MAESTRÍA EN AUDITORÍA DE TECNOLOGÍAS DE LA INFORMACIÓN

NIVEL DE APLICACIÓN DE SEGURIDAD INFORMÁTICA PARA EVITAR LA FUGA DE INFORMACIÓN EN LAS COOPERATIVAS DE AHORRO Y CRÉDITO DE LA ZONA 1 DEL ECUADOR

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

Magíster en Auditoría de Tecnologías de la Información

Por el estudiante:
Marco Antonio YANDÚN VELASTEGUÍ

Bajo la dirección de:
Mónica Jeannette FLORES MARÍN

Universidad Espíritu Santo
Maestría en Auditoría de Tecnologías de la Información
Samborondón - Ecuador
Noviembre de 2018

Nivel de aplicación de seguridad informática para evitar la fuga de información en las cooperativas de ahorro y crédito de la Zona 1 del Ecuador.

Level of computer security application to prevent the leakage of information in the savings and credit cooperatives of Zone 1 of Ecuador.

Marco Antonio YANDÚN VELASTEGUÍ[1]
Mónica Jeannette FLORES MARÍN[2]

Resumen

En el presente artículo, se expone la fuga de información como una problemática existente en las Cooperativas de Ahorro y Crédito, debido al nivel de aplicación de seguridades, se muestra las estadísticas de la información que los empleados sacan de su lugar de trabajo de acuerdo a los informes de seguridad de fabricantes y proveedores de herramientas de seguridad informática, se muestra los resultados de la investigación de campo realizada al personal de Tecnología, Sistemas, Seguridades, a través de encuestas que incluyen 38 items relacionados a personas, procesos y tecnología que intervienen en el control, distribución y resguardo de documentos físicos y digitales que contengan datos sensibles o valiosos, formas de fuga de información y sus contramedidas. Con los resultados se concluye principalmente que no se garantiza la confianza en el personal que administra el archivo de documentos físicos, base de datos, programadores, procesos batch, seguridades, puede existir pérdida de documentos físicos con información de socios y clientes, cuando se comparte información con otras entidades no toda la información se envía cifrada, las revisiones de seguridad informática revelan vulnerabilidades en la información de tarjeta habientes, estas conclusiones constituyen los insumos para establecer los criterios para el cumplimiento normativo con las recomendaciones y actividades a cumplir a corto, mediano y largo plazo que contribuyen a la problemática y a fortalecer las seguridades para evitar la fuga de información en las Cooperativas financieras.

Palabras clave: Fuga de Información, seguridad informática, iso27002, ITIL

Abstract

In this article is exposed, the leakage of information as an existing problem in the Savings and Credit Cooperatives due to the level of application of securities, it shows the statistics of the information that employees take from their place of work according to the Safety reports of manufacturers and suppliers of computer security tools, shows the results of the field research carried out to the personnel of Technology, Systems, Securities, through surveys that include 38 items related to people, processes and technology that intervene in the control, distribution and safeguarding of physical and digital documents that contain sensitive or valuable information, forms of information leakage and their countermeasures. With the results it is concluded that confidence in the personnel that manages the file of physical documents, database, programmers, batch processes, securities, can not be guaranteed, there may be loss of physical documents with information of partners and clients, when it is shared information with other entities not all information is sent encrypted, computer security reviews reveal vulnerabilities in cardholder information, these conclusions constitute the inputs to establish the criteria for compliance with the recommendations and activities to be met in the short, medium and long term that contribute to the problem and strengthen the securities to avoid the leakage of information in the financial cooperatives.

Key words | Leakage of information, Informatic security, ISO 27002, ITIL.

[1] Magister en Sistemas Informáticos Educativos. Estudiante de Maestría en Auditoría de Tecnología de Información, Universidad Espíritu Santo – Ecuador, Docente de la Universidad Politécnica Estatal del Carchi - Ecuador E-mail myandun@uees.edu.ec
[2] Magíster en Administración de Empresas. Docente de la Facultad de Sistemas de la Universidad Espíritu Santo- Ecuador. E-mail mfloresm@uees.edu.ec

INTRODUCCIÓN

Según Ernst y Young (2012) basados en una investigación realizada por Dark Reading / Information Week, el 73% de casos relacionados a fuga de información son ocasionados por el personal interno de la organización, en otras encuesta realizada por Ekran System (2015) muestra que hasta 90% de responsables de la seguridad en la empresas ven a los empleados como la mayor amenaza en seguridad informática, el Informe de McAfee (2015) sobre la encuesta realizada a 1400 profesionales de Tecnología de la Información de Reino Unido, Estados Unidos, Alemania y Australia, demostró que el 77% de las empresas son incapaces de auditar o cuantificar la pérdida tras una fuga de información, en el estudio de seguridad de Check Point (2015) como muestra la Tabla 1, se indica los datos más comunes que los empleados envían fuera de la organización.

Tabla N°1. Información que los empleados extraen de la empresa basado en el Estudio de Seguridad de la marca (Chek Point, 2015)

DATOS ENVIADOS FUERA DE LA ORGANIZACIÓN POR LOS EMPLEADOS					
	2014	2013		2014	2013
Información del propietario	45%	35%	Información de la Red	13%	14%
Datos de tarjeta de crédito	30%	29%	Archivos protegidos con contraseña	10%	10%
Registros de datos de negocios	20%	21%	Mensaje de correo confidenciales	5%	5%
Información personal	25%	22%	Números de cuentas bancarias	5%	4%
Información sobre salarios	13%	14%	Otras	27%	31%

Fuente: Chek Point 2015

Otro caso que se destaca es lo ocurrido en Bancolombia, dado que fue atacado por un grupo de hackers los cuales lograron transferir 160.000 millones de pesos a varias cuentas de Bancolombia, en donde se frustró dicho robo debido a que en el banco se tenía implementados controles internos, por esta razon los delincuentes lograron solamente llevarse el 4% de lo que pensaban hurtar Zabala, M. (2014).

De acuerdo con la encuesta realizada por Yandún (2015) aplicada a 110 empleados de la Cooperativa de Ahorro y Crédito Tulcán perteneciente a la Zona 1 del Ecuador, entre los principales resultados se obtuvo que: los empleados en su mayoría relaciona la fuga de información con el envío de datos confidenciales en impresos, archivos digitales, capturas de pantallas a través de correo electrónico y a través de otros medios de almacenamiento en la nube como Dropbox, Skype Drive; así también se puede indicar que los empleados tienen la percepción de que la fuga de información se realiza a traves de unidades de almacenamiento extraibles como USB, Cd y DVD y el desconocimiento sobre los artículos legales relacionados y las respectivas sanciones a aplicarse identificando la necesidad de capacitaciones sobre temas en: normativa legal, fuga de información y temas relacionados al empleado seguro.

Es por ello que en un artículo de la tesis doctoral que ha sido publicado en la revista Knosys Guevara, C. (2017), no solo se menciona la problemática de la fuga de información sino que presenta un algoritmo que sirve para la detección de fugas de información utilizando las bases de datos Ecuador y Unix Comands. Como resultado se propone un nuevo algoritmo que sirve para detectar los comportamientos fuera de lo normal que presenten los usuarios mientras utilizan los sistemas informáticos, dicho algoritmo identifica el comportamiento de cada usuario y sus tareas frecuentes y lo transforma en un perfil individual de comportamiento en el sistema, también clasifica actividades como posibles anomalías las mismas que se comprueban dos veces por medio de cadenas de Markov como indica Polanco, C. y Castañon, A. (2015) este procedimiento ha demostrado ser efectivo y preciso en detección y baja tasa de falsos positivos relacionados a la fuga de información, por esta razón que el objetivo de la presente

investigación es medir el nivel de aplicación de seguridad informática en las Cooperativas de Ahorro y Crédito de la Zona 1 de planificación territorial del Ecuador.

MARCO TEÓRICO

La información.

Conforme a Kunar (2013) es el conjunto de datos organizados y procesados que puede estar representados como: mensajes, instrucciones y operaciones u otra acción dentro de un computador.

Información como activo.

Para Aumatell, C. (2013) la información tiene un valor incalculable en las instituciones y se clasifican según su tipo en: archivos digitales, bases de datos, archivos impresos; también los datos que se acceden por medio de aplicaciones en servidores, equipos de comunicación, servicios de alojamiento en internet, almacenamiento en medios externos en la nube.

Activos de Información.

Arcilla-Cobián, M., San Feliu, T., Feliz, A., Calvo-Manzano, J. (2017) como una forma de incrementar la calidad en las organizaciones esta la mejora de los procesos internas especialmente los que tienen que ver con la organización de los activos de información mismos que puede ser hardware o software con los que interactua la información.

Clasificación de la información.

Como indica Dávila, L. y Pacheco, L (2017) la información se clasifica dependiendo de niveles de protección y la seguridad aplicada para poder utilizarla durante su vida útil y en cualquier formato que este disponible, además indican los responsables de la información, la información se clasifica en:

- **Información Reservada**, según Jasso, L. (2017) es la información considerada como crítica o de alta sensibilidad a la cuál se debe proteger por la relevancia que tiene para la toma de decisión empresarial ya que el impacto que llegue a manos equivocadas en muy alto y con consecuencias financieras, fraudes, imagen, esta información está disponible a un grupo reducido de personas.

- **Información restringida,** para Díaz, D. y Ramírez, M. (2015), este tipo de información es considerada sensible para las áreas internas su acceso es controlado por los dueños de la información y protegida por imagen de la organización de los empleados, proveedores y clientes.

- **Información de uso interno**, como indican García, M., Lirola, E. y Mato, V. (2017) no es reservada y su acceso es sin restricción pero dentro de la organización para compartir con terceros debe existir autorizaciones de uso e incluso un acuerdo de confidencialidad entre el usuario y el dueño de la información.

- **Información pública**, es la información que se encuentra disponible sin restrinciones y que su perdida no afecte de ninguna manera a la organización en la imagen o de forma económica Moreno, E., Ramírez, C. y Salazar, M. (2018).

Confidecialidad.

Fernández, F. (2017) indica que la confidencialidad es garantizar que la información solo sea revelada y obtenida por personas autorizadas evitando que la misma sea distribuida a terceros, Oliver Vilella, G., y Pérez Cruz, E. (2017) indican que es un derecho que tiene una comunicación de privilegio y se conoce como el intercambio de información.

Integridad.

Conforme indican Stenta, H., Rentería, J., y Riccardi, G. (2005) la integridad se refiere al hecho de garantizar que la información lógica, incluido los procesos sean exactos y que se

encuentren completos o íntegros, aplicando métodos que prevengan la modificación o eliminación de información sin autorización.

No repudio.

Caldana, D., Correa, R., y Ponce, H. (2007) indican que es similar a la integridad pero que dispone de una característica adicional que los datos no sean puestos en duda o pasen por un proceso de verificación.

Formas de fuga de la información.

Como indica Bortnik (2010), dentro de las empresa existen múltiples formas para que la información salga de forma no controlada, entre lo más común se puede mencionar la salida de documentos, datos o información a través de cualquier dispositivo externo de grabación, por medio impreso y por cualquier servicios o protocolo disponible en internet.

Formas de mitigación de la fuga de información.

Para Bowen, Salem, Hershkop, Keromytis y Stolfo (2009), evitar la fuga de información es una tarea extensa y pensar que existe mecanismos cien por ciento efectivos y que eviten la fuga de información es algo que no se dispone, Beltrán. J., Pineda, A., y Quevedo, A. (2016) exponen se puede realizar algunas acciones de protección que ayuden a mitigar la fuga de información, pero no evitar que la información siga saliendo de la empresa, así tambien Blasco, J. (2012), en su tesis doctoral indica que los mecanismos actuales con dispositivos de prevención de fuga de información (DLP) no responden efectivamente a todos los posibles ataques que compromentan la confidencialidad de la información así tambíen no analizan los comportamientos diferentes que un empleado malicioso puede tomar.

Formas básicas, medias y con dispositivos para mitigar la fuga de información.

De acuerdo con Cabrales. L, (2015) establece que las empresas deben garantizar y permitir la entrada y salida de información aplicando estrategias como: el software y hardware que se utilice en la organización deben estar actualizados con los parches de seguridad, instalar las actualizaciones recomendadas al software, los puertos de acceso de sitios web o plataformas web cerrados, bloqueo de puertos y unidades extraíbles, configuración de directivas de grupos en el sistema operativo, protección con programas antivirus y en caso que se cuente con recursos económicos necesarios Proctor, Mogull, y Oullet. (2007) muestra el cuadrante de Gartner con la clasificación de las herramientas tecnológicas DLP (Data Loss Prevention) que son las apropiadas para protección de fuga de información para Peltier, T. (2005) con un análisis de riesgos apropiado ayudaría a determinar la necesidad de la implementación con un fundamento profesional.

Castrillon, M. y Lezcano, M. (2012) indican que estas herramientas DLP no son los único y último en tecnología de prevención de fuga de información, son un complemento a los dispositivos de protección de la infraestructura como los muros de fuego (Firewall), sistemas de detección de Intrusos (IDS) y los sistemas de prevención de Intrusión (IPS), por los tanto los DLP, podría proporcionar ciertos controles para mitigar de mejor forma la fuga de información desde el interior de las empresas.

Restricción de uso de canales de comunicación, internet, email, red.

Según el fabricante de dispositivos Sophos (2018) con el uso de dispositivos como los firewall, UTM, se puede realizar filtrado de la señal de internet y restringir el acceso al servicio así como delimitar su uso de acuerdo a las funciones que desempeñan los empleados.

En este sentido Castro, M. (2017) indica que el correo electrónico corporativo debe ser utilizado con fines laborales, recomienda el control, y monitoreo de alertas que se generen en los servidores de este servicio, así también denegar el uso de correo electrónico personal.

A parte de los dispositivos mencionados anteriormente se debe restringir la instalación y

uso de aplicaciones de intercambio de información como Skype, Emule, MSN, Teamviewer, Dropbox, entre otras, dado que como menciona Teijeira, P. (2010) estas aplicaciones pueden ser agujero de seguridad, por lo tanto es recomendable bloquearlas o borrarlas como medida de mitigación para evitar la fuga de información.

Rol del personal de seguridad lógica.

Para Peltier, P. (2005) señala al Oficial de Seguridad de la Información como el rol específico y encargado de analizar, proponer, implementar y controlar las seguridades referentes a la información, estas acciones deben estar alineadas a las políticas de la empresa en caso de no existir políticas puede estar basadas a las normativas, estándares y marcos de referencias internacionales, como indica Hernández, A. (2010), el personal de seguridad informática debe estar inmerso en los procesos de auditoría informática e incluye el proceso de diagnóstico, evaluación de los entornos y activos de información.

Como mencionan Martelo, R. Tovar, L. y Maza D. (2017), el cargo de responsable de seguridad lógica se ha desempeñado por profesionales certificados en seguridad informática o incluso en auditoría informática, pero en ocasiones este cargo es ocupado por personal o profesionales informáticos y en algunos casos por otro tipo de profesionales con o sin certificaciones, en este sentido Voutssas, J. (2012) argumenta, los aspectos formales que debe cumplir el Oficial de Seguridad por sus siglas en Inglés, Information System Security Officer— ISSO como: apoyar en las auditorías informáticas, implementar controles, participar en la recuperación contra desastres que afecten a la infraestrutura de seguridad informática, para Burgos Salazar, J., y Campos, P. (2008) otras de las actividades que realiza el Oficial de seguridades lógicas es: los diagnósticos de seguridad, establecer los responsables para las áreas de seguridad informática, clasificar y controlar los activos informáticos y de seguridad, así como el análisis y control de riesgos operativos e informáticos.

Buenas prácticas de seguridad ISO 27000, ITIL.

La Organización Internacional de Normalización (ISO) se establece como un estandar internacional preparado para proporcionar los requisitos para establecer, implementar, mantener y mejorar continuamente un sistema de administración de seguridad de la información que incluye: los requisitos para sistemas de gestión de seguridad de información (ISO 27001), la guía de aplicación de buenas prácticas, controles de seguridad de la información (ISO 27002), la guía de implementación del Sistema de Gestión en Seguridad de la Información acompañado del esquema Plan, Do, Check, Act (ISO 27003), las métricas que miden la eficiencia del Sistema de Gestión de Seguridad de la Información (ISO

27004), La guía para la gestión de riesgo (ISO 27005), La guía de auditoría de los Sistemas de Gestión de Seguridad de la Información (ISO

27007), La norma para la gestión de seguridad de la información en la telecomunicaciones (ISO 27011), La guía para aplicar la continuidad de negocio en referencia a las Tecnologías de Información y comunicación (ISO 27031), la guía de protección conocida como ciber-seguridad (ISO 27032), la guía de referencia aplicable a seguridad en redes (ISO 27033), y la guía de referencia de seguridad para aplicaciones informáticas (ISO 27034).

Por otra parte, ITIL (2009) es un marco de referencia que muestra los lineamientos de la administración de los servicios referentes a Tecnología de la Información que se brindan en las organizaciones ya sean públicas o privadas.

Bon J. (2010), redactor autorizado de ITIL, indica que ITIL es una buena práctica que ha demostrado ser valida aplicandola para mejorar los servicios de tecnología de la información y un solido respaldo para las organizaciones, debido a que ITIL, enfoca la gestión de los servicios tecnológicos en su ciclo de vida que incorpora la estrategia, diseño, transición, operación y mejora continua de los servicios.

METODOLOGÍA.

Enfoque de investigación.

Se define como enfoque de la investigación cualitativa, en vista que se midió el nivel de seguridad implementadas para evitar fuga de información lógica, así también el conocimiento de los empleados en temas relacionados a seguridad, formas de mitigación, medidas de control implementadas, estos items son basados en el marco de referencia ITIL, norma ISO 27000 y las resoluciones emitidas por las organizaciones de control, el escenario de investigación son las Cooperativas de Ahorro y Crédito de la zona 1 del Ecuador y que pertenezcan al segmento uno, de cooperativas grandes según clasificación de la Superintendencia de Economía Popular y Solidaria y que tienen la mayor participación en captación y colocación de depósitos como indica la Tabla 2.

Tabla N° 2. Datos de captaciones, colocaciones y número de socios de las CAC's de la Zona 1 del Ecuador.

Al 30 de abril de 2017	Captaciones	%	Colocaciones	%	Número de socios	%
CAC's Seleccionadas	322.765.434,75	83,26 %	300.834.803,36	74,18 %	259.198	78,15 %
Total CAC's zona 1	387.635.265,98	100	405.517.670,29	100	331.635	100

Fuente: Superintendencia de Economía Popular y Solidaria (SEPS, 2017)

Como informantes se define a todo el personal de Tecnología, Sistemas, Seguridades y Operaciones de las Cooperativas de Ahorro y Crédito, en cuanto a las técnicas e instrumentos utilizadas se aplicó encuestas electrónicas, El tipo de muestra es una muestra no probabilística por conveniencia.

Las encuestas contienen 4 aspectos a evaluar relacionados con la aplicación de normativas de control interno que son: 1. La información que se gestiona en los sistemas informáticos y la información generada por otros medios en la Cooperativa, 2. Los sitios destinados para archivar los documentos físicos en especial los documentos y carpetas con información de socios y clientes en la Cooperativa, 3. El respaldo de información digital en la Cooperativa y 4. Procesos de auditoría informática internas y/o externas realizadas en la Cooperativa cada aspecto contiene entre 9 y 11 ítems los cuales se evalúa de acuerdo a la escala de Lickert en donde 1 es totalmente en desacuerdo y 5 totalmente de acuerdo.

Muestra de la investigación.

Como muestra de la presente investigación se determinó a 17 profesionales que conforman todo el personal de Tecnología, Sistemas, Seguridades y Operaciones de las Cooperativas de Ahorro y Crédito seleccionadas de la zona 1 del Ecuador.

Validación del instrumento de recolección de información.

Urrutia, M., Barrios, S., Gutiérrez, M., y Mayorga Camus, M. (2014) resaltan que la validación de jueces o experto a los instrumentos de investigación es un factor de validez del contenido y comprobar su calidad e indican que de acuerdo a la investigación, objeto de estudio, áreas geográficas, actividad laboral, entre otros aspectos, se debe determinar el número y perfil de los jueces validadores que puede variar entre 3 y 15 jueces o expertos validadores. Para la presente investigación se tomó en cuenta los objetivos de estudio, áreas geográficas y conocimiento de la temática, se determinó el número de 7 jueces o expertos validadores a los instrumentos de investigación los cuales se indican en la Tabla 3 son:

Tabla N° 3. Detalle de Juez – expertos para validación de instrumentos de investigación.

Nombre	Cargo	Organización	Años de experiencia
Ing. Eduardo Cando.	Subgerente de Tecnología y operaciones.	Cooperativa de Ahorro y Crédito 29 de Octubre	>12
Ing. Gabriel Gordón.	Supervisor de seguridades lógicas.	Cooperativa de Ahorro y Crédito Tulcán	>7
Ing. Juan Rosero.	Supervisor de seguridades físicas.	Cooperativa de Ahorro y Crédito Tulcán	>5
Msc. Luis Patiño.	Director de la Carrera de informática.	Universidad Politécnica Estatal del Carchi	>15
Msc. Carlitos Guano.	Experto Tic's y seguridad informática, Docente universitario.	Universidad Politécnica Estatal del Carchi	>10
Msc. Georgina Arcos.	Docente universitaria.	Universidad Politécnica Estatal del Carchi	>12
Msc. Jairo Hidalgo.	Experto en redes de computación Docente universitario.	Universidad Politécnica Estatal del Carchi	>10

Fuente: Autor

Instrumentos de recolección de información.

En la Tabla 4, se muestra los items que se incluyeron en el instrumento utilizado para la recolección de la información, se coloca la relacion que tiene cada item con las normativas de los organismos de control, lo relacionado a la Norma ISO 27002 y el Marco de Referencia ITIL.

Tabla N° 4. Items de los instrumentos de recolección y su relacion con normativa interna, ISO, ITIL

Nro.	Descripción del ítem	Aspecto a evaluar relacionados con normativas de control (NCSFyE-SEPS-2018).[3] (JB-2012-2148 –SBS)[4]	Relación con la normas ISO 27002 objetivos de control y/o controles	Relación con ITIL (2012)
Item 1	Se cataloga o clasifica la información en pública, privada, confidencial.		8.2.1 Directrices de clasificación: La información debería clasificarse en relación a su valor, requisitos legales, sensibilidad y criticidad para la Organización.	Diseño de Servicio - Gestion de Seguridad Asegura que la confidencialidad, integridad y disponibilidad de los activos, información, datos y servicios de TI de una organización satisfagan las necesidades acordadas del negocio.
Item 2	Se utiliza algún formulario en el que se especifique los sistemas y servicios informáticos que tiene acceso los funcionarios.		8.1.3 Uso aceptable de los activos: Se deberían identificar, documentar e implantar regulaciones para el uso adecuado de la información.	
Item 3	Se controla que la información privada y confidencial solo acceda el personal autorizado.		9.2.4 Gestión de información confidencial de autenticación de usuarios: La asignación de información confidencial para la autenticación debería ser controlada mediante un proceso de gestión controlado.	
Item 4	El personal interno encargado de administración del archivo de documentos físicos y el personal que cumple las funciones de administrador de base de datos, programadores, procesos batch, seguridades, han sido evaluados con algún tipo de test de confiabilidad, polígrafo, psicológico.		7.1.1 Investigación de antecedentes: Se deberían realizar revisiones de verificación de antecedentes de los candidatos al empleo en concordancia con las regulaciones, ética y leyes relevantes y deben ser proporcionales a los requerimientos del negocio, la clasificación de la información a la cual se va a tener acceso y los riesgos percibidos.	

[3] Norma de la seguridad física y electrónica (NCSFyE-SEPS- 2018) de la Superintendencia de Economía Popular y Solidaria (2018).

4 Resolución de Riesgo Operativo (JB-2012-2148 –SBS) de la Superintendencia de Bancos SBS (2012).

Nro.	Descripción del ítem	Aspecto a evaluar relacionados con normativas de control (NCSFyE-SEPS-2018).[3] (JB-2012-2148 –SBS)[4]	Relación con la normas ISO 27002 objetivos de control y/o controles	Relación con ITIL (2012)
Item 5	Cuando el usuario final, realiza consultas a información de saldo de socios o clientes; se almacena la consulta en algún archivo o base de datos.	(JB-2012-2148 –SBS) 4.3.8.16 Además, la entidad deberá mantener y monitorear un log de auditoría sobre las consultas realizadas por los funcionarios a la información confidencial de los clientes.		
Item 6	Se registra, protege y monitorea las actividades de los administradores y operadores de los sistemas		12.4.3 Registros de actividad del administrador y operador del sistema: Se deberían registrar las actividades del administrador y del operador del sistema y los registros asociados se deberían proteger y revisar de manera regular.	
Item 7	Se informa a sus superiores en caso de detectar casos de accesos y/o consultas de información confidencial de socios o clientes sin autorización.		12.1.2 Gestión de cambios: Se deberían controlar los cambios que afectan a la seguridad de la información en la organización y procesos de negocio, las instalaciones y sistemas de procesamiento de información.	
Item 8	Se informa a sus superiores en caso de detectarse cambios a las configuraciones de los equipos de computación, redes, sistemas y compartición de credenciales de acceso por parte de los empleados.		7.2.3 Proceso disciplinario: Debería existir un proceso formal disciplinario comunicado a empleados que produzcan brechas en la seguridad.	
Item 9	Para el acceso a los sistemas informáticos se tiene segregado al personal los roles y perfiles Ej. Administradores, supervisores, operativos, consultas.	(JB-2012-2148 –SBS) 4.3.8.12 Asegurar que exista una adecuada segregación de funciones entre el personal que administra, opera, mantiene y en general accede a los dispositivos y sistemas usados en los diferentes canales electrónicos y tarjetas.	9.2.5 Revisión de los derechos de acceso de los usuarios: Los propietarios de los activos deberían revisar con regularidad los derechos de acceso de los usuarios.	
Item 10	Se ha realizado controles como bloqueo de puertos externos, restricción de internet y correo electrónico, restricción de instalación de software, cambio de configuraciones entre otras.			Operación de Servicio, Gestión de Acceso Implementar los procedimientos definidos en la política de seguridad del sistema de información y por
Item 11	Se realiza Control de acceso de paquetes (Packet Filter/Firewall), detección de		9.4.4 Uso de herramientas de administración de sistemas: El uso de utilidades software que podrían	

Nro.	Descripción del ítem	Aspecto a evaluar relacionados con normativas de control (NCSFyE-SEPS-2018).[3] (JB-2012-2148 –SBS)[4]	Relación con la normas ISO 27002 objetivos de control y/o controles	Relación con ITIL (2012)
	intrusos y/o cifrado de comunicaciones.		ser capaces de anular o evitar controles en aplicaciones y sistemas deberían estar restringidos y estrechamente controlados.	las recomendaciones de la gestión de la disponibilidad.
Item 12	Dispone de controles, perímetros de seguridad, y monitoreo de acceso apropiados.	(JB-2012-2148 –SBS) 4.3.11.4 Implementar mecanismos de control, autenticación mutua y monitoreo, que reduzcan la posibilidad de que los clientes accedan a páginas web falsas similares a las propias de las instituciones del sistema financiero.	9.4.2 Procedimientos seguros de inicio de sesión: Cuando sea requerido por la política de control de accesos se debería controlar el acceso a los sistemas y aplicaciones mediante un procedimiento seguro de log-on	Gestionar el acceso a los servicios para los usuarios autorizados es sinónimo de implementar reglas para evitar el acceso de los usuarios no autorizados. Estas reglas también se deben conocer y comunicar a todos.
Item 13	Existe personal encargado de la administración y/o cuidado del archivo físico.		11.1.3 Seguridad de oficinas, despachos y recursos: Se debería diseñar y aplicar un sistema de seguridad física a las oficinas, salas e instalaciones de la organización.	
Item 14	Se utiliza bitácora física o digital de ingreso y salida de documentos, así como de revisión periódica de las mismas por un supervisor.	(NCSFyE-SEPS- 2018), Art. 5.1, Numeral b. Llevar actualizadas las bitacoras de seguridad		
Item 15	Dispone de Seguridad electrónica (Cámaras de vigilancia, sensores de humo, humedad, etc).	(NCSFyE-SEPS- 2018) Art. 7, Numeral a, Contar con sistemas de alarmas contra robo e incendio, enlazados por frecuencia de radio a centrales de monitoreo y respuesta. (NCSFyE-SEPS- 2018) Art. 8, Numeral a, Contar con un número adecuado de cámaras fijas y móviles de circuito cerrado de televisión.		
Item 16	Se toma las acciones de control inmediato a las advertencias o alarmas que emiten los diferentes sensores disponibles.			
Item 17	Cuenta con dispositivos de Identificación de Radio Frecuencia para bibliotecas (RFID) que genere alertas sonoras cuando se intente sacar una carpeta sin autorización.			
Item 18	Se ha sancionado a algún funcionario por no entregar la documentación solicitada del archivo en el tiempo establecido.			Mejora Continua, Gestión de Problemas. Revisar y analizar el resultado de los contratos de servicio (SLA): esta actividad es muy importante, porque va a definir

Nro.	Descripción del ítem	Aspecto a evaluar relacionados con normativas de control (NCSFyE-SEPS-2018).[3] (JB-2012-2148 –SBS)[4]	Relación con la normas ISO 27002 objetivos de control y/o controles	Relación con ITIL (2012)
				todas las acciones de esta fase.
Item 19	Se tiene establecido un procedimiento para el correcto traslado, almacenamiento, distribución, tiempo de permanencia y custodio de las carpetas con documentos de socios y clientes.		11.2.5 Salida de activos fuera de las dependencias de la empresa: Los equipos, la información o el software no se deberían retirar del sitio sin previa autorización.	
Item 20	Se dispone de alguna política que identifique el tiempo de permanencia de los documentos de socios y clientes en el archivo físico.		8.1.4 Devolución de activos: Todos los empleados y usuarios de terceras partes deberían devolver todos los activos de la organización que estén en su posesión/responsabilidad una vez finalizado el acuerdo, contrato de prestación de servicios o actividades relacionadas con su contrato de empleo.	
Item 21	La información que se genera por el sistema informático se respalda conforme se va generando.		12.3.1 Copias de seguridad de la información: Se deberían realizar y pruebas regulares de las copias de la información, del software y de las imágenes del sistema en relación a una política de respaldo (Backup) convenida.	
Item 22	La información que generan los funcionarios a través de software de ofimática se respalda fuera de sus equipos de computación			
Item 23	Dispone de servidores de respaldo de información, o sistemas basado en discos externos, en donde se almacena la información generada por los usuarios			
Item 24	Se realiza control o monitoreo a software o código malicioso que podría generar robo, destrucción, inutilización de la información almacenada.		12.4.2 Protección de los registros de información: Se debería proteger contra posibles alteraciones y accesos no autorizados la información de los registros.	
Item 25	Se mantiene los sistemas operativos, lenguajes de programación, motores de bases de datos, y otros, con las actualizaciones recomendadas por los fabricantes, así también se mantiene en control de las actualizaciones realizadas.			Gestión de los activos de servicio y configuraciones, Componentes software: sistemas operativos, herramientas de copia de seguridad, etc.
Item 26	Los respaldos permanecen en el mismo edificio o en un sitio alterno en otro edificio o ciudad		8.3.3 Soportes físicos en tránsito: Se deberían proteger los medios que contienen información contra acceso no autorizado, mal uso o corrupción durante el transporte fuera de los limites físicos de la organización.	Gestión de los activos de servicio y configuraciones, Componentes software: sistemas operativos, herramientas de
Item 27	Se realizan respaldos de información de usuarios o del			

Nro.	Descripción del ítem	Aspecto a evaluar relacionados con normativas de control (NCSFyE-SEPS-2018).[3] (JB-2012-2148 –SBS)[4]	Relación con la normas ISO 27002 objetivos de control y/o controles	Relación con ITIL (2012)
	sistema en dispositivos basado en la nube.			copia de seguridad, etc
Item 28	Se dispone de procedimientos para probar la integridad y recuperación a través de las copias de seguridad obtenidas.		12.3.1 Copias de seguridad de la información: Se deberían realizar y pruebas regulares de las copias de la información, del software y de las imágenes del sistema en relación a una política de respaldo (Backup) convenida.	
Item 29	Para enviar información a personal externo o de otra institución es obligatorio cifrar la información.		10.1.1 Política de uso de los controles criptográficos: Se debería desarrollar e implementar una política que regule el uso de controles criptográficos para la protección de la información.	
Item 30	Las empresas proveedoras de servicios que tiene acceso a la información del sistema informático, han firmado acuerdos de confidencialidad, se monitorea la actividad que estas realizan.		7.1.2 Términos y condiciones de contratación: como parte de su obligación contractual, empleados, contratistas y terceros deberían aceptar y firmar los términos y condiciones del contrato de empleo, el cual establecerá sus obligaciones y las obligaciones de la organización para la seguridad de información.	
Item 31	Se ha tomado alguna acción legal contra las empresas proveedora de servicios por prácticas no profesionales, revelar información privada, confidencial, o infringir los acuerdos de confidencialidad.			
Item 32	Los test de penetración realizado a objetivos internos y externos revelo alguna brecha de seguridad por la cual se podría fugar la información.	(JB-2012-2148 –SBS) 4.3.11.2 Realizar como mínimo una vez (1) al año una prueba de vulnerabilidad y penetración a los equipos, dispositivos y medios de comunicación utilizados en la ejecución de transacciones por banca electrónica; y, en caso de que se realicen cambios en la plataforma, se deberá efectuar una prueba adicional.		
Item 33	Las verificaciones de seguridad lógica como el “Gap Análisis PCI-DSS”, en relación a manejo de información de tarjetas habientes, revelo alguna vulnerabilidad con respecto al manejo de la información.	(JB-2012-2148 –SBS) 4.3.9.6 Establecer y ejecutar procedimientos de auditoría de seguridad en sus cajeros automáticos por lo menos una vez al año, con el fin de		

Nro.	Descripción del ítem	Aspecto a evaluar relacionados con normativas de control (NCSFyE-SEPS-2018).[3] (JB-2012-2148 –SBS)[4]	Relación con la normas ISO 27002 objetivos de control y/o controles	Relación con ITIL (2012)
Item 34	Cuándo se realiza una auditoría a los sistemas informáticos, se planifica, y acuerdan las actividades de verificación para minimizar las interrupciones a los sistemas informáticos.	identificar vulnerabilidades y mitigar los riesgos que podrían afectar a la seguridad de los servicios que se brindan a través de estos.	12.7.1 Controles de auditoría de los sistemas de información: Se deberían planificar y acordar los requisitos y las actividades de auditoría que involucran la verificación de los sistemas operacionales con el objetivo de minimizar las interrupciones en los procesos relacionados con el negocio.	
Item 35	Las Auditorías informáticas interna o externa, evidenciaron alguna no conformidad sobre fuga de información.	(JB-2012-2148 –SBS) 4.3.8.24 Es función de auditoría interna verificar oportunamente la efectividad de las medidas de seguridad que las instituciones del sistema financiero deben implementar en sus canales electrónicos; así también deberán informar sobre las medidas correctivas establecidas.		
Item 36	Se ha determinado las brechas de seguridad en base a los análisis de riesgo conforme a las recomendaciones de auditorías.			
Item 37	Se dispone de sistemas computacionales de Prevención de Fuga de Información y se monitorea la actividad o alertas generadas.	(JB-2012-2148 –SBS) 4.3.11.5 Implementar mecanismos de seguridad incluyendo dispositivos tales como IDS, IPS, firewalls, entre otros, que reduzcan la posibilidad de que la información de las transaccionesde los clientessea capturada por terceros no autorizados durante la sesión.		
Item 38	Se ha aplicado sanciones por las actividades que advierte el sistema computacional de Prevención de Fuga de Información.		7.2.3 Proceso disciplinario: Debería existir un proceso formal disciplinario comunicado a empleados que produzcan brechas en la seguridad.	

Fuente: SEPS (2018), SBS(2012), ITIL (2012) ISO 27002

Luego de la revisión de los expertos validadores se obtuvo las siguientes observaciones descritos en la Tabla 5.

Tabla N° 5. Observaciones a los instrumentos de investigación realizadas por los expertos.

Experto	Item	Aspecto a evaluar relacionados con la aplicación de normativas de control interno	Observación
Ing. Juan Carlos Rosero.	**ítem 15**: Dispone de seguridad electrónica (Cámaras de vigilancia, sensores de humo, humedad, etc),	En los sitios destinados para archivar los documentos físicos en especial los documentos y carpetas con información de socios y clientes en la Cooperativa.	Indican que en mayor número las organizaciones se ven obligadas por las entidades de control a utilizar estos dispositivo, mantener pregunta.
	ítem 17: Cuenta con dispositivos de Identificación de Radio Frecuencia para bibliotecas (RFID) que genere alertas sonoras cuando se intente sacar una carpeta sin autorización,		Manifiesta: toca analizar la viabilidad de los RFID.
	ítem 18: Se ha sancionado a algún funcionario por no entregar la documentación solicitada del archivo en el tiempo establecido		Observa: no se recomienda preguntar sobre sanciones, pero mantenga la pregunta,
Ing. Patricio Cando.	**ítem 25:** Se mantiene los sistemas operativos, lenguajes de programación, motores de bases de datos, y otros, con las actualizaciones recomendadas por los fabricantes, así también se mantiene en control de las actualizaciones realizadas	"…establecer procedimientos rutinarios para conseguir la estrategia aceptada de respaldo, para realizar copias de seguridad y probar su puntual recuperación, procedimientos de respaldo y recuperación".	Indica que verficar la actualizaciones en un ambiente de pruebas no obstante la pregunta es relevante como esta
	ítem 29: Para enviar información a personal externo o de otra institución es obligatorio cifrar la información		Observa que no es obligatorio pero si recomendable, mantener la pregunta
	item 37: Se dispone de sistemas computacionales de Prevención de Fuga de Información y se monitorea la actividad o alertas generadas.	Los procesos de Auditoría, análisis o test de los sistemas informáticos ayudan a maximizar la efectividad de los sistemas informáticos, procesos, personas, evaluación de riesgos así como identificar vulnerabilidades y generar una cultura de pro actividad frente a las amenazas internas y externas.	Indica que son muy costosos los DLP posiblemente tenga baja calificacion en este ítem.

Fuente Autor.

Los demas expertos no realizan observaciones a los ítems presentados.

ANÁLISIS DE RESULTADOS

Una vez aplicadas las encuestas basadas en las normativas seleccionadas se muestran los siguientes resultados:

Primer aspecto evaluado

Según la ISO 27002, en los controles 7 Seguridad ligada a Recursos Humanos, 8 Gestión de Activos, 9 Control de Acceso y 12 Seguridad en la operatividad, así como los procesos de Diseño de Servicio - Gestión de Seguridad y Operación de Servicio - Gestión de Acceso del Marco de Referencia ITIL, y la

Resolución JB-2012-2148 –SBS, se debe tomar en cuenta que por información se entiende los datos organizados en poder de una entidad, independiente del valor, cómo se guarde o transmite (escrita, en imágenes, oral, impresa, almacenada, proyectada, enviada por correo, fax, e-mail o en conversaciones, etc), sea propia o de fuentes externas y la seguridad de la misma consiste en preservar su confidencialidad, integridad y disponibilidad.

En relación con lo anterior los datos que se gestiona en los sistemas informáticos y la información generada por otros medios en la Cooperativa.

1. Totalmente en desacuerdo, 2. En desacuerdo, 3. indiferente, 4. de acuerdo, 5. Totalmente de acuerdo

Tabla N° 6. Primer aspecto evaluado.

		1	2	3	4	5	
Nro.	**Item**	∑	∑	∑	∑	∑	**Prom**
1	Se cataloga o clasifica la información en pública, privada, confidencial.	1	2	1	4	9	4,06
2	Se utiliza algún formulario en el que se especifique los sistemas y servicios informáticos que tiene acceso los funcionarios.	1	1	1	4	10	4,24
3	Se controla que la información privada y confidencial solo acceda el personal autorizado.	1	1	-	5	9	4,25
4	El personal interno encargado de administración del archivo de documentos físicos y el personal que cumple las funciones de administrador de base de datos, programadores, procesos batch, seguridades, han sido evaluados con algún tipo de test de confiabilidad, polígrafo, psicológico.	3	4	3	4	3	3
5	Cuando el usuario final, realiza consultas a información de saldo de socios o clientes; se almacena la consulta en algún archivo o base de datos.	2	2	3	3	7	3,65
6	Se registra, protege y monitorea las actividades de los administradores y operadores de los sistemas.	2	1	3	6	5	3,65
7	Se informa a sus superiores en caso de detectar casos de accesos y/o consultas de información confidencial de socios o clientes sin autorización.	1	1	1	5	9	4,18
8	Se informa a sus superiores en caso de detectarse cambios a las configuraciones de los equipos de computación, redes, sistemas y compartición de credenciales de acceso por parte de los empleados.	1	-	-	4	12	4,53
9	Para el acceso a los sistemas informáticos se tiene segregado al personal los roles y perfiles Ej. Administradores, supervisores, operativos, consultas.	1	-	1	2	13	4,53
10	Se ha realizado controles como bloqueo de puertos externos, restricción de internet y correo electrónico, restricción de instalación de software, cambio de configuraciones entre otras.	1	-	-	2	14	4,65
11	Se realiza Control de acceso de paquetes (Packet Filter/Firewall), detección de intrusos y/o cifrado de comunicaciones.	1	-	-	5	11	4,47

Fuente: Autor

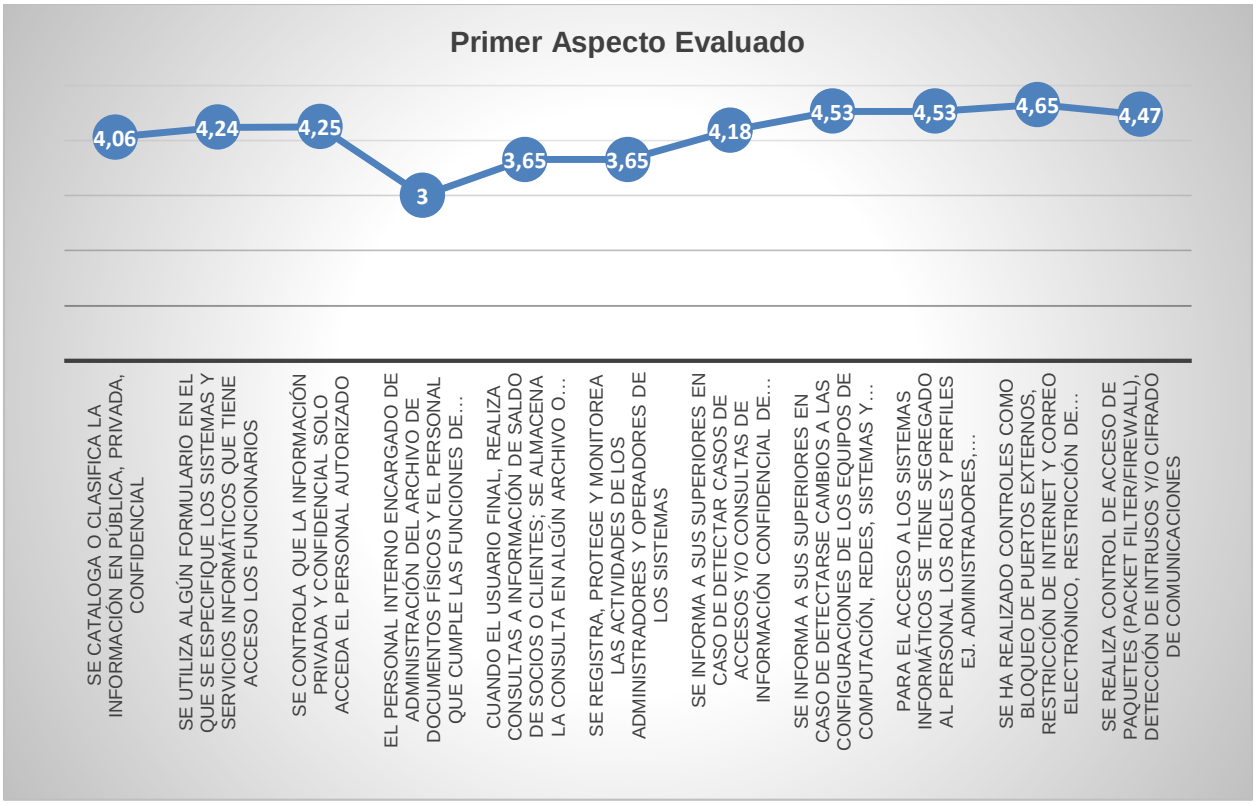

Figura 1. Primer aspecto evaluado
Elaboración: El Autor

Segundo aspecto evaluado

Tomando en cuenta los sistemas de gestión de seguridad de la información de la ISO 27002, en especial los controles 8 Gestión de Activos, 9 Control de Acceso y 11 Seguridad física y ambiental, los procesos Operación de Servicio - Gestión de Acceso, Mejora Continua - Gestión de Problemas del Marco de Referencia ITIL, la Normativa NCSFyE-SEPS- 2018 y Resolución JB-2012-2148 SBS, para el control de la documentación se debe establecer, documentar, implantar y mantener un procedimiento que permita entre otras la aprobación, revisión, identificación, control, distribución, retención, prevenir el uso de documentos obsoletos y evitar la pérdida.

Tomando en cuenta lo anterior, los sitios destinados para archivar los documentos físicos en especial los documentos y carpetas con información de socios y clientes en la Cooperativa cumple con los siguientes controles.

1. Totalmente en desacuerdo, 2. En desacuerdo, 3. indiferente, 4. de acuerdo, 5. Totalmente de acuerdo

Tabla N° 7. Segundo aspecto evaluado.

		1	2	3	4	5	
Nro.	Item	Σ	Σ	Σ	Σ	Σ	Prom
12	Dispone de controles, perímetros de seguridad, y monitoreo de acceso apropiados.	-	2	2	5	7	4,06
13	Existe personal encargado de la administración y/o cuidado del archivo físico.	1	2	-	8	5	3,88
14	Se utiliza bitácora física o digital de ingreso y salida de documentos, así como de revisión periódica de las mismas por un supervisor.	1	3	3	5	4	3,5

15	Dispone de Seguridad electrónica (Cámaras de vigilancia, sensores de humo, humedad, entre otros).	1	-	-	4	10	4,47
16	Se toma las acciones de control inmediato a las advertencias o alarmas que emiten los diferentes sensores disponibles.	1	-	1	5	9	4,31
17	Cuenta con dispositivos de Identificación de Radio Frecuencia para bibliotecas (RFID) que genere alertas sonoras cuando se intente sacar una carpeta sin autorización.	6	4	1	2	3	2,5
18	Se ha sancionado a algún funcionario por no entregar la documentación solicitada del archivo en el tiempo establecido.	-	3	5	5	3	3,5
19	Se tiene establecido un procedimiento para el correcto traslado, almacenamiento, distribución, tiempo de permanencia y custodio de las carpetas con documentos de socios y clientes.	1	3	2	6	3	3,47
20	Se dispone de alguna política que identifique el tiempo de permanencia de los documentos de socios y clientes en el archivo físico.	1	3	2	5	5	3,63

Fuente: Autor

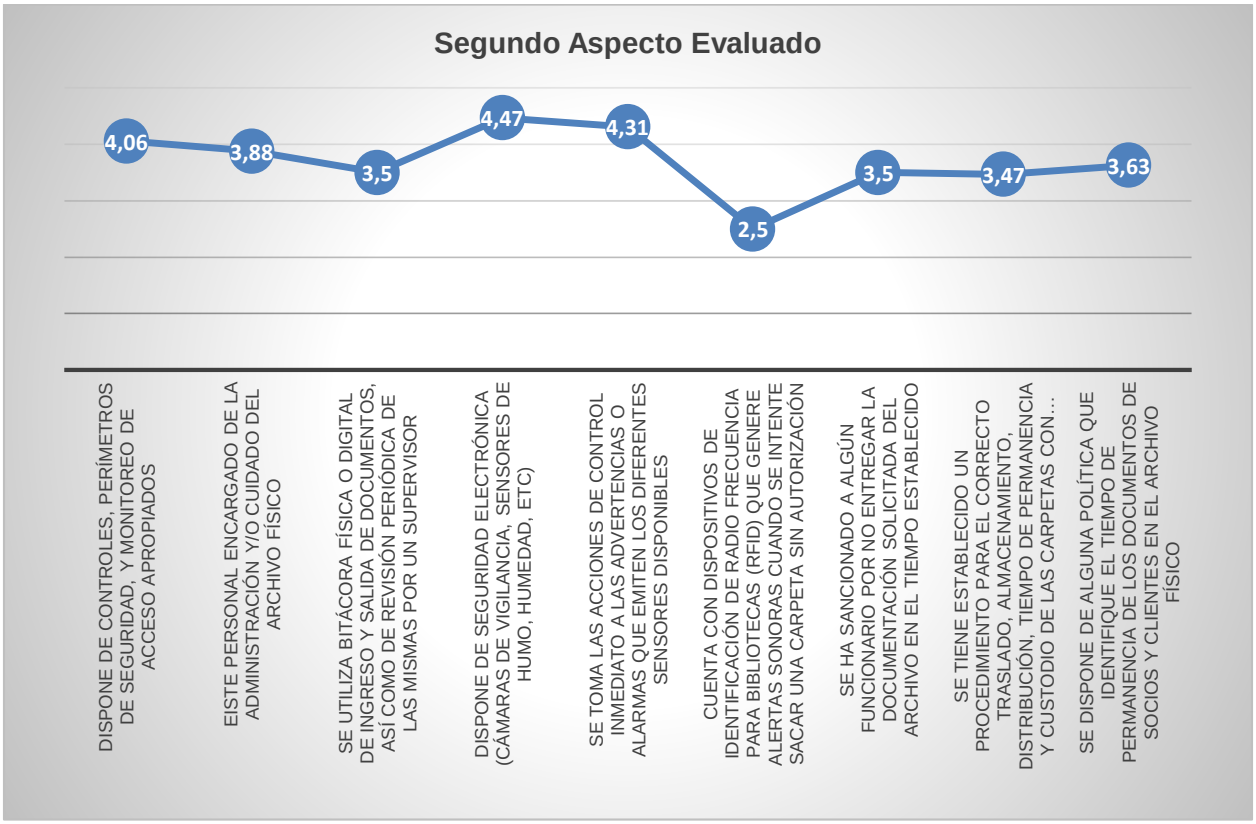

Figura 2. Segundo aspecto evaluado
Elaboración: El Autor

Tercer aspecto evaluado

Según la ISO 27002, dentro de las seguridades en las operaciones se establece el control 12.3 Copias de seguridad, que implica:

> "…establecer procedimientos rutinarios para conseguir la estrategia aceptada de respaldo, para realizar copias de seguridad y probar su puntual recuperación, procedimientos de respaldo y recuperación, determinar estrategia de respaldo y recuperación, el tipo de almacenamiento, soporte a utilizar, frecuencia de copia y prueba de soportes, técnicas de cifrado a copias de seguridad y archivos que contengan datos sensibles o valiosos".

Así también los controles 8 Gestión de Activos, 10 Cifrado y 12 Seguridad en la operatividad, de la ISO 27002 y el proceso Gestión de los activos de servicio y configuraciones del Marco de Referencia ITIL.

De acuerdo al criterio antes mencionado, para el respaldo de información digital en la Cooperativa se realiza las siguientes acciones.

1. Totalmente en desacuerdo, 2. En desacuerdo, 3. indiferente, 4. de acuerdo, 5. Totalmente de acuerdo

Tabla N° 8. Tercer aspecto evaluado.

		1	2	3	4	5	
Nro.	**Item**	∑	∑	∑	∑	∑	**Prom**
21	La información que se genera por el sistema informático se respalda conforme se va generando.	1	-	-	6	9	4,38
22	La información que generan los funcionarios a través de software de ofimática se respalda fuera de sus equipos de computación.	1	3	1	3	8	3,88
23	Dispone de servidores de respaldo de información, o sistemas basado en discos externos, en donde se almacena la información generada por los usuarios.	1	-	1	4	10	4,38
24	Se realiza control o monitoreo a software o código malicioso que podría generar robo, destrucción, inutilización de la información almacenada.	-	1	2	5	8	4,25
25	Se mantiene los sistemas operativos, lenguajes de programación, motores de bases de datos, y otros, con las actualizaciones recomendadas por los fabricantes, así también se mantiene en control de las actualizaciones realizadas.	-	2	4	3	7	3,94
26	Los respaldos permanecen en el mismo edificio o en un sitio alterno en otro edificio o ciudad.	1	-	-	5	10	4,44
27	Se realizan respaldos de información de usuarios o del sistema en dispositivos basado en la nube.	4	2	6	1	3	2,81
28	Se dispone de procedimientos para probar la integridad y recuperación a través de las copias de seguridad obtenidas.	1	-	4	6	5	3,88
29	Para enviar información a personal externo o de otra institución es obligatorio cifrar la información.	1	3	1	7	3	3,53

Fuente Autor.

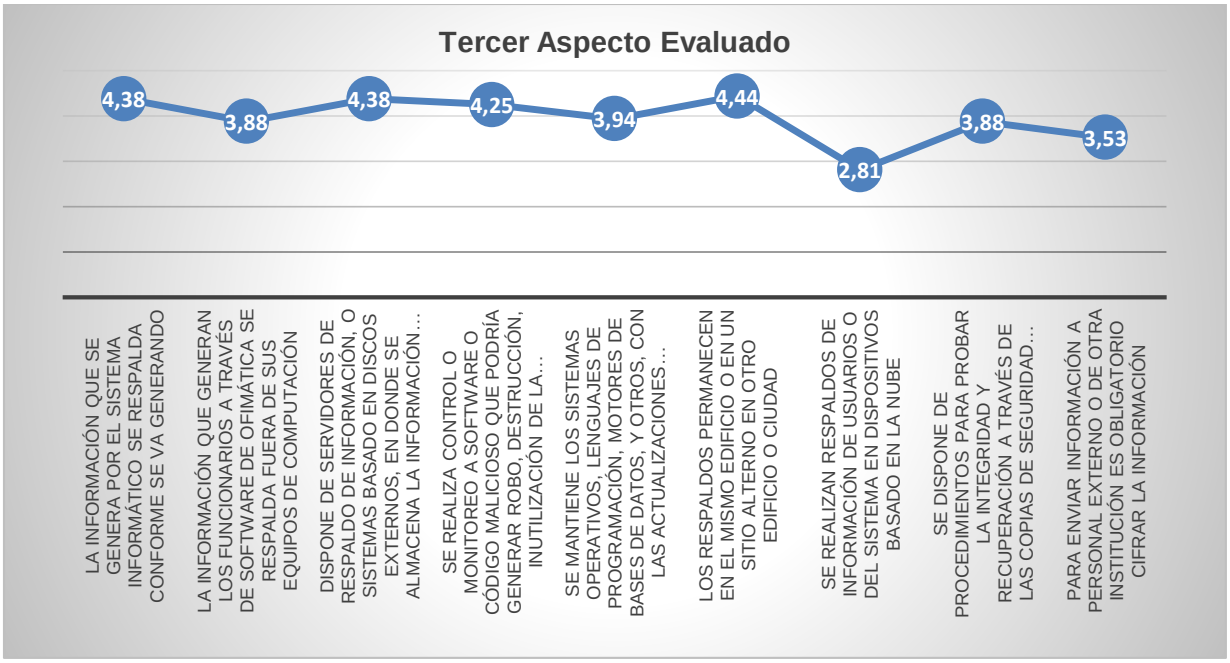

Figura 3. Tercer aspecto evaluado
Elaboración: El Autor

Cuarto aspecto evaluado

Como la Resolución JB-2012-2148 de la SBS y los controles en los controles 7 Seguridad ligada a Recursos Humanos y 12 Seguridad en la operativida los procesos de Auditoría de la ISO 27002, los análisis o test de los sistemas informáticos ayudan a maximizar la efectividad de los sistemas informáticos, procesos, personas, evaluación de riesgos así como identificar vulnerabilidades y generar una cultura de pro actividad frente a las amenazas internas y externas.

Así también existe la limitación y acuerdos con proveedores para el acceso a los sistemas y servicios informáticos.

En relación a las revisiones internas y/o externas realizadas en la Cooperativa se realiza.

1. Totalmente en desacuerdo, 2. En desacuerdo, 3. indiferente, 4. de acuerdo, 5. Totalmente de acuerdo

Tabla N° 9. Cuarto aspecto evaluado.

		1	2	3	4	5	
Nro.	**Item**	∑	∑	∑	∑	∑	**Prom**
30	Las empresas proveedora de servicios que tiene acceso a la información del sistema informático, han firmado acuerdos de confidencialidad, se monitorea la actividad que estas realizan.	-	2	3	3	8	4,06
31	Se ha tomado alguna acción legal contra las empresas proveedora de servicios por prácticas no profesionales, revelar información privada, confidencial, o infringir los acuerdos de confidencialidad.	3	4	4	2	3	2,88
32	Los Test de Penetración realizado a objetivos internos y externos revelo alguna brecha de seguridad por la cual se podría fugar la información.	-	3	4	5	3	3,53
33	Las verificaciones de seguridad lógica como el “Gap Análisis PCI-DSS”, en relación a manejo de información de tarjetas habientes, revelo alguna vulnerabilidad con respecto al manejo de la información.	2	5	2	4	3	3,06
34	Cuándo se realiza una auditoría a los sistemas informáticos, se planifica, y acuerdan las actividades de verificación para minimizar las interrupciones a los sistemas informáticos.	1	-	-	7	8	4,31
35	Las Auditorías informáticas interna o externa, evidenciaron alguna no conformidad sobre fuga de información.	1	5	5	2	3	3,06

36	Se ha determinado las brechas de seguridad en base a los análisis de riesgo conforme a las recomendaciones de auditorías.	-	3	1	8	4	3,81
37	Se dispone de sistemas computacionales de Prevención de Fuga de Información y se monitorea la actividad o alertas generadas.	1	3	3	4	5	3,56
38	Se ha aplicado sanciones por las actividades que advierte el sistema computacional de Prevención de Fuga de Información.	4	2	4	2	4	3

Fuente Autor.

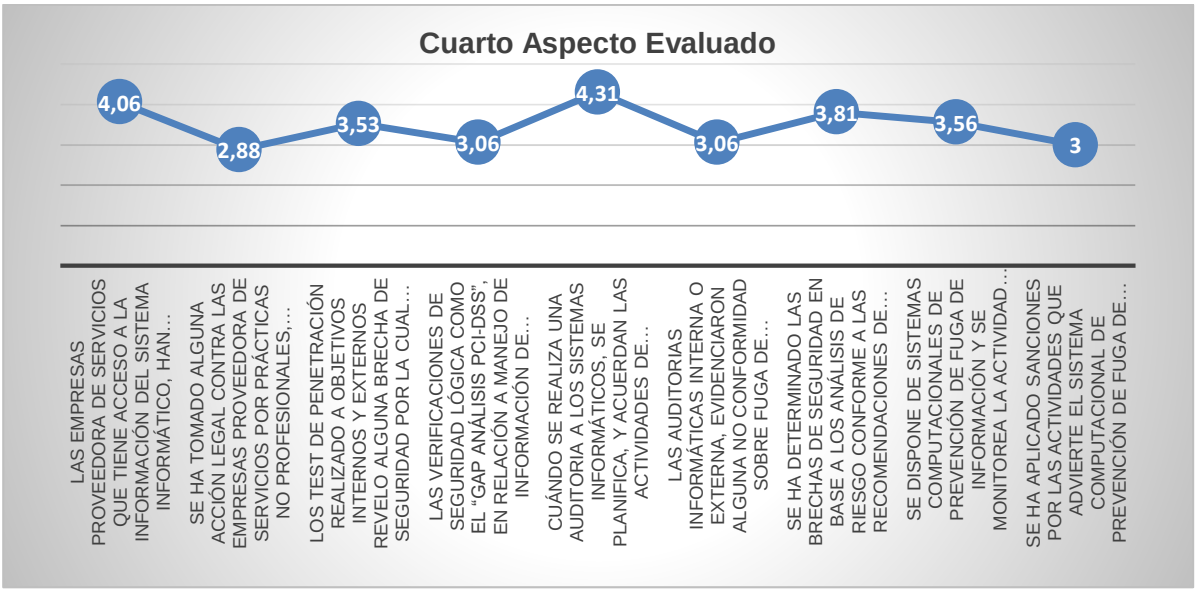

Figura 4. Cuarto aspecto evaluado
Elaboración: El Autor

Para obtener el promedio en cada ítem se suman todas las respuestas de acuerdo a la escala de Lickert seleccionada y se divide para el número de respuestas obtenidas. Como ejemplo se explica cómo se obtuvo el promedio de 4,06 en el primer ítem se cataloga o clasifica la información en pública, privada, confidencial que se muestra en la Tabla Nro 5, se observa los siguientes resultados:

Opción seleccionada	1	2	3	4	5
# personas que seleccionan opción	1	2	1	4	9

Es decir se obtiene un 1, dos 2, un 3, cuatro 4 y nueve 5, sumando estos resultados se obtiene un total de 69 este resultado se divide para el número de respuestas 17 dando como promedio 4,06

Con la información que se gestiona en los sistemas informáticos y la información generada por otros medios en la Cooperativa los siguientes ítems tienen valoraciones bajas específicamente:

- El personal interno encargado de administración del archivo de documentos físicos y el personal que cumple las funciones de administrador de base de datos, programadores, procesos batch, seguridades, han sido evaluados con algún tipo de test de confiabilidad, polígrafo, psicológico; con un promedio de 3 sobre 5 lo que es preocupante en razón que no se puede garantizar al cien por ciento que el personal encargado de proceso críticos para la empresa sea confiable.

- Cuando el usuario final, realiza consultas a información de saldo de socios o clientes; se almacena la consulta en algún archivo o base de datos, en este caso con un promedio de 3,65 sobre 5, indica que el personal no

está seguro que las consultas sobre información de socios sean almacenadas en algún archivo del sistema a pesar de ser un tema normativo

- Se registra, protege y monitorea las actividades de los administradores y operadores de los sistemas; de igual forma con un promedio de 3,65 sobre 5, no se conoce por parte del personal que las actividades que realizan sobre el sistema esté siendo monitoreadas.

Los sitios destinados para archivar los documentos físicos en especial los documentos y carpetas con información de socios y clientes en la Cooperativa los siguientes Ítems tienen valoraciones bajas específicamente:

- Se utiliza bitácora física o digital de ingreso y salida de documentos, así como de revisión periódica de las mismas por un supervisor; con un promedio de 3,5 sobre 5 este aspecto demuestra que no se lleva el registro adecuado o falta de control a los mismos, lo que podría ocasionar pérdida de información de los socios y clientes de la Cooperativa.

- Cuenta con dispositivos de Identificación de Radio Frecuencia para bibliotecas (RFID) que genere alertas sonoras cuando se intente sacar una carpeta sin autorización; este aspecto tiene un promedio de 2,5 sobre 5 es decir que se desconoce del tema o no se dispone de estos dispositivos de alerta sobre sustracción de documentación

- Se ha sancionado a algún funcionario por no entregar la documentación solicitada del archivo en el tiempo establecido; al tener un promedio de 3,5 sobre 5, se deduce que en algún momento ya se sancionó a algún o algunos funcionarios por no entregar la documentación solicitada de los archivos institucionales.

- Se tiene establecido un procedimiento para el correcto traslado, almacenamiento, distribución, tiempo de permanencia y custodio de las carpetas con documentos de socios y clientes; al tener un promedio 3,47 sobre 5 en este aspecto indica que puede existir el procedimiento para el traslado, almacenamiento, distribución, pero posiblemente no se aplique correctamente dicho procedimiento tal como se encuentre establecido.

- Se dispone de alguna política que identifique el tiempo de permanencia de los documentos de socios y clientes en el archivo físico, con el promedio de 3,63 sobre 5, este aspecto indica que se dispone de la política que indique que tiempo los documentos de socios y clientes se los debe mantener físicamente en los archivos institucionales.

El respaldo de información digital en la Cooperativa se analiza los siguientes Ítems tanto con valoraciones bajas específicamente:

- Se realizan respaldos de información de usuarios o del sistema en dispositivos basado en la nube con un promedio de 2,81 sobre 5, indica que el personal no está de acuerdo con esta afirmación es decir que no se utiliza este tipo de tecnología para resguardar la información.

- Para enviar información al personal externo o de otra institución es obligatorio cifrar la información con un promedio de 3,53 sobre 5 este porcentaje indica que no toda la información que el personal envía no se lo hace de forma cifrada y en caso de que información pueda caer en manos equivocadas esta pueda ser interpretada o leída con facilidad.

- De forma positiva se tiene que la información que se genera por el sistema informático se respalda conforme se va generando con un promedio de 4,38 sobre 5, indica que se aplica una buena práctica como es que la información siempre se va respaldando en cualquier medio.

Las revisiones de auditorías informáticas ya sean internas o externas en la Cooperativa así como la interacción que se realiza como proveedores

de servicios informáticos se analizan los siguientes Ítems en especial los que tienen valoraciones bajas:

- Se ha tomado alguna acción legal contra las empresas proveedora de servicios por prácticas no profesionales, revelar información privada, confidencial, o infringir los acuerdos de confidencialidad con un promedio de 2,88 sobre 5, indica que no se ha tomado acciones legales en contra de proveedores o profesionales por prácticas no profesionales o no se han dado ese tipo de casos.

- Las verificaciones de seguridad lógica como el "Gap Análisis PCI-DSS", en relación a manejo de información de tarjetas habientes, revelo alguna vulnerabilidad con respecto al manejo de la información tiene un promedio de 3.06 sobre 5, indica que puede haber revelado algún tipo de vulnerabilidad referente a la información de tarjeta habientes

- Se ha aplicado sanciones por las actividades que advierte el sistema computacional de Prevención de Fuga de Información. al tener un promedio de 3 sobre 5, puede ser que no se dispone de un sistema computacional especializado para prevenir la fuga de información.

Tomando como base los resultados de los cuatro aspectos evaluados los cuales contiene cada uno diferentes afirmaciones se dispone de suministros necesarios para realizar la recopilación de buenas prácticas de seguridad para mitigar la fuga de información, conjuntamente con las recomendaciones a llevarse a cabo en el corto o mediano plazo aplicable a las Cooperativa de Ahorro y Crédito participantes.

CONCLUSIONES

Con la investigación realizada al personal de las áreas de Tecnología, Sistemas, Seguridades y Operaciones de las Cooperativas de Ahorro y Crédito que tienen sus oficinas matrices en la zona 1 del Ecuador, se analizaron cuatro aspectos relacionados a medir el nivel de seguridades implementadas para evitar la fuga de información basadas en normativas como la ISO 27002, la Norma de control respecto de la seguridad física y electrónica (NCSFyE-SEPS-2018) de la Superintendencia de Economia Popular y Solidaria SEPS (2018), la Resolución de Riesgo Operativo (JB-2012-2148–SBS) de la Superintendencia de Bancos SBS (2012) y los procesos Diseño de Servicio - Gestión de Seguridad, Operación de Servicio - Gestión de Acceso, Mejora Continua - Gestión de Problemas, Gestión de los activos de servicio y configuraciones del Marco de Referencia ITIL.

Luego del análisis en cada aspecto se concluye lo siguiente:

Primer aspecto, el tratamiento y protección que se da a la información que se gestiona en los sistemas informáticos, no se garantiza la confianza en el personal encargado de administrar el archivo de documentos físicos, administrador de base de datos, programadores, procesos batch, seguridades, dado que no se aplicado un test de confiabilidad, así también no se está seguro que las consultas realizadas por cualquier usuario a los saldos de socios y clientes se almacenen en un archivo para su revisión y control de auditoria y están cien por ciento seguros que sean monitoreadas las actividades de administradores y operadores de los sistemas en especial al acceder a las bases de datos.

Segundo aspecto los controles en los sitios destinados para archivar los documentos físicos de información de socios y clientes, puede existir casos de pérdida de información de socios o clientes dado que no se lleva el registro adecuado o falta de control a los mismos, así también la salida de documentación física del archivo puede realizarse sin inconvenientes debido a que no se cuenta con dispositivos que generen alarmas sonoras y existen escasos controles por parte de los responsables de los archivos físicos o sus procesos no se están

aplicando de forma adecuada, no se ha aplicado sanciones a los funcionarios por no entregar la documentación física al archivo en el tiempo establecido.

Tercer aspecto seguridades al respaldo de información digital, al momento de realizar las encuestas no se contaba con sistemas de respaldo de la información de equipos informáticos del personal, se realiza de forma individual y manualmente, así también cuando se comparte información con otras entidades no toda la información se envía cifrada, si se realiza el respaldo diario de la data en dispositivos externos.

Cuarto aspecto lo relacionado a revisiones de auditorías informáticas y la interacción con proveedores de servicios informáticos, no se ha dado casos o no se han tomado acciones legales en contra de proveedores de servicios informáticos por revelar información privada, confidencial, o infringir los acuerdos de confidencialidad, así también verificaciones de seguridad informática externa ha revelado vulnerabilidades referente a la información de tarjeta habientes.

También se determinó que el personal profesional asignado para los departamentos de Tecnología, Sistemas, Seguridades es insuficiente para las tareas que se realiza, en algunos casos el personal tiene múltiples funciones adicionales, haciendo que la implementación, control, capacitación y validación de políticas y cumplimiento normativo referente a la fuga de información no sea realizada con la importancia que esta se merece.

Tomando en cuenta que el cumplimiento de todos los ítems de la encuesta en un promedio de 5/5 determina el estado ideal referente al nivel de seguridades para prevenir la fuga de información, de acuerdo a los resultados obtenidos se determina que el nivel de cumplimiento el promedio en cada aspecto es el siguiente: primero 4.11, segundo 3.70, tercero 3.94, y cuarto 3,47 de forma general el nivel de aplicación de seguridades es de 3,80 sobre 5.

El presente paper tuvo algunas limitaciones, el estudio se realizó en dos Cooperativas financieras grandes ubicadas en la Zona 1 del Ecuador debido a la ubicación geográfica de las mismas, no se aplicó los instrumentos a los usuarios finales u oficinistas ya que se requería el criterio del personal dependiente de Sistemas, Tecnología, Seguridades y por razones de seguridad no se pudo acceder a los centros de datos o sistemas informáticos para verificar la existencia de herramientas tecnológicas que prevengan la fuga de información.

Se recomienda, realizar pruebas de concepto con proveedores de tecnología para gestionar la seguridad informática con herramientas tecnológicas de prevención de fuga de información DLP como medidas proactivas y de ser factible realizar su implementación.

Así como se puede implementar hardware, también se puede desarrollar aplicaciones específicas como complemento que permitan determinar los factores de comportamiento de los usuarios y determinar el tipo de información y los medios electrónicos por los que se fuga la información.

Al tener la información referente al nivel de aplicación de medidas de seguridad para evitar la fuga de información se establecerá los criterios para la mitigación y/o cumplimiento normativo con las recomendaciones y actividades a llevarse a corto, mediano y largo plazo.

Como trabajos futuros se puede realizar estudios y experimentación con el uso de hardware y software de prevención de fuga de información y contrastar la información proporcionada a través de las encuestas con los resultados de los experimentos. Así también queda abierta la posibilidad de futuros estudios referentes a cumplimiento normativos y aplicación de buenas prácticas en las instituciones participantes y ser referente en las demás Cooperativas de Ahorro y Crédito de las diferentes zonas de planificación ecuatoriana.

Puede aplicarse esta investigación en otro tipo de organizaciones diferentes a las financieras, sean

estas públicas o privadas y medir el nivel de seguridades implementadas para prevenir la fuga de información.

Referencias Bibliográficas

Aumatell, C. (2013). *Auditoría de la información identificar y explotar la información de las organizaciones.* Barcelona, España: Editorial UOC.

Arcilla-Cobián, M., San Feliu, T., Feliz, A,. Calvo-Manzano, J. (2017). Implementación de una biblioteca de activos de proceso orientada a la gestión de la capacidad de servicios de TI. *International Journal of Information Systems and Software Engineering for Big Companies* (IJISEBC), 4(2), 43-51.

Beltrán. J., Pineda, A., y Quevedo, A. (2016). *Análisis de los riesgos que causan la fuga de información en la empresa Asesorías Contables y Revisoría Fiscal JAA SAS.* (tesis de especialización). Universidad Católica, Bogotá, Colombia.

Bon J. (2010), *Fundamentos de ITIL V3.* Holanda, Editorial Van Haren Publishing

Bortnik, S. (2010). ¿Qué es la fuga de información? Recuperado de: https://www.welivesecurity.com/la-es/2010/04/13/que-es-la-fuga-de-informacion/.

Bowen, Salem, Hershkop, Keromytis y Stolfo (2009), Designing Host and Network Sensors to Mitigate the Insider Threat. Recuperado de: https://ieeexplore.ieee.org/document/5210091

Blasco J. (2012). *Information Leakage and Steganography: Detecting and Blocking Covert Channels.* (tesis doctoral). Unversidad Carlos III, Madrid, España. Recuperado de: https://e-archivo.uc3m.es/bitstream/handle/10016/15506/tesis_jorge_blasco_alis_Resumen.pdf

Burgos Salazar, J., y Campos, P. (2008). Modelo Para Seguridad de la Información en TIC. Recuperado de: http://ceur-ws.org/Vol-488/paper13.pdf.

Cabrales, L. (2015). La fuga de información, el mayor riesgo para la reputación corporativa. Recuperado de: http://unimilitar-dspace.metabiblioteca.org/bitstream/10654/6336/1/CabralesDuranLuisaCristina2015.pdf

Caldana, D., Correa, R., y Ponce, H. (2007). Competencias de los auditores gubernamentales chilenos para la obtención de evidencia electrónica de auditoría. Recuperado de: http://www.scielo.org.mx/pdf/cya/n22/n223a2.pdf

Castro, M. (2017). Control del correo electrónico del trabajador: una mirada desde los derechos humanos. Recuperado de: http://cspabogados.com.ar/control-del-correo-electronico-del-trabajador/.

Castrillon, M. y Lezcano, M. (2012). *Metodología para prevenir la fuga de información aplicando un sistemas DLP en las empresas del sector financiero*. (tesis de especilización). Universidad San Buena Aventura, Medellín, Colombia. Recuperado de: https://bibliotecadigital.usb.edu.co/bitstream/10819/1607/1/Metodologia_Fuga_Informacion_Castrillon_2013.pdf

Check Point (2015). Reporte de Seguridad 2015. Recuperado de: http://ipesa.com/doc/CheckPoint-2015-SecurityReport_Espanol.pdf

Dávila, L. y Pacheco, L (2017). Evaluación de riesgos: Estudio de la fuga de datos en los sitios web del Ecuador. *Pro sciences: revista de producción, ciencias e*

*investigació*n, e-issn: 2588-1000, vol. 1, n 2, septiembre 2017, pp. 15-20. Recuperado de: http://journalprosciences.com/index.php/ps/article/view/11/23

Díaz, D. y Ramírez, M. (2015). *Inventario y clasificación de activos de la información de la empresa Xperia Technologycredit para fortalecer los procesos y procedimientos asociadas a la tecnología Data Loss Prevention – DLP*. (tesis de especilización). Universidad Piloto de Colombia, Bogota, Colombia.

Ernst y Young (2012). Prevención de Fugas de Información Soluciones DLP – un enfoque para el negocio. *Isaca Capitulo Monterrey*. Recuperado de: https://www.isaca.org/chapters7/Monterrey/Events/Documents/20121025%20Preveci%C3%B3n%20de%20Fuga%20de%20Datos.pdf

Ekran System (2015). Ekran System Help File. Recuperado de: https://www.ekransystem.com/sites/default/files/file_resources/Ekran_help_1.pdf

Fernández, F. (2017). La mediación electrónica, la confidencialidad y la protección de datos de carácter personal. Recuperado de: https://www.raco.cat/index.php/InDret/article/download/290026/378336

García, M., Lirola, E. y Mato, V. (2017). La transformación digital de la distribución comercial: la tienda física, de caja brick and mortar a nodo omnicanal.

Guevara, C. (2017). *Desarrollo de algoritmos eficientes para identificación de usuarios en accesos informáticos* (tesis doctoral). Universidad Complutense de Madrid, Madrid, España. Recuperado de: http://eprints.ucm.es/46037/1/T39510.pdf

Hernández Arias, A. (2010). Auditoría Informática y Gestión de Tecnologías De Información y Comunicación (TICs).*Compendium, 13* (25), 3-4.

Itil. (2009). Information Technology Infraestructure Library. Recuperado de: http://www.grupojanus.com/GJ1514/index.php?option=c

Jasso, L. (2017). Seguridad nacional, inteligencia militar y acceso a la información en México. *URVIO, Revista Latinoamericana de Estudios de Seguridad* No. 21 - Quito, diciembre 2017 - pp.140-156. Recuperado de: http://revistas.flacsoandes.edu.ec/urvio/article/view/2931/2023

Kumar, A. (2013). Comparative evaluation of algorithms for effective data leakage detection. Information & Communication Technologies (ICT), 2013 IEEE Conference on IEEE.

McAfee (2015). Informe de McAfee Labs sobre amenazas. Recuperado de: http://www.ebankingnews.com/wp-content/uploads/2015/03/Informe-McAfee-Labs.pdf.

Martelo, R. Tovar, L. y Maza, D. (2017), Modelo Básico de Seguridad Lógica. Caso de Estudio: el Laboratorio de Redes de la Universidad de Cartagena en Colombia. Recuperado de: https://scielo.conicyt.cl/pdf/infotec/v29n1/0718-0764-infotec-29-01-00003.pdf

Moreno, E., Ramírez, C. y Salazar, M. (2018). El derecho de acceso a información pública como mecanismo de control social: Análisis comparado en cinco países latinoamericanos. Gobernar: *The Journal of Latin American Public Policy and Governance* Volume 2 Issue 1 Open state, public governance controls and accountability.

Oliver Vilella, G., y Pérez Cruz, E. (2017). *La confidencialidad*. Recuperado de http://www.uprc.edu/wp-content/uploads/sites/20/2017/04/La-confidencialidad.pdf

Peltier, T. (2005). *Information Security Risk Analysis.* New York, EE UU*:* Editorial AuerBatch.

Polanco, C. y Castañon, A. (2015). Cadenas de Markov un vistazo al futuro, Revista cultural de nuestra América.

Proctor, Mogull, & Oullet. (2007). Magic Quadrant for Content Monitoring and Filtering and Data Loss Prevention, Gartner Inc. Gartner Inc.

Sophos. (2018). Sophos UTM Home Edition. Recuperado de: https://www.sophos.com/es-es/products/free-tools/sophos-utm-home-edition.aspx.

Stenta, H., Rentería, J., y Riccardi, G. (2005). Plataforma computacional para gestion de información en la simulación hidrológica-hidraulica del escurrimiento superficial. Recuperado de: http://www.fceia.unr.edu.ar/curiham/Publicaciones/cna%202005_%20stenta%20renteria%20riccardi.pdf.

Superintendencia de Bancos (2012), resolución JB-2012-2148. Recuperado de: http://oidprd.sbs.gob.ec/medios/PORTALDOCS/downloads/normativa/2012/resol_JB-2012-2148.pdf

Superintendencia de Economía Popular y Solidaria. (2017). Productos estadisticos. Quito, Pichincha, Ecuador: Recuperado de: http://www.seps.gob.ec/estadistica?captaciones-y-colocaciones.

Superintendencia de Economía Popular y Solidaria. (2018). Norma de control respecto ala seguridad física y electrónica. Recuperado de: http://www.seps.gob.ec/documents/20181/25522/SEPS-IGT-IR-IGJ-2018-021.pdf/551765bf-a84b-44d6-b05f-986757f0066e

Teijeira, P. (2010). Proteccion de datos. Obtenido de ¿Conoces las 5 principales vías de fuga de información? Cómo cumplir con la LOPD. Recuperado de: https://pabloteijeira.wordpress.com/2010/06/02/%C2%BFconoces-las-5-principales-vias-de-fuga-de-informacion-como-cumplir-con-la-lopd/.

Urrutia, M., Barrios, S., Gutiérrez, M., y Mayorga Camus, M. (2014). Métodos óptimos para determinar validez de contenido. Recuperado de: http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S0864-21412014000300014.

Voutssas, J. (2012). Preservación documental digital y seguridad informática. Recuperado de: http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S0187-358X2010000100008.

Yandún, M. (2016). *Curso virtual sobre prevención de fuga de información lógica usando herramientas de autor* (tesis de maestría). Universidad Tecnologica Israel, Quito, Ecuador.

Zábala, M. (18 de marzo de 2018). *Resultó inocente frente al "robo del siglo", pero fallo para repararlo no aparece*: Recuperado de: http://www.elespectador.com/noticias/judicial/el-robo-del-siglo-no-alcanzo