MAESTRÍA EN AUDITORIA DE TECNOLOGÍA DE LA INFORMACIÓN

Desarrollo de un modelo de seguridad utilizando herramientas Data Loss Prevention (DLP), en las instituciones de Educación superior (IES). Caso Universidad ECOTEC.

Propuesta de artículo presentado como requisito para la obtención del título:

Magíster en Auditoría de Tecnologías de la Información

Por la estudiante:
Johanna Andrea NAVARRO ESPINOSA

Bajo la dirección de:
Cesar Martín GONZALES ARBAIZA

Universidad Espíritu Santo
Maestría en Auditoría de Tecnología de la Información
Samborondón - Ecuador

Enero del 2017

Desarrollo de un modelo de seguridad utilizando herramientas Data Loss Prevention (DLP), en las Instituciones de Educación Superior (IES). Caso Universidad ECOTEC

Development of a security model using Data Loss Prevention (DLP) tools in higher education institutions (IES). ECOTEC University Case

Johanna Andrea NAVARRO ESPINOSA[1]

Resumen

El presente artículo propone un modelo de seguridad utilizando herramientas DLP, para prevenir la fuga de datos e información interna en las IES, tomando como caso de estudio la Universidad ECOTEC. El modelo de seguridad proporciona una visión integral, de los componentes indispensables, que una organización debe considerar antes de implementar una herramienta DLP, así como los ejes transversales que permiten la sensibilización y concientización de los usuarios y la mejora continua del modelo de seguridad, acorde a los objetivos organizacionales. Finalmente, se realiza una simulación para validar el modelo en la IES, obteniendo como resultados la disminución de la fuga de datos internas, a través de un modelo sistémico que contribuye a las estrategias de seguridad informática favoreciendo la continuidad del negocio.

Palabras clave:	DLP, Prevención de fuga de datos, Clasificación de la información, modelo de seguridad, políticas de seguridad.

Abstract

This article proposes a security model using DLP tools, to prevent leakage of data and internal information in HEIs, taking as a case study the ECOTEC University. The security model provides an integral view of the indispensable components that an organization must consider before implementing a DLP tool, as well as the transversal axes that allow the awareness and awareness of the users and the continuous improvement of the security model, according to To organizational goals. Finally, a simulation is performed to validate the model in the IES, obtaining as results the reduction of the internal data leakage, through a systemic model that contributes to the strategies of computer security favoring the business continuity.

Key words	DLP, Data leak prevention, Classification of information, security model, security policies.

[1] Ingeniera en Sistemas y Telecomunicaciones. Coordinadora de la Unidad de seguimiento a graduados y Docente, de la Universidad ECOTEC.

INTRODUCCIÓN

La seguridad de la información, es un tema que cada día adquiere mayor relevancia a nivel mundial. Las amenazas tanto externas como internas, cada día se incrementan y se diversifican los patrones y frecuencias de ataques, conllevando a que día tras día, se aumente el porcentaje de fuga de información. Las organizaciones conscientes de esta problemática global, se esfuerzan por implementar mejores controles que protejan la información sensible y/o confidencial, utilizando mecanismos orientados a prevenir los canales de fuga (CISCO, 2016).

En aquellas con un nivel de madurez más amplio, se encuentran mecanismos de defensa en profundidad[2], donde cada nivel se instala en función de las amenazas y los bienes a proteger (DCSSI, 2004). Sin embargo, en otras donde no se cuentan con los recursos necesarios que permita poseer un nivel de seguridad adecuado, la información o datos se encuentran expuestos a la fuga o pérdida.

Existen herramientas como los antivirus, que monitorean la infección de virus o malware, cuya una de sus acciones provoca la fuga de información. Por otra parte, existen los DLP que son herramientas (hardware o software), centradas en la seguridad de los datos, siendo efectivas, si se cuentan con los insumos necesarios para su funcionamiento. Algunos analizan el tráfico en la red buscando coincidencia con patrones establecidos, otros inspeccionan en tiempo real la información en las estaciones de trabajo (Moreno, 2009).

El problema, es que las soluciones DLP, no pueden funcionar de manera independiente, es decir, requiere la existencia de una solución sistémica, que integre procesos claros y definidos, e identificación y clasificación de su información para un correcta configuración y funcionamiento de una herramienta DLP, orientado a prevenir o mitigar la fuga de los datos o información interna.

El objetivo de esta investigación, es diseñar un modelo de seguridad integral para la prevención de fuga de datos internos de las IES, utilizando herramientas DLP. Como caso de estudio se tomará la Universidad ECOTEC, donde en base a sus necesidades generales, permitirá sustentar la metodología utilizada y validación modelo, a través de la simulación.

El modelo proporciona una visión integral, de los requerimientos con los que debe contar una organización antes implementar una herramienta DLP, componentes que deberían considerar en la selección de la herramienta, y acciones complementarias después de la implementación. Cabe indicar que, dentro del modelo, no se plantea ni recomienda una herramienta o fabricante especifico.

MARCO TEÓRICO

La seguridad de la información, en las últimas décadas, es un elemento más a considerar dentro de las organizaciones, debido al crecimiento de las tecnologías y de los volúmenes de información (McAfee, 2014). La creciente tendencia hacia lo digital, permite que la información se presente de diversas formas como mensajes de correo electrónico, hojas de cálculo, documentos de texto, archivos de bases de datos, que se transmite por múltiples canales y vías, ampliando la brecha de la seguridad de la información (ISACA, 2010).

Las organizaciones, de acuerdo a su naturaleza y tamaño, implementan mecanismos y controles de seguridad, para proteger la información que consideran es “Confidencial”, y que puede ser de tipo financiera, comercial u operativa (CISCO, 2016).Existen soluciones que operan de manera independiente, como firewall, antivirus, antispam,

[2]Defensa es profundidad, es una defensa global y dinámica, que coordina varias líneas de defensa que cubren toda la profundidad del sistema.

que no son suficientes, debido a la diversificación y potencia de los ataques, lo que genera para las organizaciones un alto costo operativo y administrativo (Flórez , Arboleda , & Cadavid, 2012).

La red nacional de educación e investigación (CEDIA) en Ecuador, realizo una encuesta acerca de la seguridad de la información en las Instituciones de Educación superior (IES), pertenecientes a la red, en la cual se evidencia que el 82% no cuentan con presupuestos asignados para la gestión de seguridad, aunque 36% de la IES si posee un área destinada a tratar los amenazas y riesgos relacionados con la seguridad de la Información, mientras que el 50% de las IES encuestadas, se encuentra en un nivel jerárquico Operativo (CEDIA, 2014). Po lo anterior, se evidencia la falta de sensibilición y compromiso por parte de los empresarios y directivos, para mitigar y reducir los riesgos de la fuga de información desde el interior de la organización (Burgos & Campos , 2008)

De acuerdo con Pacheco (2010), uno de los temas mas discutidos es la fuga de información, que afecta la privacidad y confidencialidad de las organizaciones, y de los cuales en los últimos años se han presentado incidentes de seguridad relevantes como fue el mencionado caso de wikileads (Pacheco, 2011). Las amenazas que afectan la seguridad de la información se distribuyen en distintos niveles de criticidad según sea la orientación y el ámbito de su aplicación (Burgos & Campos , 2008).

De acuerdo con Liu & Kuhn (2010) , la perdida de datos se puede dividir en: Fuga: Cuando los datos sensibles / confidenciales ya no pertenecen a la organización, perdiendo su confidencialidad, y generando otros problemas como el robo de identidad; y la desaparición /daño: en donde la copia correcta de datos, ya no esta disponible para la organización, careciendo, por tanto de integridad y disponibilidad (Liu & Kuhn, 2010).

Según, Cabarique, Salazar, y Quintero (2015), definen la fuga de información, como un incidente que permite que una persona ajena a la organización, tenga acceso a datos que solo deberían conocer el personal autorizado. Por su parte, Pacheco (2011), la define como lo que ocurre cuando algún dato o activo de información que tenga valor para una organización, pasa a manos ajenas, perdiendo la cualidad de confidencialidad que le fue otorgada.

Sin embargo, se han planteado trabajos que buscan solucionar los problemas relacionados a su implementación, aportando metodologías acompañadas de soluciones existentes en el mercado. Acosta (2015), propone la utilización de un Software propietario, donde su solución arranca a partir de la implementación del producto, cubriendo la información requerida. Por su parte, Castrillón y Lezcano (2013), presentan su metodología enfocado al sector financiero, destacando el funcionamiento técnico de los DLP, apoyado en un solución propietaria.

Causas de la fuga de información

Malware

De acuerdo, con la encuesta anual de Cisco (2016), demuestra que una de las mayores amenazas que se relaciona con la fuga de información son los Malware, que opera a través de la infección de navegadores (60%), utilizando sistemas de nombre de dominio (DNS) (91.3%) e iniciando comunicaciones cifradas a través de puertos no autorizados, con el fin de tomar el mando/ control o robar datos (Cisco 2016). Los malware presentan distintas formas y tipos, lo cuales permite acceder a equipos, explotar vulnerabilidades y afectar la privacidad de forma directa (Pacheco, 2011).

Accesos no autorizados

Según, el informe técnico de Cisco (2008), indica que el 39% de los profesionales de TI, se enfrentaron a accesos no autorizados a la red o instalaciones empresariales, siendo los empleados la principal causa. El 46% de incidentes, se dieron con mayor frecuencia en pequeñas y medianas empresas (Cisco, 2008).

Servicios en la nube

El crecimiento desmedido de los servicios ofrecido en la nube, virtualización y las redes sociales, proporcionaron nuevos modelos de comunicación y contribuyeron a ampliar la brecha de seguridad. Estos servicios son utilizados por las organizaciones, empleados, contratistas y clientes, para comunicarse e intercambiar información, además, de ofrecerle a los usuarios propiedades como la movilidad, conectividad, colaboración y almacenamiento, lo que dificulta la labor de los profesionales de TI (Ca Technologies, 2012)

Tecnologías móviles

Su principal funcionalidad es mantener conectada a los usuarios en todo momento y lugar. No obstante, su rápida proliferación y el fácil acceso a software de intercambio de archivos aumentó el riesgo de pérdida o fuga de datos (Websense, 2013). De acuerdo, con el Instituto Nacional de estadísticas y Censos (INEC) (2014), el 16.9% de las personas mayores a 5 años, posee un teléfono inteligente, sobrepasando la cifra registrada en 2011 en un 141%. El estudio refleja también, que el 28% de la población tiene acceso a internet, y el 40% utilizo datos en su celular.

Estas tendencias han sido adoptadas por las organizaciones, donde los empleados llevan sus dispositivos móviles, ipads y portátiles, a sus lugares de trabajo (Cisco, 2008). Exponiendo la información sensible fuera de la organización, a esto sumado, la calidad de las cámaras de los celulares, que cada día incrementa, y hace posible la fuga de información a través de imágenes, audios y archivos, hacia distinta plataformas de servicios en la nube (3M, 2013).

Por otra parte, el fenómeno BYOD (Bring Your Own Device), donde los empleados llevan consigo dispositivos móviles a sus lugares de trabajo, con el fin de dar movilidad a los procesos del negocio, y esto es respaldado por las organizaciones, ya que “estarían” reduciendo sus costos asociados a la adquisición y mantenimiento de equipos. No obstante, es otra preocupación para los directores de TI, ya que deben revisar sus políticas organizaciones, y controles para supervisar y reducir los riesgos asociados (Saro & Férnandez, 2013), (Sánchez, 2002).

Políticas Organizacionales

Las políticas organizacionales, son desarrolladas para orientar o dirigir a los miembros de una organización acerca de sus responsabilidades en cada área, estas pueden ser generales o específicas, como es el caso de las políticas de seguridad (Medina, 2015).

La implementación de Políticas de Seguridad de la Información es un proceso técnico y administrativo que debe abarcar a toda la organización, y debe estar avalado y respaldado por la alta dirección o gerencia (Burgos & Campos , 2008). De acuerdo, con el estudio de Deloitte (2007), distintas compañías de gran tamaño enfrentaron crisis de seguridad de la información, por lo cual, un 69% han fortalecido su infraestructura para prevenir los ataques externos, sin embargo, solo el 56% mostro confianza para enfrentar ataques internos.

La ética y comportamiento organizacional, es un factor fundamental en la reducción de fuga de información interna, como lo menciona el Centro de Investigación de Ética (ERC) (2016) , en la encuesta mundial sobre ética empresarial, donde se investigan los factores que conllevan a empleados realizar acciones que atenten contra las políticas empresariales, debilitando las normas de la organización, los valores éticos, y la integridad en sus lugares de trabajo. A partir del año 2000 se evidencia, la aparición de los problemas de ética vinculados a la fuga de datos.

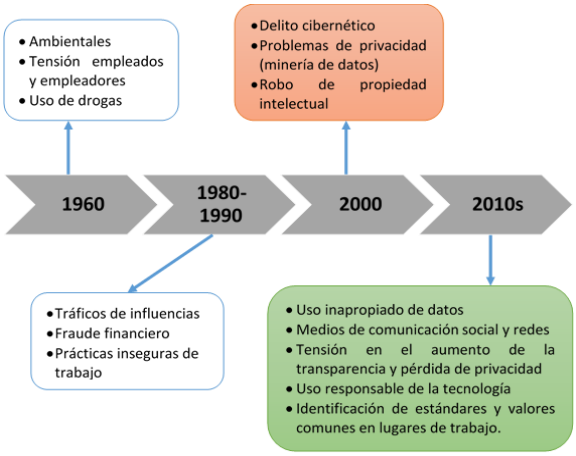


Figura No.1. Línea de tiempo de los problemas éticos.
Elaboración: Autor
Fuente: Ethics and Compliance Iniciative (ECI)

Existen, estandares de seguridad de la información, marcos de referencia y metodologias, que pueden concebirse como un punto de partida para adaptar procedimientos específicos. Su implementación debe ser priorizada ,planificada y enmarcada acorde a las necesidades organizacionales para lograr su uso eficaz (IT Governance Institute, 2008).

Normas y estandares

COBIT

Es un marco de referencia globalmente aceptado para el gobierno de TI. Basado en estándares de la industria y las mejores prácticas. Enfocado en el nivel estrategico, donde los ejecutivos pueden asegurarse de que se ajusta de manera eficaz con los objetivos del negocio y dirigir mejor el uso de TI para obtener ventajas comerciales. COBIT brinda un lenguaje común a los ejecutivos de negocios para comunicar las metas, objetivos y resultados a los profesionales de auditoría, informática y otras disciplinas (IT Governance Institute, 2008).

ISO 27002:2013

El objetivo principal es proporcionar direccionamiento a los responsables de la implementación de seguridad de la información de una organización. Incluye un conjunto de mejores practicas para desarrollar y mantener normas de seguridad y de gestión, ademas de incluir enfoque dirigido a la gestion del riesgo y directrices para su tratamiento (IT Governance Institute, 2008)

ITIL

Enfocado a la gestión de servicios de TI, que incluye la planificación, aprovisionamiento, diseño, implementación, operación, apoyo y mejora de los servicios de TI, alineado a los objetivos organizacionales. ITIL proporciona un marco de trabajo de mejores prácticas integral, consistente y coherente para la gestión de servicios de TI y los procesos relacionados. (IT Governance Institute, 2008)

Data Loss Preventión (DLP)

De acuerdo, con la definición de ISACA (2010), son “mecanismos utilizados detectar y prevenir que la información confidencial se “fugue” hacia afuera de los límites de la organización para un uso no autorizado, lo cual puede ser por medios físicos y/o lógicos”. Por su parte, Pacheco (2011) afirma que:

> “*Todos estos mecanismos tienen como objetivo el monitoreo y control de los datos digitales que circulan en una infraestructura tecnológica, ya sea por medio de filtrado de contenidos web, por aplicación de políticas en el uso de determinados datos previamente identificados como sensibles, o por el bloqueo de la conexión de dispositivos no marcados como confiables*”. *Pág. 5.*

Existen diversos fabricantes que ofrecen servicios DLP, como complemento a otros servicios; por otro lado, existen otros que lo ofrecen como una solución de primer plano que se integra a la infraestructura de TI. Algunos de los retos que enfrentan las soluciones DLP son:

- *Volumen de los datos.* La cantidad de información aumenta en las organizaciones, y su falta de clasificación se percibe como datos

desorganizados y dispersos, lo que dificulta la eficacia de los DLP.

- *Resistencia a las TI*. Parte del funcionamiento de los DLP, es configurar la información que se va a proteger. Al no tener un escenario claro de procesos y flujo de la información, conlleva a que las soluciones presenten una gran cantidad de "falsos positivos".
- *Resistencia del usuario*. La desconfianza que se puede generar al instalar un agente DLP en una estación de trabajo, puede conllevar a que los usuarios interrumpan su correcto funcionamiento. (Sophos, 2008).

METODOLOGÍA

El enfoque de la investigación es de tipo cualitativa, debido a que "Estudia la realidad en su contexto natural, tal y como sucede, intentando sacar sentido de, o interpretar los fenómenos de acuerdo con los significados que tienen para las personas implicadas (Rodriguez, Gil, & Gárcia, 1996).

Se utiliza como método la Investigación-acción participativa ya que la autora, realizo observación directa y participativa de las actividades dentro de la organización. El método de investigación-acción participación (IAP) combina dos procesos, el de conocer y el de actuar, implicando en ambos a la población cuya realidad se aborda (Eizaguirre & Závala , 2006).

En la IAP se siguen básicamente cuatro fases, aunque no siempre se diferencian nítidamente unas de otras. a*) La observación participante*, en la que el investigador se involucra en la realidad que se estudiará, relacionándose con sus actores y participando en sus procesos. b) *La investigación participativa*, en la que se diseña la investigación y se eligen sus métodos, basados en el trabajo colectivo, la utilización de elementos de la cultura popular y la recuperación histórica. El investigador presenta al grupo los diversos métodos disponibles para la obtención de información, explicándoles su lógica, eficacia y limitaciones, para que aquél los valore y elija en base a los recursos humanos y materiales disponibles. Para la recogida de información se usan técnicas como la observación de campo, la investigación en archivos y bibliotecas, las historias de vida, los cuestionarios, las entrevistas, etc. La información es recogida, y luego sistematizada y analizada, por la propia comunidad, siendo el papel del investigador de mero facilitador. c) *La acción participativa* implica, primero, transmitir la información obtenida al resto de la comunidad u otras organizaciones, mediante reuniones, representaciones teatrales u otras técnicas, y, además, con frecuencia, llevar a cabo acciones para transformar la realidad. d) *La evaluación*, sea mediante los sistemas ortodoxos en las ciencias sociales o simplemente estimando la efectividad de la acción en cuanto a los cambios logrados, por ejemplo, en cuanto al desarrollo de nuevas actitudes, o la redefinición de los valores y objetivos del grupo (Guzmán, Alonso, Pouliquen, & Sevilla, 1994)

Cabe indicar que, para el presente trabajo de investigación, solo se contempla las fases de observación e investigación participativa, a través de la exploratoria y descripción de las necesidades, que dan origen al diseño del modelo de seguridad. Además, se utilizó el método de entrevistas dirigidas hacia el personal de TI, para conocer de las políticas y controles existentes.

Sin embargo, el alcance de la investigación, contempla el diseño del modelo de seguridad, realizar el diagnóstico inicial a partir de los constructos del modelo, realizar la simulación inicial sin aplicar una herramienta específica, donde los expertos dan su aporte a cada una de las variables.

Se utiliza estadística descriptiva para valorar el nivel del impacto generado, de la probabilidad de la fuga de datos de los SI, a través de los canales identificados.

A continuación, se presenta el modelo de seguridad, que concibe la utilización de una

herramienta DLP, como parte de la solución integral para prevenir la fuga de datos internos:

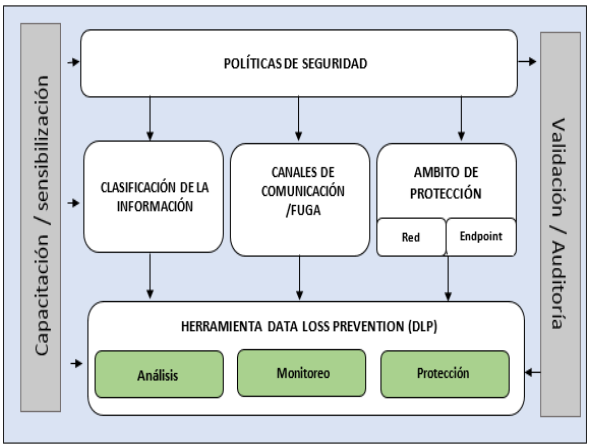


Figura No. 2. Modelo de seguridad para la prevención de fuga de datos.
Fuente: Elaboración del autor.

COMPONENTES DEL MODELO DE SEGURIDAD

Politicas de seguridad

Las organizaciones debe manejar una gestión de procesos, de manera organizada y eficiente, con el objetivo de poder identificar la comunicación y el transito que debe llevar la información. (Ca Technologies, 2012)

Por lo tanto, es necesario tomar los principios de Gobierno de TI, donde la optimización de recursos tecnologicos como soporte fundamental del resto de servicios universitarios (Férnandez & LLorens , 2014). Según, el informe de CISCO (2008), la falta de políticas de seguridad y el incumplimiento de los empleados de dichas políticas son factores significativos en la pérdida de información.

Por lo cual, se debe establecer políticas de seguridad desde un marco estratégico, con la finalidad de proteger la información, contra la divulgación, modificación o destrucción (Wurzler, 2013). Se toma como referencia la norma ISO /IEC 27002:2013, que direcciona hacia las politicas y medidas de seguridad, que contribuyen a prevenir la fuga de información interna:

Tabla No. 1. Políticas en base a la norma ISO/IEC 27002
Política de clasificación de la información
Política de control de accesos
Política de manejo de activos
Política de seguridad fisica
Política de respaldos
Política de divulgación de la información

No obstante, es necesario realizar un analisis de riesgo que permita identificar las amenazas, vulnerabilidades y su nivel de impacto, para posterior declarar e implementar procedimientos y controles[3] que ayuden a prevenir, mitigar y reducir la fuga de información (Guevara, 2013) (Ca Technologies, 2012).

Clasificación de la Información

Generalmente, en la mayoria de soluciones DLP, se definen las políticas y reglas de protección al paso que identifica la información considerada como confidencial. Sin embargo, para el autor esta no es una relación coherente, por lo cual para el modelo propuesto la identificación y clasificación de la información se considera en segunda instancia.

La protección de la información, gira al rededor de la conservación de principios fundamentales: *la confidencialidad*, que implica que la informacion es accesible solo por personas autorizadas, *la integridad*, que hace referencia

[3] Un “Control” es lo que permite garantizar que cada aspecto, que se valoró con un cierto riesgo, queda cubierto y auditable (Cisco, 2008).

que la información este correcta y sin modificaciones o errores y *la disponibilidad*, que indica que la informacion este accesible, cuando sea necesario (Symantec, 2010).

Es fundamental, antes de pensar en implementar una solución DLP, clasificar la información e identificar los lugares donde residen y su trayectoria de un sistema a otro (ISACA, 2010). De acuerdo, con la metodologia MAGERIT (2012) , la informacion puede ser clasificada en *Confidencial, Difusión limitada, Sin clasificar y de carácter público*; sin embargo, estos niveles estan supeditados por la criticidad de cada uno de los prinicipios de la información, y determinada por la organización.

Adicional, se debe considerar los diversos lugares donde puede alojarse los datos, de acuerdo a su utilización por los sistemas de información(SI) y los usuarios:

Datos en reposo: Considerados los datos que se encuentran alojados en servidores de archivos, redes de area de almacenamiento(SAN), bases de datos.

Datos en movimiento: Hace referencia a los datos transmitidos por la red a traves de correo electronico, la web o FTP.

Datos en uso: Comprende la informacion alojada en los puestos de trabajo, y las acciones derivada como copiar datos a un dispositovo USB, enviar datos a una impresora o intecambio de información entre aplicaciones (ISACA, 2010).

Canales de comunicación/Fuga

Se encuentran concebidos en aquellos canales informaticos por donde existe la probabilidad de una fuga de información. Acorde a la cantidad de aplicaciones y servicios que utilice la organización, se incrementarán los mecanismos de protección.

Para el modelo se presentan los siguientes:

Red: Refiere a la red utilizada por las aplicaciones o servicios para su funcionamiento, y que constituyen un canal de fuga de información. Las aplicaciones mas comunes en la organizaciones son el servicio de correo electronico, redes sociales, Mensajeria instantanea, almacenamiento u otros servicios en la nube, así como impresoras en red (Moreno, 2009).

Estaciones de trabajo: Generalmente, la información y los datos, que son utilizados por los usuarios son almacenados en ubicaciones locales, por lo que desde alli, esta información puede ser transportada a diferentes medios de almacenamiento externos como Discos duros y USB.

Se debe considerar la tendencia BYOD, donde la brecha de fuga de información se acrecenta, ya que no se dará una separación saludable de la información laboral y personal. (Saro & Férnandez, 2013).

Pérdida /Robo: Tiene una probabilidad menor de ocurrencia, pero es inherente que la pérdida de los dispositivos como portatiles, USB y dispositivos de almacenamiento, que representan una fuga de información.

Ambito de protección

Una vez que se han culminado con el segundo y tercer componente del modelo, es necesario preguntar ¿En donde es necesario proteger la información?, ¿Qué aplicaciones o servicios representan canales para la fuga de información?. La cantidad de canales de comunicación por donde se pueda producir la fuga de información, va a depender del tamaño de la arquitectura de la organización, de las aplicaciones y servicios ofrecidos, y por ende los protocolos de comunicación utilizados (Ponemon Instute, 2013). Por lo cual se establecen los siguientes ambitos de protección:

Red: Destinado a proteger la información que sea transmitida, a través del servicio de correo electrónico, redes sociales y demás servicios en la nube, analizando el tráfico web para garantizar que las solicitudes HTTP/HTTPS, no provengan ni se dirijan a ubicación sospechosas producidas

por malware, así como transferencias de archivos por el protocolo FTP[4] (CISCO, 2016).

Endpoint: Hace referencia a la proteccion en las estaciones de trabajo de los usuarios, donde se alojan datos provenientes de los sistemas de información. Es necesario, controlar los accesos a aplicaciones no esenciales o autorizadas, transferencia de archivos, conexiones inalambricas o sincronización de dispositivos móviles (celulares, tablets e ipads). Así, como tambien la salida a impresoras en red, dispositivos físicos como dispositivos de almacenamiento extraíbles, Bluetooth, Wi-Fi y otros dispositivos Plug and Play (Sophos, 2008).

Herramientas DLP

En el mercado existen una diversidad de soluciones DLP, ofrecido por reconocidos fabricantes a nivel de seguridad. Indistintamente, la solución seleccionada debe cumplir con tres etapas:

Analisis: Es la etapa inicial, donde se establecen las políticas/reglas de protección, de acuerdo con la etapa de clasificación de la información, provenientes de los sistemas de información, bases de datos y aplicaciones de servicio utilizadas por los usuarios. Se incluyen tecnicas y mecanismos, como fingerprint, filtros por tipos de archivos, contenidos o usuarios. (Cososys, 2012).

Monitoreo : En esta etapa, es esencial establecer un periodo de tiempo, en el cual se monitorea el comportamiento de los datos a traves en la red (datos en reposo y en movimiento), almacenamiento o descargas de datos en dispositivos moviles u otros medios de almacenamiento (datos en reposo) (Liu & Kuhn, 2010). Opciones adicionales, que se pueden odoptar estan orientadas al monitoreo de Portapapeles para evitar que los usuarios Copien/Peguen información confidencial, deshabilitar Imprimir Pantalla, escanear datos compartidos en la red, bloquear la impresión de datos connfidenciales por impresoras locales o compartidas en la red, Listas Blancas de URL, entre otros. (Cososys, 2012).

Estas políticas deberán estar orientadas inicialmente, a un modo de “alerta”, con el objetivo de predecir los impactos que puedan generarse en los procesos del negocio, y en lo posterior se revise y optimizen las políticas de protección del DLP (ISACA, 2010).

Protección: Al finalizar el periodo, las herramientas DLP incluyen interfaces de gestión, donde de evidencia los datos que fueron transferidos, en el momento y aplicación a traves de la cual se lo hizo. (Cososys, 2012). En esta etapa se detecta los incidentes que se generan por el uso unadecuado de la informacion, y se previene su fuga, a traves de acciones como el bloqueo o eliminación.

Validación / auditorias

Se considera como eje transversal este componente, debido a que contribuye al mejoramiento continuo del modelo, es decir, una vez que se tome en cuenta todos las etapas del modelo, y haya culminado el periodo de monitoreo de la herramienta DLP, a traves de los informes y conocimiento de los profesionales de TI, se reduciran los falsos positivos, se identificará y ajsutarán aquellas reglas, politicas y procesos, acorde a los objetivos organizacionales.

Capacitación y sensibilización

La capacitación /sensibilización, forma parte transversal del modelo, y es primordial diseñar una estrategia de concientización sobre la responsabilidad en el manejo de la información y sus posibles consecuencias laborales y legales. (Cabarique , Salazarr , & Quintero, 2015). Con lo anterior, se buscará la efectividad y eficacia del modelo de seguridad implantado en función de la prevención de la fuga de información interna.

[4] File Transfer Protocol, 'Protocolo de Transferencia de Archivos'.

ANÁLISIS DE RESULTADOS

El diseño del modelo de seguridad, surge a partir de una amplia búsqueda bibliográfica, acerca de las soluciones DLP, sus beneficios y principales problemas que han impedido su proliferación en materia de seguridad. Además, se considera la experiencia obtenida en la exploración y configuración de soluciones DLP.

Para dar inicio de la validación del modelo a través de la simulación, se realizaron entrevistas al personal de TI compuesto por Director de sistemas, Coordinador de red, encargado de soporte a usuarios y web master. De los resultados obtenidos de las entrevistas, con respecto al primer componente del modelo, se puede indicar que la IES, se encuentra en un nivel repetible (hablando en términos de madurez). Es decir, al ser una institución joven, posee políticas y procedimientos, concebidos para proteger los sistemas e información que se utiliza en su giro de negocio. Sin embargo, en lo que respecta a políticas de seguridad de la información, se refleja, en ausencia de políticas claras, definidas y documentadas.

Por su parte, en el segundo componente de clasificación de la información, la IES posee sistemas de información propios, que soportan los procesos principales, relacionados con su giro de negocio.

Se presenta una matriz cualitativa de la información definida como confidencial, donde se identifica la información generada por (6) los SI, que representa la unidad de análisis, y se valora la probabilidad del impacto en las dimensiones de seguridad, que representan las características.

Tomando en cuenta la metodología del Magerit, se elabora la siguiente tabla que permite valorar el nivel de impacto de la fuga, la probabilidad de acuerdo a una escala del 1 al 5, y por la subjetividad del experto, al ser una empresa pequeña se consideraron los siguientes porcentajes de fuga.

Tabla No. 2. Niveles de impacto

Nivel	Escala	% de fuga
MUY ALTO	5	> 40%
ALTO	4	30 al 40%
MEDIO	3	20 al 30 %
BAJO	2	10 al 20 %
MUY BAJO	1	< 10 %

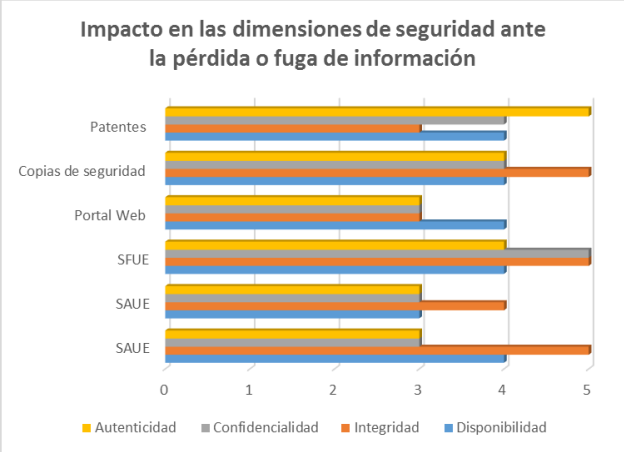
Elaboración Propia.
Fuente: Metodología Magerit

Tabla No. 3. Impacto de la información VS dimensiones de información

		Dimensiones			
Sistema de información	**Datos / Información**	**Disponibilidad**	**Integridad**	**Confidencialidad**	**Autenticidad**
SAUE	**Información académica**: Datos de los estudiantes, Récord de notas, pensum académico, Títulos.	4	5	3	3
SAUE	**RRHH:** Datos de empleados, sueldos, vacaciones, documentación personal.	3	4	3	3
SFUE	**Información Financiera** :Datos financieros: balances, presupuestos, gastos.	4	5	5	4
Portal Web	**Portal web:** Sistema virtual de enseñanza-aprendizaje,	4	3	3	3
Copias de seguridad	**Copias de seguridad:** Respaldos de seguridad de la información en las bases de datos	4	5	4	4
Patentes	Sistemas informáticos, aplicaciones (biblioteca, eco buses etc.)	4	3	4	5

Elaboración Propia
Fuente: Universidad ECOTEC

Gráfico No. 1. Impacto de las dimensiones de seguridad



Elaboración Propia.
Fuente. Universidad ECOTEC

Al carecer de políticas de seguridad claras y definidas, la información se encuentra expuesta a ataques informáticos, manipulación por parte de los usuarios que compromete las dimensiones de la seguridad de la información, evidenciado en los gráficos que No. 1 y 2, donde la dimensión más comprometida es la integridad.

Gráfico No. 2. Promedio general de las dimensiones de seguridad.

Elaboración Propia.
Fuente. Universidad ECOTEC

Se utilizó estadística descriptiva, de las cuatro dimensiones de seguridad, donde se muestra que en promedio de integridad es la dimensión que presenta mayor impacto (4.17), respecto a las demás dimensiones, esto de se debe a que tiene mayor dispersión de los datos, como lo indica el coeficiente de variación (24%).

Tabla No. 4. Impacto de la información VS dimensiones de información

	Disponibilidad	Integridad	Confidencialidad	Autenticidad
Media	3,83	4,17	3,67	3,67
Error típico	0,17	0,40	0,33	0,33
Media na	4,00	4,50	3,50	3,50
Moda	4,00	5,00	3,00	3,00
Desviación estándar	0,41	0,98	0,82	0,82
Coeficiente de variación	11%	24%	22%	22%
Curtosis	6,00	-2,39	-0,30	-0,30
Coeficiente de asimetría	-2,45	-0,46	0,86	0,86
Rango	1,00	2,00	2,00	2,00
Mínimo	3,00	3,00	3,00	3,00
Máximo	4,00	5,00	5,00	5,00
n	6,00	6,00	6,00	6,00

Elaboración Propia.
Fuente. Universidad ECOTEC

Se elaboró una matriz de valoración, antes de validar el modelo de seguridad, utilizando una herramienta DLP para la prevención de los datos, con la finalidad de valorar la probabilidad de la fuga de la información proveniente de los SI, en relación a los canales identificados, obteniendo los siguientes resultados.

Tabla No. 5. Matriz de impacto antes de validar el modelo seguridad, utilizando herramientas DLP

		Sistema de información			
	Canales de fuga	SAUE	SFUE	ATRIUM	Portal WEB
Red	Correo Electrónico	5	5	4	4
	Redes sociales	5	5	5	5
	Mensajeria instantanea	4	4	4	4
	Almacenamiento en la nube	5	5	5	5
PC Local	Usb / Flash	5	5	5	4
	Disp. Externos de almacenamiento	5	5	5	4
	Impresoras en red	5	5	4	4
Pérdida/ robo	Portátiles	5	5	5	3
	USB, CD, DVD	5	5	5	3
	Cintas de respaldo	3	3	3	3

Elaboración Propia
Fuente: universidad ECOTEC

Como se observa en la matriz anterior, el 60% de la información tiene probabilidad de fuga muy alta al tener una valoración de 5, el 25% probabilidad alta al tener una valoración de 4 y el 15% probabilidad media con valoración de 3. Esto se debe, a que carece de políticas y controles, que impidan la fuga de la información a través de aplicaciones de red y pc locales. La mayoría de los servicios están basados en la nube, por lo cual facilita la transmisión y almacenamiento de la información al exterior de la organización.

Considerando el análisis anterior, en conjunto con el personal de TI, se llevan a cabo actividades basadas en el modelo propuesto, que permitan cumplir con cada uno de los componentes. Después, se utiliza la matriz de valoración utilizada anteriormente, para valorar la probabilidad del impacto ante la fuga de información, obteniendo los siguientes resultados:

Tabla No. 6. Matriz de impacto después de validar el modelo seguridad, utilizando herramientas DLP

		Sistema de información			
	Canales de fuga	SAUE	SFUE	ATRIUM	Portal WEB
Red	Correo Electrónico	3	3	2	2
	Redes sociales	3	3	3	3
	Mensajeria instantanea	2	2	2	2
	Almacenamiento en la nube	3	3	3	3
PC Local	Usb / Flash	3	3	3	2
	Disp. Externos de almacenamiento	3	3	3	2
	Impresoras en red	3	3	2	2
Pérdida/ robo	Portátiles	3	3	3	1
	USB, CD, DVD	3	3	3	1
	Cintas de respaldo	1	1	1	1

Elaboración Propia
Fuente: universidad ECOTEC

En base a las matrices obtenidas, antes y después de la validación del modelo, se definieron los siguientes puntos:

- ✓ Existe una disminución del impacto y probabilidad de fuga de información, por lo que la implementación fue efectiva, al establecer políticas y controles de seguridad, y permitir los accesos correctos a los usuarios.

- ✓ En la simulación, la valoración de la probabilidad de impacto de fuga e datos es media (60%), debido a que la IES, basa su funcionamiento de algunos servicios esenciales, utilizando servicios gratuitos en la nube, por lo cual queda un sesgo de fuga de la información, que no puede ser controlada debido a la característica de sus servicios.

- ✓ El funcionamiento de la herramienta DLP seleccionada, continuará siendo efectiva, a medida que se sigan ajustando y perfeccionando las políticas de protección en base al monitoreo continuo, identificando a su vez, aquellos usuarios que infrinjan las políticas establecidas y socializadas.

CONCLUSIONES

Los ataques informáticos y la fuga de información, son problemas que deben ser primordiales en cualquier organización, incluso en las IES, donde al carecer de sensibilización en cuanto a seguridad de la información, por no ser un objetivo de su giro de negocio, contribuyó a la identificación de los requisitos del modelo de seguridad para la prevención de fuga de datos.

La implementación de las herramientas DLP, debe concebirse, desde las necesidades organizaciones, para su eficiente funcionamiento. Estas herramientas, proporcionan una amplia perspectiva del flujo de los datos, y los canales de comunicación utilizados para exteriorizar la información, contribuyendo con un modelo de defensa en profundidad, en donde el actor principal es la información.

De acuerdo, a la simulación realizada, la utilización del modelo de seguridad para prevenir la fuga de datos internos, corrobora que los resultados son satisfactorios.

El modelo de seguridad, basado en la utilización de herramientas para la prevención de fuga de datos internos, proporciona una solución integral de los componentes que se requieren antes de decidir implementar una herramienta DLP, así, como los ejes transversales que permiten la prevención de la fuga de datos, a través de concientización y capacitación de los usuarios, y la mejora continua, por medio de la validación y ajuste de las políticas.

Las limitaciones que se presentaron en esta investigación, es la utilización de la herramienta, y validación de componentes como la sensibilización que enmarcan la utilización de estudios más profundos.

Tomando en cuenta, los resultados obtenidos, se plantea como trabajo futuro de investigación, la implementación del modelo de seguridad, utilizando una herramienta DLP, que cumpla con las características establecidas. Así, como contrastar los resultados obtenidos en esta investigación, con los resultantes de la implementación total.

BIBLIOGRAFÍA

3M. (2013). *Un Nuevo Estudio Identifica a la Privacidad Visual como un Eslabón Débil en las Prácticas de Seguridad Informática.* Argentina.

Acosta, X. (2015). *Desarrollo de un modelo de seguridad para la prevención de perdida de datos en las pymes.* Obtenido de http://dspace.udla.edu.ec/handle/33000/4476

Brightman, I., & Buith, J. (2007). *Treading Water. The 2007 Technology,Media & Telecommunications Security Survey.*

Burgos, J., & Campos , J. (2008). *Modelo Para Seguridad de la Información en TIC.* Obtenido de http://ceur-ws.org/Vol-488/paper13.pdf

Ca Technologies. (2012). *Protección de su información : 10 factores fundamentales para el éxito de la implementación.*

Cabarique , A., Salazarr , C., & Quintero, Y. (24 de Octubre de 2015). *Factores y causas de la fuga de información sensibles en el sector empresarial.*

Castrillón, M., & Lezcano , M. (2013). *Metodología para prevenir la fuga de información, aplicando DLP en el sector financiero.* Obtenido de http://docplayer.es/7926139-Metodologia-para-prevenir-la-fuga-de-informacion-aplicando-un-sistema-dlp-en-las-empresas-del-sector-financiero.html

CEDIA. (FEBRERO de 2014). *INFORME DE RESULTADOS DE LA "1° ENCUESTA DE SEGURIDAD DE LA INFORMACIÓN EN UNIVERSIDADES ECUATORIANAS MIEMBROS DE CEDIA".*

Cisco. (2008). *Fuga de datos a nivel mundial: Riesgos y errores comunes de los empleados.*

CISCO. (Enero de 2016). *Informe anual de seguridad 2016.* Obtenido de http://www.cisco.com/c/dam/m/es_es/internet-of-everything-ioe/iac/assets/pdfs/security/cisco_2016_asr_011116_es-es.pdf

Cososys. (2012). *Cómo implementar una solución de Prevención de Pérdida de Datos.* Obtenido de www9EndpointProtector9es

DCSSI. (19 de Julio de 2004). *La defensa en profundidad aplicada a los sistemas de información.* Obtenido de conseil.dcssi@sgdn.pm.gouv.fr

ECI. (2013). *Ethics and compliance Iniciative*. Obtenido de Capacitar a las organizaciones para que construyan y mantengan programas de E & C de alta calidad.: https://www.ethics.org/resources/free-toolkit/ethics-timeline

ECI. (2016). *Ethics and compliance iniciative.* Obtenido de Global Business Ethics Survey: www.ethics.org

Eizaguirre, M., & Závala , N. (2006). *Investigación-acción participativa (IAP).* Obtenido de http://dicc.hegoa.efaber.net/listar/mostrar/132

Férnandez, A., & LLorens , F. (2014). *Gobierno de las TI para las Universidades.*

Flórez , W., Arboleda , C., & Cadavid, J. (12 de 03 de 2012). *SOLUCIÓN INTEGRAL DE SEGURIDAD PARA LAS PYMES MEDIANTE UN UTM.*

Guevara, L. M. (2013). *Análisis de riesgos de los sistemas de información.*

Guzmán, G., Alonso, A., Pouliquen, Y., & Sevilla, E. (1994). *Las metodologías participativas de investigación: el aporte al desarrollo local endógeno, Instituto de Sociología y Estudios Campesinos, ETSIAM.* Obtenido de http://www.terceridad.net/sc3/Por_Tema/2_Metodo_IA_IP/Apoyo_2/metdolog%EDas%20participativas_X.pdf

INEC. (16 de mayo de 2014). *Ecuador en Cifras.* Obtenido de http://www.ecuadorencifras.gob.ec/12-millones-de-ecuatorianos-tienen-un-telefono-inteligente-smartphone/

ISACA. (2010). Prevención de fuga de datos. Rolling meadowns.

IT Governance Institute. (2008). *Alineando Cobit 4.0, ITIL, e ISO/IEC 27002.*

Liu, S., & Kuhn, R. (Abril de 2010). *Data Loss Prevention.*

McAfee. (Septiembre de 2014). *McAfee Data Loss Prevention Endpoint.*

Medina, M. (Junio de 2015). *Creadess.* Obtenido de http://www.creadess.org/index.php/informate/sostenibilidad-empresarial/cultura-organizacional/14830-politica-organizacional-concepto-y-esquema-en-la-empresa

Ministerio de Hacienda y Administraciones Públicas. (2012). MAGERIT V3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. En *LIBRO II. CATÁLOGO DE ELEMENTOS.* Madrid: Ministerio de Hacienda y Administraciones Públicas.

Moreno, D. (Abril de 2009). *¿Que preocupa? prevención de fuga de información.*

Pacheco, F. (19 de Enero de 2011). *Fuga de información: ¿una amenaza pasajera?* Obtenido de www.eset-la.com

Ponemon Instute. (2013). *2013 Costo of data breach Study: GLobal Analysis.*

Rodriguez, G., Gil, J., & Gárcia, E. (1996). *Metodología de investigación cualitativa.* Obtenido de https://scholar.google.es/scholar?q=related:0yi5Xln0EicJ:scholar.google.com/&hl=es&as_sdt=0,5

Sánchez, V. (15 de JUNIO de 2002). *Proquest.* Obtenido de http://search.proquest.com/docview/315891375/4D915073D99341F7PQ/16?accountid=130858

Saro, J., & Férnandez, J. (2013). La gestión segura de la información en movilidad ante el fenómeno BYOD: ¿Bring Your Own Device =Bring Your Own Disaster? *SIC*, 67-73.

Sophos. (JUNIO de 2008). *Detener la fuga de datos:Aprovechando su inversión existente en seguridad .* Obtenido de www.sophos.com

Symantec. (2010). *Fuga de Información, Un negocio en crecimiento.*

Websense. (2013). *Prevención unificada contra la contra la pérdida de datos para gateways, puntos finales y detección.*

Wurzler, J. (Abril de 2013). *Information Risks & Risk Management.*