. |
| **Etiquetado** | |
| **Acceso** | |
| **Almacenamiento** | |
| **Reproducción** | |
| **Distribución** | |
| **Destrucción** | |

**Tabla 1** Información Pública, Exclusiva y Almacenada

## Información que contiene datos de carácter personal

La información debe ser trata bajo los principios de legislación en materia de protección de datos vigentes en cada país en el que opera, y la normativa de la organización

## Responsable de Protección de Datos

– En materia de protección de datos, las empresas, se regiren conforme resulte de las previsiones de las leyes de los países en los que operan, así como a la política de privacidad de la empresa, y al resto de normativa interna aprobada en dicha materia.

– Cada unidad de negocio cuenta con un responsable local de protección de datos, que se encargará de velar por el cumplimiento de la normativa nacional e internacional en materia de privacidad, así como de la política de privacidad de la organización y cualquier normativa relacionada.

– El responsable de protección de datos se encarga de comunicar, según los medios establecidos por la legislación vigente, las posibles incidencias en el tratamiento de datos de carácter personal, tanto a las autoridades designadas como a los usuarios afectados.

## Personal dedicado a la Protección de Datos

Cada unidad de negocio debe asegurar que las funciones propias de protección de datos se desempeñan en su organización (a través de distintas unidades en diversas áreas, entre otras Servicios Jurídicos, Cumplimiento, Seguridad, etc.), por lo que deberá dotar cuantos medios humanos, materiales, tecnológicos y presupuestarios devengan necesarios para su cumplimiento.

Estas funciones incluyen, a título numerativo, pero sin resultar excluyente:

– Asegurar el cumplimiento de las obligaciones en materia de protección de datos derivadas de la legislación vigente que resulte de aplicación, de la política de privacidad de la empresa, de la normativa global de seguridad y del resto de normativa interna.
– Asegurar la adecuada atención de las peticiones relativas a datos de carácter personal recibidas en la unidad de negocio, por ejemplo, peticiones de ejercicio de derechos por los afectados.
– Elaborar y mantener actualizado el listado de tratamiento o ficheros que incluyen datos de carácter personal, según la legislación vigente.
– Velar por la actualización del listado de personal con acceso a tratamiento de datos o ficheros de carácter personal, responsabilidad del propietario de dicha información.
– Asegurar a correcta aplicación de las medidas de seguridad aplicables a los datos de carácter personal, según la legislación vigente.
– Asegurar la formación y concienciación en privacidad de todo el personal de la unidad de negocio, así como de los diferentes colaboradores / personal externo que maneje información de la compañía.

## Despliegue Servicio DLP

En la siguiente sección se muestran todos los detalles relacionados a la implementación inicial:

ISSN 2523-6776

– Data Loss Prevention (DLP)

Estas soluciones son implementadas de manera satisfactoria en la red de la organización, permitiendo incrementar considerablemente los niveles de seguridad, así como mejorar la administración y respuesta frente a incidentes gracias al traspaso de conocimiento experto entregado a los administradores y personal de soporte.

**Implementación DLP**

La implementación de la solución DLP monitorea la información sensible o critica que los usuarios finales pudieran enviar fuera de la red corporativa, por medio de extraíbles, correo, web, esta solución también ayuda a un administrador de red a controlar que datos.

Se generan unas tablas para tener una descripción puntual del servidor PO y el servidor de Base de Datos., como se observa en la tabla 2.

| **Características Servidor** | |
|---|---|
| | Detalles |
| Nombre | |
| Sistema Operativo | |
| Memoria | |
| Procesador | |
| Storage | |
| Dirección IP | |
| Máscara | |
| Gateway | |
| Servidores DNS | |
| Plataforma Virtual | |
| Nodos Gestionados | |
| Antimalware Local | |

**Tabla 2** Tabla descriptiva de los diferentes Servidores

**Actividades DLP**

La implementación de la solución DLP se realiza acorde a las metodologías y buenas prácticas establecidas por Intel Security Professional Services.

Proceso de Implementación

Actividades PO:

– Respaldo de Base de Datos.
– Depuración de eventos de amenazas.
– Depuración de eventos cliente.
– Generación de punto de restauración.
– Actualización de versión de consola.

Instalación y Configuración Inicial:

– Instalación del Módulo DLP en la consola de administración ePO.
– Instalación de Extensiones para DLP.

Definición de Políticas y Configuraciones de Seguridad:

– Se generaron 4 políticas de protección para monitorear las actividades de los usuarios con información sensible.
– Política Big Box.
– Política Big Data.
– Política Datos Personales.
– Política Test TI.

Pruebas de Correcto Funcionamiento:

Se validaron las políticas creadas para cada tecnología con usuarios finales. Se realiza un respaldo de la base de datos, y se genera un snapshot de la consola, esta tarea se recomienda realizarla una vez cada 3 meses dependiendo de los cambios que se apliquen durante este lapso de tiempo, como también es recomendable mover los archivos generados a una unidad de respaldo, por mayor seguridad, ya que este respaldo se guarda en el servidor local.

**Consola PO -Purchase Order**

| **Versión de Solución** | **Nodos cubiertos** | **Porcentaje de Cobertura** |
|---|---|---|
| 11.0.400 | 7 | 0.5% |

**Tabla 3** Versiones instaladas

Se valida que la versión instalada en la consola PO. Se actualiza la consola a una nueva versión, para su mejor funcionamiento y compatibilidad con el módulo de DLP a utilizar.

**Activación de Eventos en Base de Datos**

Se valida que se tengan demasiados eventos de amenazas y eventos de clientes almacenados en la base datos.

Se aplica una depuración de eventos para liberar espacio en la base de datos.

ISSN 2523-6776

Se instala el Módulo DLP con sus extensiones correspondientes

**DLP Políticas:**

Se generan 3 política de prueba:

– Organización_Test_Big_Box;

Con las siguientes reglas cada una:

– Almcenamiento_extraible_Organización
– Capturas_pantalla_ Organización;
– Impresión_ Organización;
– Nube_ Organización;
– Portapapeles_ Organización
– Organización _Correo;
– Web_ Organización

**Resultados**

**Resultados cuantitativos**

La implementación de DLP concluyó satisfactoriamente, otorgando a la organización una avanzada plataforma de:

Protección de Información Sensible en la red.

Reportes de Cobertura

Reportes de actividad y detecciones de las soluciones DLP.


**Gráfico 1** Tipos de incidentes principales

Se logró obtener el top 10 incidentes con mayor detección, como podemos ver en la siguiente imagen nos muestra el número de veces que han tomado información sensible y por qué medio, al igual nos muestra las veces que han ingresado alguna USB.

Usuarios con mayor infracciones, como podemos ver en la siguiente imagen, es el top 10 de usuarios que han tratado de obtener información sensible, por medio de portapapeles, por alguna aplicación en la nube, por captura de pantalla, por correo, por una página web, por algún medio de impresión, o bien ingresado alguna USB.

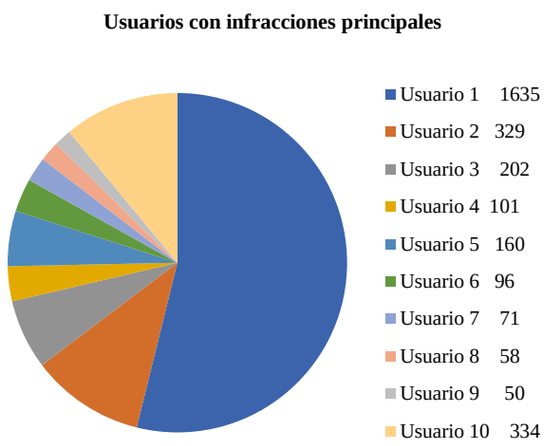


**Gráfico 2** Usuarios con infracciones principales

**Resultados cualitativos**

– PO.
Actualización de versión.
Depuración de eventos

– DLP.

Se encuentra en óptimas condiciones de funcionamiento, y óptima para activación de políticas de bloqueo, brindando visibilidad y almacenamiento de eventos de extracción de información sensible, sin contratiempos ni problemas conocidos a la fecha de finalización de los trabajos de configuración base inicial
Configuración de políticas de monitoreo para validar que usuarios y que información sensible es extraída y por qué medio, llámese USB, correo, captura de pantalla, web (URL's), nube (Box, Dropbox, Google Drive, iCloud, Office 365, One Drive, Syncplicity), impresión, portapapeles.

ISSN 2523-6776

– Configuración de tarea de instalación de Agente DLP.
– Configuración de Clasificaciones de información por medio de directorios, aplicaciones de base de datos como (Squirrel, Oracle SQL Developer), y páginas web específicas

## Conclusiones

Con el desarrollo de este trabajo de investigación se denota la importancia que tiene la protección y prevención de fuga de información en cualquier organización, y que existen herramientas que nos pueden ayudar a conseguir este objetivo**.**

Se logra desarrollar una guía de implementación estándar que pueda ser aplicada en cualquier organización.

Podemos decir que la solución DLP implementada está estable y en proceso de activación de bloqueo, permitiendo a la organización tener un control de fugas de información, detectarlas y minimizarlas.

## Referencias

Anaya Solano, D. A., & Ojeda Field, L. F. (2020). Elaboración del prototipo de un sistema de control de variables atmosféricas automatizado para el cultivo de plantas bajo invernadero en ambiente indoor en la Región Caribe (Doctoral dissertation, Universidad de la Costa).

Calvo, Arantxa. (2016, 03, 11). Fuga de información, la mayor amenaza para la reputación corporativa. Disponible: http://www.redseguridad.com/opinion/articulos/fuga-de-informacion-la-mayor-amenaza-para-la-reputacion-corporativa/

C. (2020). Diseño e implementación de un sistema automático de suministro trifásico permanente y optimización del consumo energético para la Avícola “Flor María”.

Guía de Seguridad y Mejores Prácticas, Centro de Seguridad de la Información, recuperado 31 de Marzo 2016 de: https://benchmarks.cisecurity.org

HUANCA, T., & EDDY, A. (2020). MONITOREO Y DIAGNÓSTICO DE LA OPERACIÓN DE UNA COLUMNA DE FLOTACIÓN PILOTO USANDO MÉTODOS DE PROYECCIÓN (PCA).

Kanagasingham, P. (Agosto 2015). Sans Institute. Obtenido de: http://www.sans.org/reading-room/whitepapers/dlp/data-loss-preventio-32883

La Scala, M. (2020). De las redes inteligentes a las ciudades inteligentes. ISTE Group.

McAfee. (2016, 03, 11). McAfee data loss prevention la solución de prevención contra la pérdida de datos líder del mercado. Disponible: https://www.mcafee.com/enterprise/es-mx/products/dlp-endpoint.html

Miguel Pérez Julio Cesar. (2015), Protección de Datos y Seguridad de la Información. México: Ra-Ma Araya Álvarez, R., & Merizalde Dobles, J. G. (2020). Informe técnico: Pruebas a escala piloto en el Sistema de Potabilización La Guaria, Valle de La Estrella, Limón. – Cazco Barba, L.

Mogull, R. (Diciembre 2016). Searchdatacenter. Obtenido de: http://searchdatacenter.techtarget.com/es/consejo/Como-evitar-errores-de-implementacion-de-DLP

Security Murugiah Souppaya Karen Scarfone, recuperado 05 de Septiembre 2016 de: http://dx.doi.org/10.6082/NIST.SP.800-46r2

ISSN 2523-6776