DISEÑO E IMPLEMENTACIÓN DEL PROYECTO DE DLP (DATA LOSS PREVENTION), PARA LAS DIRECCIONES (DIRECCIÓN ADMINISTRATIVA, DIRECCIÓN FINANZAS, DIRECCIÓN DE PLANEACIÓN Y PRESUPUESTACIÓN Y SECRETARIA DE GABINETE) DEL MINISTERIO DE DEFENSA NACIONAL.

DEIBY ALEJANDRO ALVARADO AVENDAÑO

INSTITUCION UNIVERSITARIA POLITÉCNICO GRANCOLOMBIANO

FACULTAD DE INGENIERÍA Y CIENCIAS BASICAS

INGENIERIA EN TELECOMUNICACIONES

BOGOTA

2016

DISEÑO E IMPLEMENTACIÓN DEL PROYECTO DE DLP (DATA LOSS PREVENTION), PARA LAS DIRECCIONES (DIRECCIÓN ADMINISTRATIVA, DIRECCIÓN FINANZAS, DIRECCIÓN DE PLANEACIÓN Y PRESUPUESTACIÓN Y SECRETARIA DE GABINETE) DEL MINISTERIO DE DEFENSA NACIONAL.

DEIBY ALEJANDRO ALVARADO AVENDAÑO

Proyecto presentado como requisito para obtener el titulo de Ingeniero en Telecomunicaciones

Wilmar Jaimes Fernández

Asesor

INSTITUCION UNIVERSITARIA POLITÉCNICO GRANCOLOMBIANO

FACULTAD DE INGENIERÍA Y CIENCIAS BASICAS

INGENIERIA EN TELECOMUNICACIONES

BOGOTA

2016

CONTENIDO

LISTA DE TABLAS

1. JUSTIFICACIÓN

La seguridad de la información, ha venido teniendo un nivel de atención elevado puesto que el manejo de la información personal y de las organizaciones es de vital importancia tenerla resguardada, para esto se han implementado herramientas de seguridad de la información que nos ayudan ejercer controles en el uso de esta misma.

Teniendo en cuenta el área de la seguridad de la información en el Ministerio de Defensa, es de gran importancia aplicar estos controles debido a que tiene como objetivo la protección de la información, divulgación o destrucción no autorizada de la información sensible, con el fin de mitigar estos riesgos y no generar un impacto negativo donde afecte su planeación estratégica.

Para aplicar estos controles tendremos en cuenta el levantamiento de información y los controles que el funcionario crea conveniente para ejercer la protección sobre esta información.

La universidad podrá utilizar la información consignada en este documento para la posterior consulta sobre DLP.

Para el proceso de formación académica el Politécnico Grancolombiano aporta a la práctica empresarial los conceptos básicos teóricos y prácticos suficientes para poder configurar y verificar el estado de la plataforma de DLP, clasificación de información de forma clara y que como profesional pueda transmitir la información a otras personas con la finalidad de que ellos puedan hacer esto sin causar ningún traumatismo teniendo en cuenta su integridad, confidencialidad y disponibilidad.

2. INTRODUCCION

La seguridad de la información se puede definir como un conjunto de medidas técnicas, organizativas y legales que permiten a cualquier organización asegurar la confidencialidad, integridad y disponibilidad del sistema de información.

Debido a la problemática que acarrea el almacenamiento, transporte, acceso y procesado de la información, el presente trabajo muestra la implementación de cómo prevenir la fuga de información marcada como confidencial en el Ministerio de Defensa Nacional en cinco dependencias Administrativa, Dirección Finanzas, Dirección de planeación y presupuestación y Secretaria de Gabinete sin poner en riesgo al personaje que la manipula o al funcionario propiamente dicho.

La metodología que se usa para el desarrollo de este trabajo está enmarcada en 3 grandes fases las cuales son: Levantamiento de la información, Activación de pruebas y una producción.

En la fase de levantamiento de información se realiza en cada de las direcciones, se alistan los recursos Hardware y Software. Posteriormente se crean políticas para implementar en la plataforma de seguridad.

En la fase de pruebas donde los resultados obtenidos se comparan con los resultados esperados con el fin de localizar fallos en la implementación de controles en las políticas de seguridad.

En la fase de producción se realizarán los debidos análisis a los casos presentados en la plataforma para determinar si hay una posible fuga de información o si es un falso positivo, teniendo en cuenta los casos fortuitos de cada dependencia se estudiarán la viabilidad de realizar una regla de omisión.

3. OBJETIVO GENERAL

Garantizar por medio de herramientas de seguridad informática, el correcto uso de la información sensible con la que cuenta actualmente el Ministerio de Defensa Nacional para sus direcciones (Dirección Administrativa, Dirección Finanzas, Dirección de Planeación y Presupuestación y Secretaria de Gabinete), Implementando la metodología desarrollada por la organización mencionada anteriormente, que se encuentra divida en tres grandes fases (Levantamiento de Información, Pruebas y Producción), esto se desarrolla con el fin de salvaguardar la confidencialidad, integridad y disponibilidad de la información.

3.1 OBJETIVOS ESPECÍFICOS

- Documentar toda la información requerida para la debida implementación de los controles en la herramienta de seguridad.
- Verificar la configuración de los appliances para el correcto uso de análisis de datos y transferencia de esta información.
- Verificar instalación y versión de los agentes en el cliente final de cada una de las dependencias pertenecientes al proyecto de DLP.
- Elaborar y afianzar las políticas de seguridad construidas en la herramienta de DLP, para mitigar la fuga de información y reducir la cantidad de incidentes generados en la plataforma de DLP.
- Cumplir con los tres pilares de la seguridad de la información, como lo son confidencialidad, integridad y disponibilidad de los datos marcados como sensibles y apoyarnos en herramientas extras de otras áreas de IT.

4. MARCO REFERENCIAL

La seguridad de la información es un tema que demanda la mayor atención en cualquier organización, la protección de los datos que maneja cada una, bien sea propios, clientes, proveedores, personas naturales o jurídicas entre otras. [1]

En cuanto a las organizaciones, éstas requieren que los tres pilares encargados de salvaguardar dichos datos a saber, confidencialidad, disponibilidad e integridad, sean bien gestionados para mitigar posibles vulnerabilidades que tenga la entidad. [2]

No obstante lo que más impacta en la perdida de datos sensibles para la organización entre la parte tecnológica y humana, es esta última donde se presentan las mayores vulnerabilidades en seguridad de la información. [1][5]

Según el fabricante Symantec, quien comercializa soluciones de seguridad basadas en el concepto de DLP[1], este concepto se enfoca en detectar un entorno en el cual se está fugando la información, por ejemplo: correo electrónico, almacenamiento en la nube, medios removibles y adicional a esto cómo mueven estos datos dentro de la red LAN de la organización. [4]

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. [3]

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

[1] DLP (DATA LOSS PREVENTION) el cual traducido al español significa "prevención de la fuga de datos" ha tenido una cantidad de acrónimos importantes como: IPC (Información, protección y Control), CMF (control de Contenidos y filtrado) entre otros, todas estas se resguardan y se utilizará el acrónimo universal que sería DLP. [6]

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 al Ministerio de Defensa Nacional y sus respectivas Fuerzas.

Estas necesidades se identificaron claramente por la Oficina Asesora de Sistemas del Ministerio de Defensa Nacional. Como resultado de esta identificación se propuso la implementación de un proyecto DLP que mitigue riesgos de pérdida de información de la institución. En particular el proyecto del que es objeto este documento, implementarán políticas para controlar el tipo de información que maneja actualmente el core de negocio de la dependencia en la cual se iniciara el proyecto de DLP.

Para dar inicio al proyecto se requiere la presentación ante la directora de la dependencia, una vez la directora apruebe este proyecto se procederá a darle una charla de sensibilización a los funcionarios pertenecientes a esta dependencia, posteriormente se procede a realizar mesas de trabajo en la cuales se ayuda a la correcta clasificación de la información, una vez se haya clasificado de forma correcta la información se procederá a realizar las controles para mitigar la fuga de información.

Para los controles de la información se puede restringir el almacenamiento en dispositivos USB, controlar las impresiones de documentos marcados como confidenciales, controlar el envió de correos con información confidencial a dominios externos al Ministerio de Defensa como Hotmail, Gmail entre otros, adicional a esto podemos controlar las acciones dentro de las aplicaciones como copiar y pegar texto, también podemos controlar el envió de estos documentos dentro de la red LAN.

Las fuentes que utilizaremos para la elaboración de este proyecto estarán relacionadas con documentación que tenga el Ministerio de Defensa Nacional, Normas ISO 27001:2013, modelos de implementación de DLP y artículos de investigación.

5. METODÓLOGIA DE IMPLEMENTACION.

Para el desarrollo de la práctica empresarial, se tuvo en cuenta la metodología que ya tiene avalada el Ministerio De Defensa Nacional para así cumplir con nuestras actividades y cronograma estipulado con éxito.

El proyecto de Prevención de fuga de la información, esta constituido en tres fases las cuales son: Levantamiento de Información, pruebas y puesta en producción. A continuación se explicaran las actividades y la metodología implementada en cada una de estas fases mencionadas anteriormente.

En la primera fase (Levantamiento de Información), se tienen 3 actividades las cuales son: Levantamiento de información del CORE de negocio de la dependencia a implementar el proyecto, Alistamiento de Hardware y Software para el correcto tratamiento de la información y por último la creación de políticas en la plataforma de DLP.

Para la ejecución de estas actividades se desarrolló la siguiente metodología, las cuales se relacionan en la siguiente tabla.

Tabla 1. Metodología fase 1 (Levantamiento de información).

Actividad	Metodología
Levantamiento de información del CORE de negocio de la dependencia	- Reunión y aprobación con la Directora de la dependencia en la cual se va a implementar el proyecto de DLP.
	- Mesas de trabajo con los coordinadores o líderes de área, para realizar la correcta clasificación de la información.
	- Levantamiento de actas en la cual se dejan los acuerdos, pendientes y observaciones.
Alistamiento de Hardware y software para el tratamiento de información	- Revisar configuración en los appliance.
	- Verificar que el agente se encuentre instalado y actualizado en la estación de trabajo
	- Coordinar permisos en los recursos compartidos.

Creación de Políticas en la Plataforma	- Determinar los controles que se quieran ejercer sobre la información marcada como confidencial.
	Se utiliza la plataforma de DLP para la creación de Políticas.

Fuente: Autores.

En la segunda fase (Pruebas), se tienen 2 actividades las cuales son: Fase de pruebas de DLP y monitoreo de reglas. Para la ejecución de estas actividades se desarrolló la siguiente metodología, las cuales se muestran en la siguiente tabla.

Tabla 2. Metodología fase 2 (Pruebas).

Actividad	Metodología
Pruebas DLP	- Auditar políticas creadas, con el fin de no generar traumatismos a la hora de lanzarlas a producción.
Monitoreo de Reglas	- Revisión de los incidentes generados en la plataforma de DLP.
	- Determinar si es una posible fuga de información.
	Si: se le informa al dueño de la información
	No: Monitorear incidentes del usuario.

Fuente: Autores.

En la tercera fase (Producción), se tienen 2 actividades las cuales son: Puesta en producción y afinamiento de políticas y Reuniones de Seguimiento. Para la ejecución de estas actividades se desarrolló la siguiente metodología, las cuales se muestran en la siguiente tabla.

Tabla 3. Metodología fase 3 (Producción).

Actividad	Metodología
Puesta en producción y Afinamiento	- Las políticas que se encuentren en prueba, pasan a ejercer controles configurados.
	- Ajustes a políticas configuradas
Monitoreo de Reglas	- Reunión periódica para dar a conocer el estado en el cual se encuentra el proyecto de DLP a los jefes de dependencia.
	- Levantamiento de actas

Fuente: Autores.

Para lograr el éxito del proyecto en las dependencias (Dirección Administrativa, Dirección Finanzas, Dirección De Planeación Y Presupuestación Y Secretaria De Gabinete), Se hace necesario aplicar paso a paso la metodología mencionada anteriormente sin excluir ninguna actividad propuesta ya que cada una de ellas cumple un objetivo específico en dicho proceso,

En la aplicación de esta metodología se tuvo algunos inconvenientes a la hora de agendar las reuniones con los jefes de las dependencias, pues se debe a que tienen una agenda bastante ocupada y se puede llegar a prolongar el proyecto en un tiempo indeterminado.

6. CRONOGRAMA

Tabla 4. Cronograma de actividad fase 1 (Levantamiento de información).

Fases	Actividad	Mes	Fecha Inicio	Fecha Fin
Fase I (Levantamiento de información)	Levantamiento de Información de CORE de negocio de cada Dirección.	Enero Febrero Marzo	04-ene-16	31-mar-16
	Alistamiento de recursos de Hardware y Software para el tratamiento de información.	Enero	18-ene-16	29-ene-16
	Creación de políticas en la plataforma	Febrero Marzo	08-feb-16	16-mar-16

Fuente: Autor.

Tabla 5. Cronograma de actividad fase 2 (Pruebas).

Fases	Actividad	Mes	Fecha Inicio	Fecha Fin
Fase II (Pruebas) Fase II (Pruebas)	Fase de Pruebas DLP	Febrero Marzo	15-feb-16	16-mar-16
	Monitorio de Reglas DLP	Febrero Marzo Abril	15-feb-16	29-abr-16

Fuente: Autor.

Tabla 6. Cronograma de actividad fase 2 (Puesta en Producción).

Fases	Actividad	Mes	Fecha Inicio	Fecha Fin
FASE III (PRODUCCION)	Puesta en producción y afinamiento de políticas	Abril Mayo	16-mar-16	30-abr-16
	Reunión de seguimiento con jefes de oficina	Febrero Marzo Abril Mayo	15-feb-16	30-abr-16

Fuente: Autor

7. CONCLUSIONES

- Se realizaron reuniones con los jefes de las direcciones a las cuales se les presento el proyecto de DLP y se dejaron actas en donde estipula quien es el encargado de la informacion, las tareas pendientes por parte de la direccion y de la Oficina Asesora de Sistemas y acuerdos entre las dos direcciones.

- Se verifico que la plataforma este funcionando de forma optima para la transferencia de datos, esto se hace con el fin de validar la correcta configracion en la red.

- En cada dependencia en la cual se aplico el proyecto de prevencion de fuga de informacion se verifico cada estacion de trabajo en la busqueda del agente de cliente final actualizada e instalada correctamente.

- Se configuraron las politicas de seguirdad a cada direccion, teniendo encuenta los controles que se querian ejecutar por parte del coordinador acargo de la informacion.

- Se van afianzando las politicas creadas de acuerdo a requerimientos expresos de la alta direccion o del dueño de la informacion, estos solicitud se hace llegar por medio de correo electronico.

- Se garantiza la confidencialidad, integridad y disponibilidad de la informacion con la ayuda de herramientas pertenecientes a otras areas dentro de la Oficina Asesora de Sistemas.

8. REFERENCIAS BIBLIOGRAFICAS

[1] Steffens, Hans. (2011,03,11). Prevencion de fuga de datos (DLP) en 5 sencillos pasos. Disponible: Http://liacolombia.com/2010/09/prevencion-de-fuga-de-datos-dlp-en-5-sencillos-pasos/

[2] Blogfirmae. (2014, 10, 14). Pilares de la seguridad de la información: confidencialidad, integridad y disponibilidad. Disponible: http://blog.firma-e.com/pilares-de-la-seguridad-de-la-informacion-confidencialidad-integridad-y-disponibilidad/

[3] Rouse, Margaret. (2013, 12, 01). Prevención de perdida de datos (DLP). Disponible: http://searchdatacenter.techtarget.com/es/definicion/Prevencion-de-perdida-de-datos-DLP

[4] Symantec. (2016, 03, 11). Symantec data loss prevention la solución de prevención contra la perdida de datos líder del mercado. Disponible: http://www.symantec.com/es/mx/data-loss-prevention/

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

[6] K. Perkins, "Data Loss Protection," pp. 1075–1092, 2013.