XXV ASAMBLEA GENERAL OLACEFS SANTIAGO DE QUERÉTARO, MÉXICO

PONENCIA BASE

TEMA TÉCNICO II: LA IMPORTANCIA DEL USO DE BASE DE DATOS Y DE LA SEGURIDAD DE LA INFORMACIÓN PARA EL FORTALECIMIENTO DE LAS TIC Y PARA EL EJERCICIO EFICIENTE DEL CONTROL FISCAL

NOVIEMBRE 23 AL 27 DE 2015

Dada la gran variedad de amenazas que surgen cada día con el uso de las tecnologías de la Información y de las telecomunicaciones TIC, el acceso a internet y el comercio electrónico, la preocupación por la seguridad de la información se ha incrementado durante los últimos años y es así como diferentes organizaciones, instituciones de normalización, entidades gubernamentales y profesionales de diferentes áreas, han trabajado en la creación y actualización de estándares y mejores prácticas para la seguridad de la información.

Las entidades poseen diversa información que debe ser protegida, teniendo en cuenta los riesgos a los que está expuesta, en los diferentes espacios y momentos en la que ésta se gestiona.

Es importante para las entidades adelantar el establecimiento de sistemas de seguridad de la información que les permitan manejar los riesgos identificados para proteger los datos personales, manejar la reserva y realizar una gestión segura de la tecnología como elementos importantes en la protección de la relación del Estado con sus ciudadanos y de las entidades estatales entre sí.

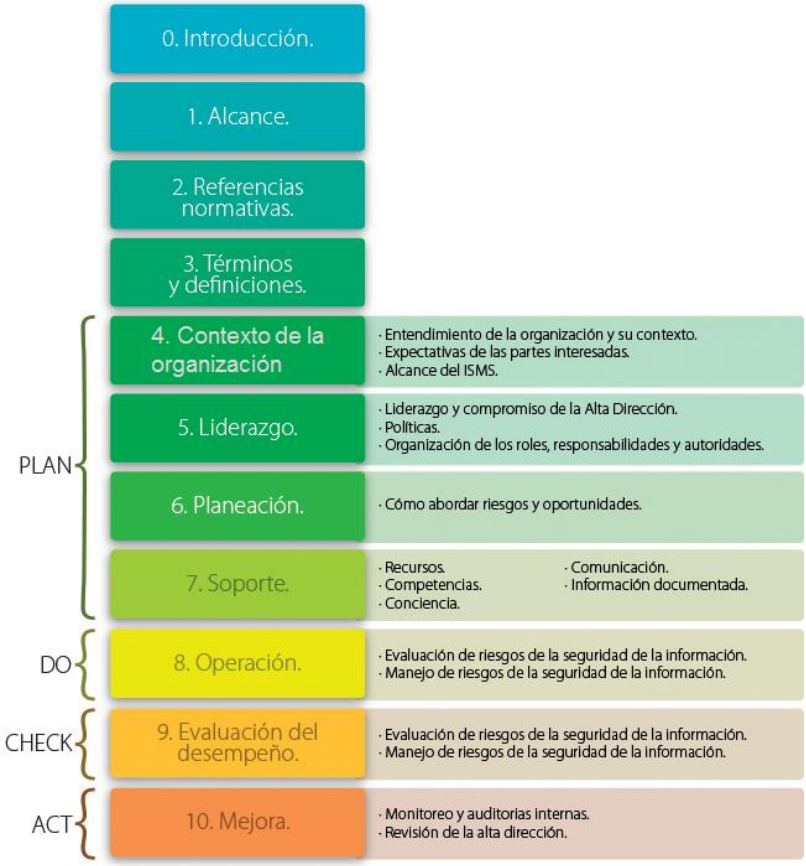
Un importante aporte en este sentido lo ha dado la familia de Normas ISO/IEC 27000 o Normas ISO 27000 que comprende la familia de estándares de ISO (International Organization for Standardization) e IEC (International Electrotechnical Commission) que proporcionan un marco para la creación del sistema de gestión de la seguridad de la información (SGSI) y un conjunto de normas que especifican los requisitos para establecer, implantar, poner en funcionamiento, controlar, revisar, mantener y mejorar el SGSI.

Dentro de estas normas ya desarrolladas y publicadas están la ISO/IEC 27000 que define el vocabulario estándar, conceptos y términos empleados en la familia 27000, la ISO/IEC 27001 que especifica los requisitos para implantar un SGSI certificable conforme a las normas 27000 y define cómo es, cómo se gestiona y cuáles son las responsabilidades; con puntos clave como gestión de riesgos y mejora continua; y la ISO/IEC 27002:

compilación de buenas prácticas para la gestión de la seguridad con recomendaciones sobre qué medidas aplicar para asegurar los sistemas de información de una organización, descripción de los objetivos de control (aspectos a analizar para garantizar la seguridad de la información) y detalla los controles recomendables a implantar (medidas a tomar).

Esta norma fue actualizada al nuevo estándar ISO/IEC 27001:2013, que sirve de guía para la implementación de los controles de seguridad de la organización y de las prácticas más efectivas para gestionar la seguridad de la información y en donde las categorías de los controles definidos se han mezclado, buscando que los dominios de control tengan una estructura más coherente.

[1]. Estructura del estándar ISO/IEC 27001:2013



Fuente: Magazcitum, el Magazine para los profesionales de la Seguridad de TI
http://www.magazcitum.com.mx/?p=2397#.Vgw3GkVZicw

[1] Estructura del estándar ISO/IEC 27001:2013, http://www.magazcitum.com.mx/?p=2397#.Vgw3GkVZicw

El objetivo de la ISO/IEC 27001:2013 Dominios Anexo “A” complementa la definición de los dominios de control especificada en la ISO 27001:2005 para los aspectos prácticos y operativos de la implantación del SGSI, “las principales modificaciones se ven reflejadas en la estructura y el contenido de los controles que conforman el Anexo “A”, donde el número total de dominios era de 11 y ahora son 14 y se reduce el número de controles de 133 a 113, todo como resultado de un proceso de fusión, exclusión e incorporación de nuevos controles de seguridad.” [2]

Figura 2. Dominios Anexo “A” de ISO 27001:2013

Fuente: Magazcitum, el Magazine para los profesionales de la Seguridad de TI
http://www.magazcitum.com.mx/?p=2397#.Vgw3GkVZicw

Las organizaciones en general y en particular las Entidades Fiscalizadoras Superiores – EFS para realizar el ejercicio eficiente del control fiscal y basados en las normas y buenas prácticas de seguridad de la información, se encuentran en proceso de buscar un equilibrio entre el nivel de seguridad adecuado para cada una y el costo / beneficio, el cual plantea dos preguntas importantes

[2] Dominios Anexo “A” Objetivos de Control ISO 27001: 2013 http://www.magazcitum.com.mx/?p=2397#.Vgw3GkVZicw

¿Cuáles son los controles adecuados y necesarios que las Entidades Fiscalizadoras Superiores - EFS pueden implementar en su infraestructura de TI, que pueda ofrecer una seguridad en su información tanto a nivel interno como externo?

¿En qué momento las EFS pueden tener la suficiente confianza que ha aplicado los controles pertinentes a su información?

Para las organizaciones en general, la seguridad de la información es primordial; y para abordar este componente es importante que se vea no solo desde la perspectiva del cumplimiento, sino que se debe buscar un enfoque de ***seguridad integrado*** el cual busca ser predictivo y proteger de manera proactiva de cualquier incidente de seguridad que pueda comprometer la información.

Es recomendable para las EFS alinear su estrategia de seguridad con las necesidades propias de su misión, identificar y proteger la información crítica, aplicar controles de seguridad y verificar el cumplimiento de los mismos.

Para la aplicación de este nuevo enfoque de seguridad, es importante contar con el compromiso de la alta gerencia, porque es desde ese punto de la organización que se generan las estrategias y políticas inherentes a las organizaciones y que son aplicables al interior de las mismas, siendo relevante la formulación de la política de seguridad de la información y las demás que se desprenden de ella; así mismo se requiere socializarla a los empleados, terceras partes y clientes.

Las EFS están llamadas a realizar un ejercicio de control fiscal eficiente sobre el uso de los recursos públicos, a evaluar los mecanismos de rendición de cuentas y de transparencia existentes, lo que se ve reflejado en la percepción de la eficiencia de la administración pública. Para que esta labor sea oportuna y eficaz, las EFS se han apoyado en las Tecnologías de la Información y las Comunicaciones – TIC y es así como han realizado inversiones para fortalecerse en este aspecto, protegerse y dar mayor seguridad a la información que gestionan antes de ser publicada o compartida.

Si bien la información publicada y compartida por la EFS es abierta, antes de ser liberada tiene carácter de clasificada o reservada y desde esta perspectiva debe ser tratada con todos los criterios de seguridad que permitan garantizar su confidencialidad, integridad, disponibilidad y no repudio.

Se observa que las EFS a nivel Latinoamérica están conscientes de la importancia de la protección de la información en todos los momentos de la gestión de la misma, desde que es insumo interno y que aún no se encuentra liberada hasta que se constituye en datos abiertos. En cada uno de estos momentos se requiere mecanismos de protección para asegurar la información.

El estudio técnico realizado, se encaminó a evaluar los avances alcanzados por las EFS a nivel regional (Latinoamérica), con relación a aspectos de seguridad basados en temas relevantes de la Norma ISO 27002, Controles de seguridad, e ISO 27001:2013 que permitió reconocer las principales herramientas con que cuentan las EFS para garantizar

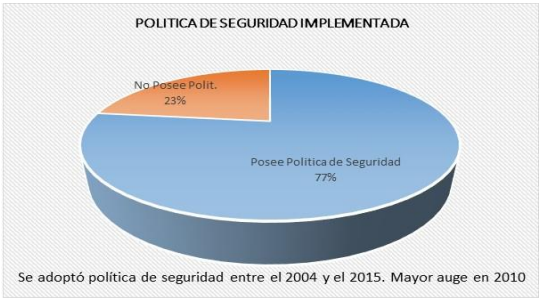
la seguridad de la información que procesan y gestionan para su posterior liberación, evidenciar las buenas prácticas aplicadas en aspectos de seguridad informática, reconocer los mecanismos de seguridad empleados en el intercambio de información, identificar los riesgos; así como, comprobar la existencia o proceso de conformación de equipos de respuesta a incidentes de seguridad informática.

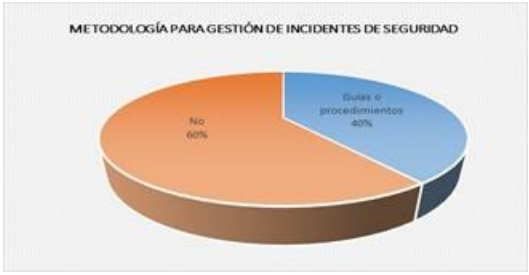
El tema técnico “La importancia del uso de base de datos y de la seguridad de la información para el fortalecimiento de las TIC y para el ejercicio eficiente del control” fue desarrollado abordando para el tema de seguridad los siguientes dominios de la Norma ISO 27002 que ayudaron a tener una visión general del estado actual en que se encuentran las EFS, frente al reto de emplear las TIC´s para fortalecer el ejercicio del control fiscal.

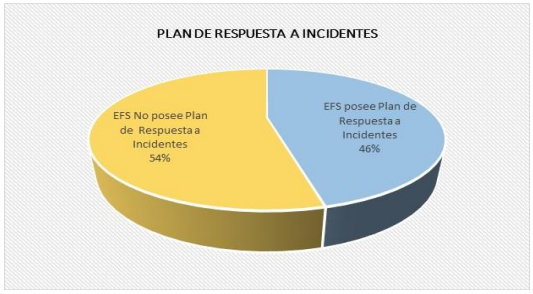
Desde esta visión se inició con la aplicación de encuestas orientadas al sondeo de la situación actual de trece (13) EFS del sector de Latinoamérica en cuanto a la aplicación de algunos dominios de la ISO 270001:2013 que dejan ver lo siguiente:

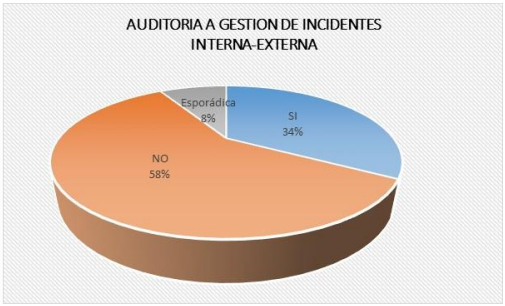
1. BUENAS PRACTICAS SEGURIDAD DE LA INFORMACION

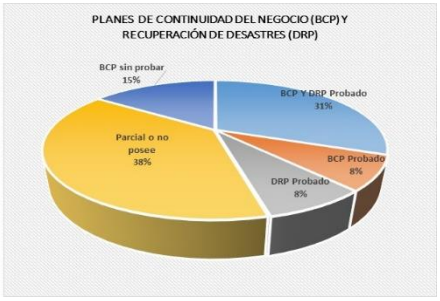
Resultados Encuestas Buenas Prácticas Seguridad de la Información











En los resultados de las encuestas buenas prácticas para la seguridad de la información se evidencia que en el dominio relacionado con **política de seguridad**, el 77% de las EFS encuestadas cuentan con una política de seguridad, el mayor auge en la implementación se da entre de 2014 y 2015 iniciando en 2010, lo que permite ver que la mayoría de la EFS cuentan con este primer paso para ayudar a proyectar las metas de

seguridad de la información en sus organización. El 62% de las entidades tiene clasificada la información. Este resultado es concordante con lo manifestado con relación compromiso de la alta dirección respecto a la seguridad de la información en donde el 62% de las EFS manifiestan contar con este apoyo, mientras el 23% dicen no cuenta con este y el 15% tiene apoyo de tipo limitado o esporádico.

En el domino de **gestión de incidentes** se observó que más del 58% (Metodología para gestión de incidentes, plan de respuesta a incidentes y metodología para gestión de incidentes y análisis de vulnerabilidades) no tiene metodologías, ni procesos para gestión de incidentes y análisis de vulnerabilidades, el 42% restante cuentan con mecanismos y metodologías para gestionar los incidentes de seguridad. De otra parte el 58 % manifiesta no realizar auditoria internas o externas a los procesos de incidentes, mientras el 34% si la realiza y el 8% lo hacen de manera esporádica.

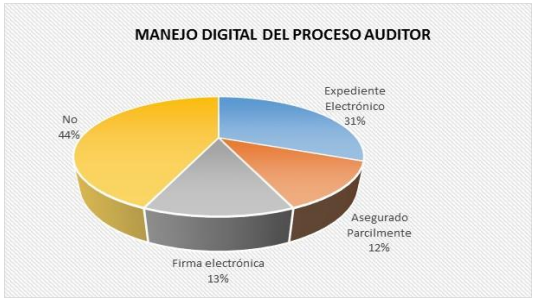
En cuanto al dominio relacionado con aspectos de la **Seguridad de la Información en la Gestión de la Continuidad de Negocio** se observa que el 38% de las EFS encuestadas no cuentan ni con planes de continuidad del negocio, BCP (Business Continuity Planning, por sus siglas en inglés) ni con plan de recuperación de desastres DRP (Disaster Recovery Plan, por sus siglas en inglés), el 31% de las EFS han probado un BCP y un DRP, el 8% ha probado al menos un DRP y el otro 8% restante solo ha probado un BCP, lo que demuestra un interés en garantizar la continuidad del negocio.

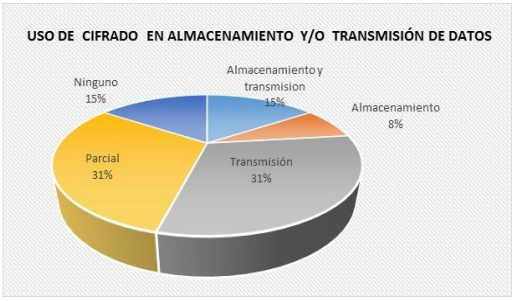
En el dominio de **Seguridad de la información en las relaciones con suministradores,** se abordó el tema de acuerdos de privacidad NDA (Non Disclosure Agreement, por sus siglas en inglés) y de niveles de servicio – SLA (Service Level Agreement, por sus siglas en inglés) y se ve que el 62 % de las EFS cuenta con acuerdos de privacidad y de niveles de servicio, mientras que tan solo el 15% tiene únicamente acuerdos de niveles de servicio y el otro 15% tiene acuerdos de niveles de confidencialidad y solamente el 8% no tiene acuerdos de servicios ni niveles de privacidad; lo que permite concluir que igualmente existe interés por la aplicación de estos niveles de servicio con sus proveedores.

2. SEGURIDAD DE LA INFORMACION

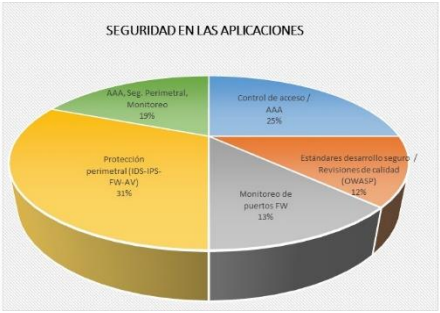
Resultados Encuestas Seguridad de la Información

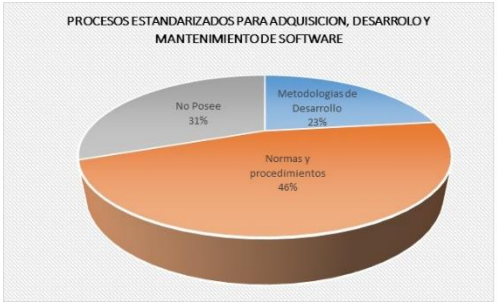
Dominio Cifrado



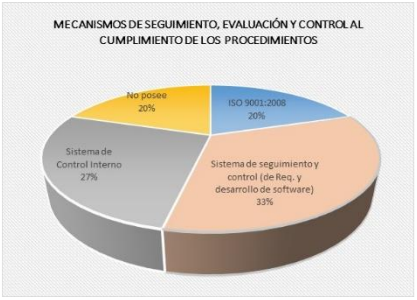


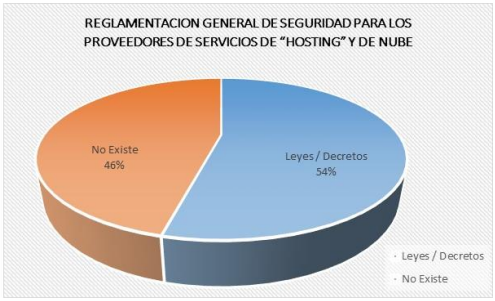
Dominio aadquisición, desarrollo y mantenimiento de los sistemas de información





Dominio de Cumplimiento





Fuente: EFS colaboradoras para la desarrollar el tema Técnico No. 2

Dominio Cifrado

El objetivo planteado en este dominio es el uso de sistemas y técnicas criptográficas para la protección de la información con base en el análisis de riesgo efectuado, con el fin de asegurar una adecuada protección de la confidencialidad e integridad de la información.

En los resultados de la Encuesta sobre Seguridad de la Información, a nivel de dominio de **cifrado** y con relación al manejo digital del proceso auditor se observa que el 44% de las EFS no cuenta con un manejo digital del proceso auditor, el 31% tiene o registra el proceso con expediente electrónico, el 13% aplica firma electrónica a sus procesos y el 12% lo ha asegurado parcialmente.

En el uso de cifrado en el almacenamiento y/o transmisión de datos el 31 % de las EFS encuestadas cifra en la transmisión, el 31% hace un cifrado parcial, el 15% cifra tanto en la transmisión como en el almacenamiento y el 8% solo en el almacenamiento; mientras un 15% no hace cifrado, lo representa un alto riesgo de seguridad, pues personas no autorizadas podrían tener acceso la información de forma indebida, bien sea en la fuente de generación, en la transmisión o en el repositorio de datos.

En cuanto al **Dominio Adquisición, desarrollo y Mantenimiento de los sistemas de información** cuyo objetivo se encamina a asegurar que en la adquisición y el desarrollo de los sistemas de información se incluyan controles de seguridad y validación de los datos, así como a definir los métodos de protección de la información crítica o sensible; y a definir y documentar los procedimientos y normas que se aplicarán durante el ciclo de vida de los aplicativos y en la infraestructura de base en la que se apoyan, se evaluó el tema de seguridad en las aplicaciones y en el uso procesos estandarizados para la adquisición, desarrollo y mantenimiento de software.

Se detectó que mediante la implementación de metodologías de desarrollo y estandarización de normas y procedimientos, el 69% de las EFS ha desarrollado procesos estandarizados para adquisición, desarrollo y/o mantenimiento de software, de tal manera que se propende por garantizar niveles de seguridad en las aplicaciones

En cuanto a **seguridad de aplicaciones** se indagó sobre las medidas de seguridad empleadas, encontrando que el 100% de las EFS tienen presente el tema de seguridad de las aplicaciones, destacando la implementación de estándares, desarrollo seguro, revisiones de calidad (OWASP - Open Web Application Security Project - Proyecto abierto de seguridad de aplicaciones web); uso de controles de acceso (autorización, autenticación y auditoría – AAA). A nivel de infraestructura de red de datos, protección perimetral a través de IDS- Intrusion Detection System o Sistema de Detección de Intrusos, IPS- Intrusion Prevention System o Sistema de Prevención de Intrusos; firewall de red y de aplicaciones y el Antivirus/antispam, de uso más generalizado.

En el dominio de **cumplimiento** está encaminado a evitar el incumplimiento de las obligaciones legales, de reglamentación o contractuales y estatutarias relacionadas con seguridad de la información y de cualquier requisito de seguridad.

Se observó que se han desarrollado mecanismos de seguimiento, evaluación y control al cumplimiento de los procedimientos definidos, alineados con estándares. De igual forma el 92 % de las EFS manifiestan tener reglamentación para la recolección, uso y procesamiento de información personal; mientras que con relación a la reglamentación general de proveedores de servicios de hosting y de nube solo el 54% tiene leyes y decretos relacionados.

3. Conformación de grupos de respuesta a incidentes de seguridad CSIRT

Los grupos de respuesta a incidentes de seguridad CSIRT (Computer Security Information Response Teams por sus siglas en inglés) o los Equipos de Emergencia CERT (Computer Emergency Response Team[3], término registrado por EEUU) son equipos de trabajo especializados, que realizan respuesta de manera centralizada a incidentes de seguridad ya sea a nivel operativo o de coordinación; surgen como respuesta ante las amenazas a las que se ve avocada la información que se publica en Internet; se encargan de dar respuesta a incidentes de seguridad de la información, conservando las características de disponibilidad, integridad, confidencialidad y auditoría de la información para los servicios básicos de red, correo electrónico, mensajería instantánea, internet, intranet, portal institucional, capacitación entre otros.

El CSIRT o CERT ofrecen servicios reactivos como generación de alertas, advertencias, gestión de incidentes de seguridad y gestión de vulnerabilidades; servicios proactivos como: comunicados, observatorio tecnológico, configuración y mantenimiento de herramientas, aplicaciones e infraestructura de seguridad, servicios de detección de intrusos y difusión de información relacionada con la seguridad y finalmente, servicios relacionados con la gestión de calidad de la seguridad como análisis de riesgos, plan de continuidad de negocio y recuperación de desastres, educación y entrenamiento. Los mecanismos y estructuras de control, implementadas por los administradores de los diferentes servicios y el nivel de importancia de la cultura de control en las áreas de TIC, se han visto amenazados por el incremento del porcentaje de incidentes de seguridad, que influyen en las áreas administrativas, financieras y de gestión y afectan los resultados misionales. Esto genera que los incidentes que se presentan sean atendidos de forma inoportuna, sin metodologías apropiadas; sin dejar registro, de la ocurrencia del incidente, del seguimiento, tratamiento, solución y prevención que garantice una respuesta adecuada, controlando la aparición de nuevos eventos que afecten la seguridad y minimizando los riegos de la misma.

Resultados Encuestas CSIRT

Con el fin de compartir la evaluación realizada con relación al avance que las EFS poseen en relación con el tema, se puede afirmar que 10 de las 13 que remitieron sus aportes, cuentan con personal especializado en seguridad informática, arrojando el promedio menor a dos (2) especialistas, que además de gestionar la infraestructura de red de datos,

[3] Carnegie & Mellon CERT: http://www.cert.org

realizan monitoreo y/o atención de incidentes. Adicionalmente, el 46% manifestó tener implementado un grupo de seguridad de la información, sin embargo sólo el 31% (4 EFS) confirma que este grupo de trabajo se encuentra institucionalizado y que existe la figura de oficial de seguridad informática en la EFS.

Se pudo identificar contradicciones en respuestas de los ítems 1.4 "¿Se han presentado fallas en la seguridad sobre la información almacenada en los archivos de bases de datos?" y el 5.10 "¿Se realiza seguimiento a los incidentes de seguridad que se han presentado en la EFS?". Una falla de seguridad es considerada como un incidente.

En la pregunta 1.4, el 67% de EFS respondieron no haber presentado "fallas en la seguridad sobre la información almacenada en los archivos de bases de datos"; sin embargo, en la respuesta dada a la pregunta 10, el 85% de EFS contribuyentes manifiesta realizar "seguimiento a los incidentes de seguridad".

1.4 Fallas en la seguridad sobre la información almacenada	NO
Puerto Rico	
Perú	x
Chile	x
Cuba	x
Costa Rica	x
Argentina	x
Nicaragua	x
Venezuela	x
México	x
República Dominicana	x
Honduras	
Panamá	x
Colombia	

5.10 Seguimiento a incidentes de seguridad	**Si**
Puerto Rico	x
Perú	
Chile	x
Cuba	x
Costa Rica	x
Argentina	x
Nicaragua	x
Venezuela	x
México	x
República Dominicana	x
Honduras	
Panamá	x
Colombia	x

Fuente: EFS colaboradoras para la desarrollar el tema Técnico No. 2

Igual situación se presenta en el ítem 5.11 "Acciones preventivas a los incidentes de seguridad registrados", cuando se afirma "incidentes registrados" está sugiriendo que ya se materializó el riesgo y se evidenció el incidente

1.4 Fallas en la seguridad sobre la información almacenada	NO
Puerto Rico	
Perú	x
Chile	x
Cuba	x
Costa Rica	x

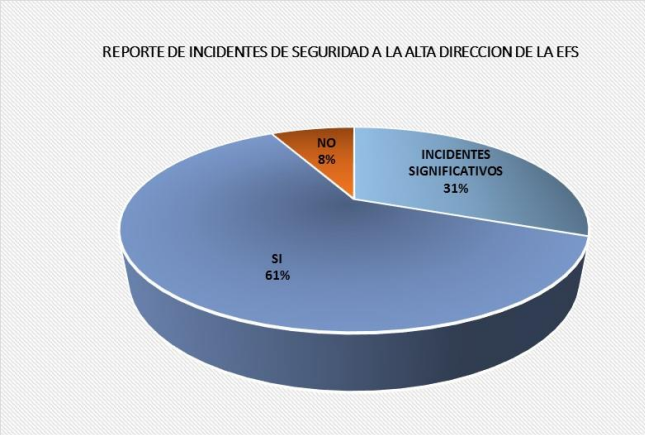
5.11 Acciones preventivas a los incidentes de seguridad registrados	**Si**
Puerto Rico	x
Perú	x
Chile	
Cuba	x
Costa Rica	x

Argentina	x
Nicaragua	x
Venezuela	x
México	x
República Dominicana	x
Honduras	
Panamá	x
Colombia	

Argentina	x
Nicaragua	x
Venezuela	x
México	x
República Dominicana	x
Honduras	x
Panamá	x
Colombia	x

Fuente: EFS colaboradoras para la desarrollar el tema Técnico No. 2

El 61% de EFS declaran reportar la información de los incidentes de seguridad a nivel de la alta dirección cuando la situación lo amerita, reportan incidentes significativos o a solicitud; sin embargo, también se hace reporte a la jefatura de la unidad y al gerente de apoyo:



Fuente: EFS colaboradoras para la desarrollar el tema Técnico No. 2

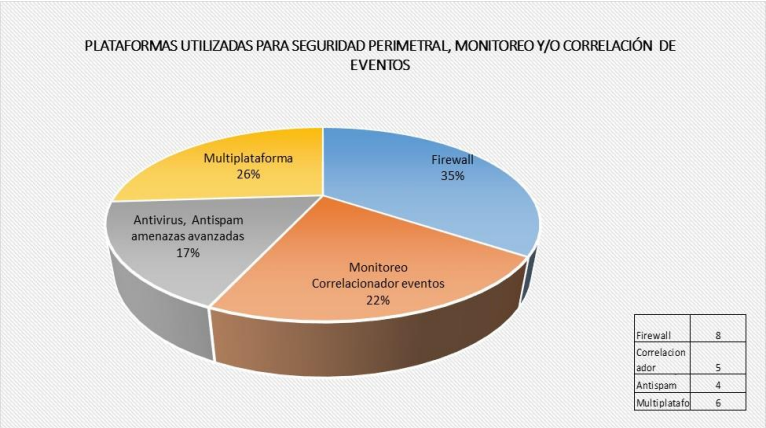
Con relación a plataformas se utilizan para seguridad perimetral, monitoreo y/o correlación de eventos de seguridad de la información se presenta diversidad de marcas y elementos activos de monitoreo, de bloqueo, entre otros.

4. ¿Qué plataformas se utilizan para seguridad perimetral, monitoreo y/o correlación de eventos de seguridad de la información?	Firewall red	Firewall aplicaciones	Correlacionador de eventos	Monitoreo BD Red Servidores	Antivirus	Anti spam	Amenazas avanzadas	Multiplataforma
Puerto Rico	UTM	x	NO	x			x	
Perú	Fortigate	Fortiweb	Solar Winds	Imperva	Sophos	Barracuda	Fireye	
Chile	NexGeneration		SIEM	x				Seguridad Perimetral
Cuba								SWL Windows

4. ¿Qué plataformas se utilizan para seguridad perimetral, monitoreo y/o correlación de eventos de seguridad de la información?	Firewall red	Firewall aplicaciones	Correlacionador de eventos	Monitoreo BD Red Servidores	Antivirus	Anti spam	Amenazas avanzadas	Multiplataforma
Costa Rica	x	x						
Argentina								Juniper, Zenworks,Squid-Shorewall, Nac Forescout
Nicaragua	x							
Venezuela								Seguridad Perimetral basada en HIPS
México								Seguridad Perimetral.PA-3020. Palo Alto Networks
República Dominicana	x			x			x	
Honduras								NO hay respuesta
Panamá	x							
Colombia	x	x	x	x	x	x	x	x

Para presentar de modo general, fueron agrupados los elementos en cuatro grandes categorías: firewall, monitoreo y correlacionador de eventos, antivirus y multiplataforma

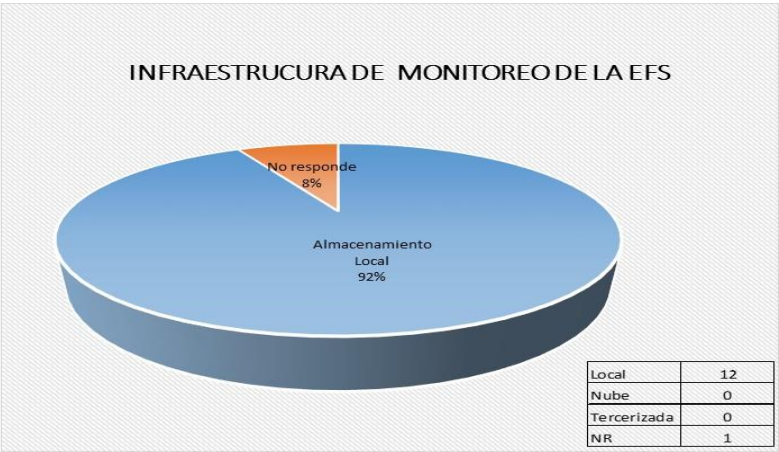
4. ¿Qué plataformas se utilizan para seguridad perimetral, monitoreo y/o correlación de eventos de seguridad de la información?	Firewall	Monitoreo Correlacionador eventos	Antivirus Antispam amenazas avanzadas	Multiplataforma
Puerto Rico	x	x	x	
Perú	x	x	x	
Chile	x	x		x
Cuba				x
Costa Rica	x			
Argentina				x
Nicaragua	x			
Venezuela				x
México				x
República Dominicana	x	x	x	
Honduras				
Panamá	x			
Colombia	x	x	x	x



Fuente: EFS colaboradoras para la desarrollar el tema Técnico No. 2

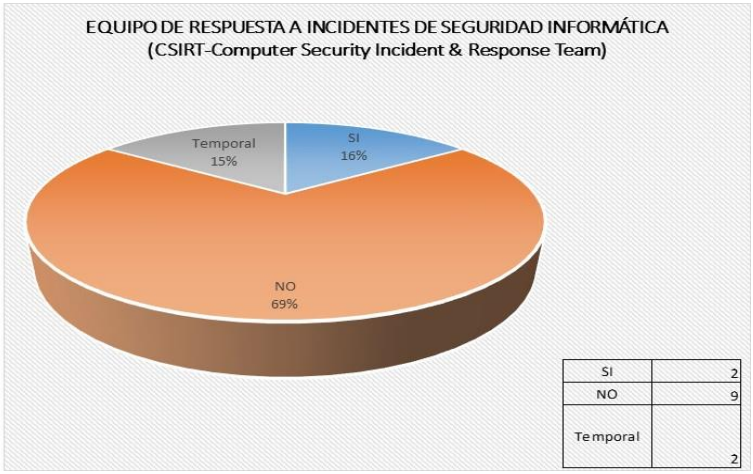
Las EFS revelaron que el 92% de la infraestructura de monitoreo y seguridad que posee la EFS es local

5. ¿La infraestructura de monitoreo y seguridad que posee la EFS se encuentra: Tercerizada, en la nube, local, otra (Especifique)?	Tercerizada	Nube	Local
Puerto Rico			x
Perú			x
Chile			x
Cuba			x
Costa Rica			x
Argentina			x
Nicaragua			x
Venezuela			x
México			x
República Dominicana			x
Honduras	No responde		
Panamá			x
Colombia			x



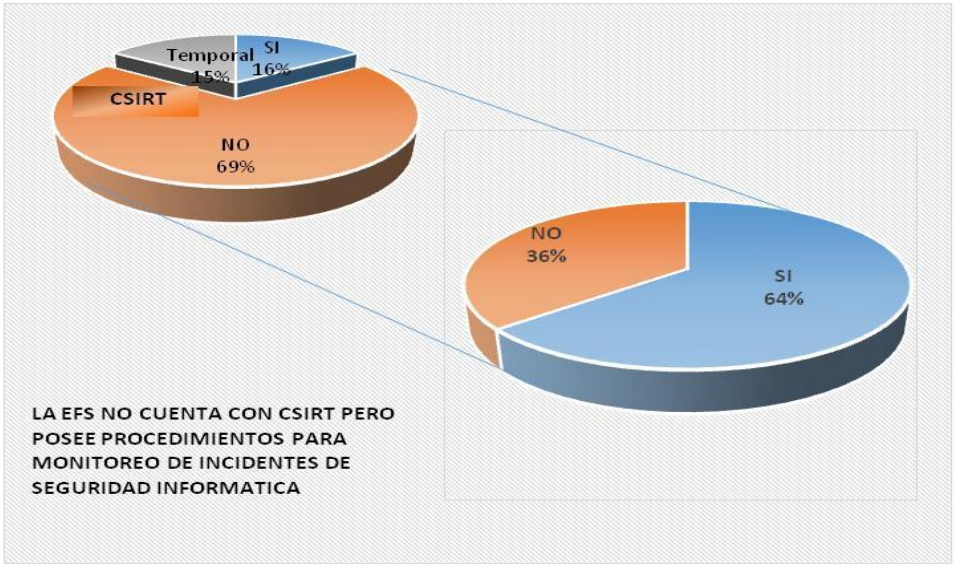
Fuente: EFS colaboradoras para la desarrollar el tema Técnico No. 2

Retomando el equipo de respuesta a incidentes de seguridad – CSIRT, se encontró que esta área organizacional aún es reciente, lo que genera que muy pocas EFS la tengan implementada o creada y en conformación. No obstante, 4 EFS tienen identificados los servicios que va a prestar el CSIRT, su entorno y grupo de clientes.



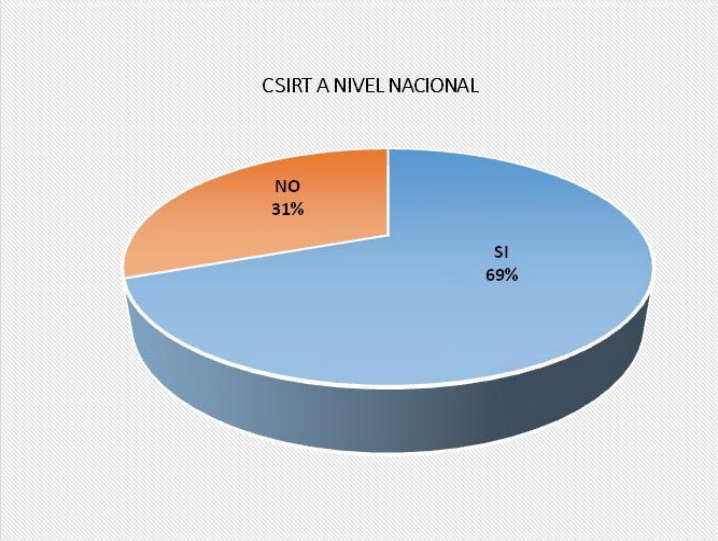
Fuente: EFS colaboradoras para la desarrollar el tema Técnico No. 2

Puesto que la gran mayoría no cuenta con un CSIRT implementado, se indagó sobre la existencia de procedimientos para monitorear los incidentes de seguridad informática; a esta inquietud el 69% respondió no tener implementado el CSIRT, sin embargo de ese 69%, el 64% declaró poseer procedimientos para monitorear los incidentes de seguridad informática.



Fuente: EFS colaboradoras para la desarrollar el tema Técnico No. 2

Con relación a la existencia a nivel nacional de un equipo de respuesta a incidentes de seguridad informática (CSIRT) el 31% manifestó la no existencia de esta iniciativa a nivel nacional.

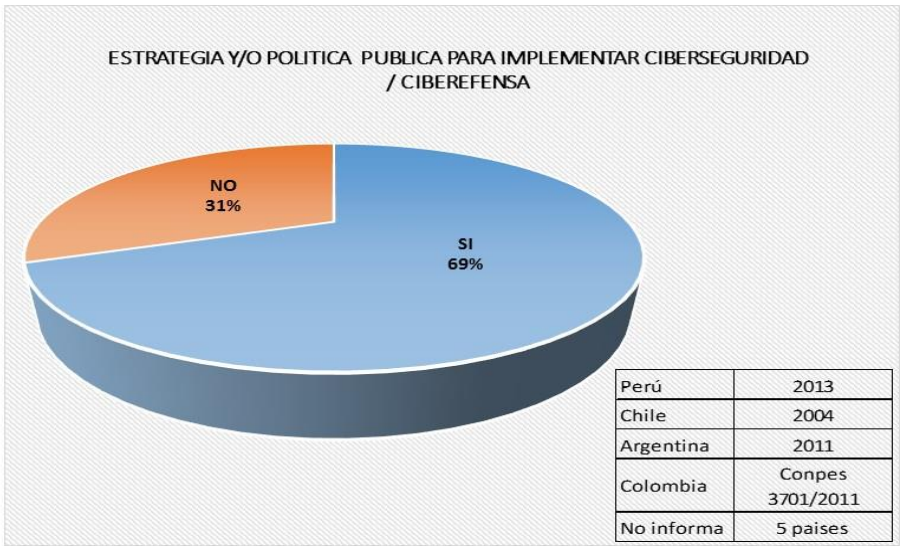


Fuente: EFS colaboradoras para la desarrollar el tema Técnico No. 2

Equipo de respuesta a incidentes de seguridad informática (CSIRT / CERT)?	Si	No	Nombre
Puerto Rico		x	La Ofc. Gerencia y Presupuesto dispone de un grupo para atención de incidentes de seguridad.
Perú	x		Sistema de Coordinación de la Administración Pública (Pe-CERT)
Chile	x		ClCert
Cuba	x		CuCERT
Argentina	x		ICIC - Prog. Nal. de Infraestructuras Criticas de Información y Ciberseguridad
Venezuela	x		VenCert
México	x		Administración Pública Federal
República Dominicana	x		Oficina Presidencial de Tecnologías de la Información y Comunicación OPTIC
Panamá	x		CSIRT Panamá
Colombia	x		ColCERT

Fuente: EFS colaboradoras para la desarrollar el tema Técnico No. 2

Por último se preguntó por la existencia de una estrategia o política pública para implementar un mecanismo de ciberseguridad / Ciberdefensa a nivel nacional y desde que fecha el país ha estado trabajando en el tema. De las respuestas se analizó que a excepción de la Contraloría General de la República de Chile que ha tratado el tema desde el 2004, las demás EFS iniciaron su trabajo entre el 2011 y el 2013.

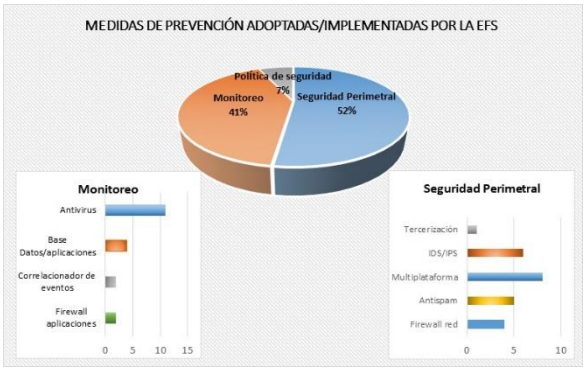


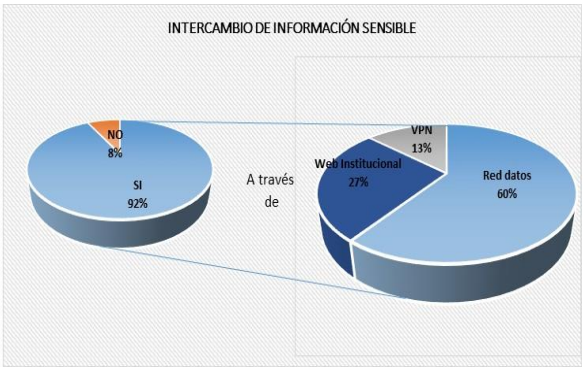
Fuente: EFS colaboradoras para la desarrollar el tema Técnico No. 2

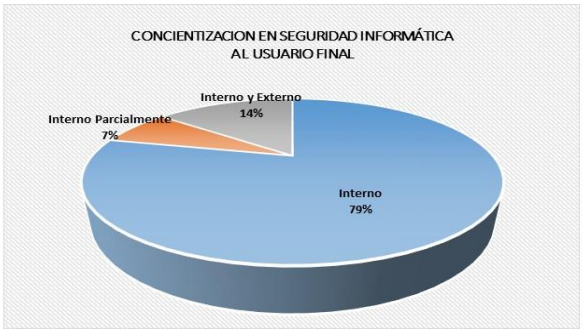
4. MECANISMOS DE SEGURIDAD PARA INTERCAMBIO DE INFORMACIÓN

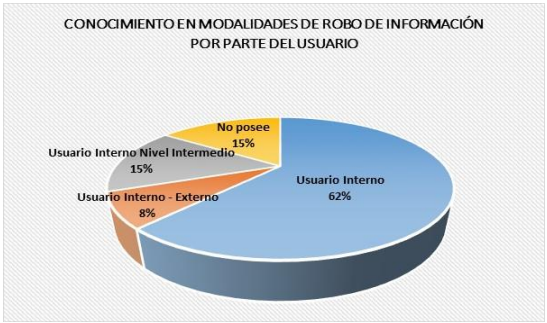
En el dominio 13 Seguridad de las comunicaciones se contempla el objetivo de control Transferencia de Información

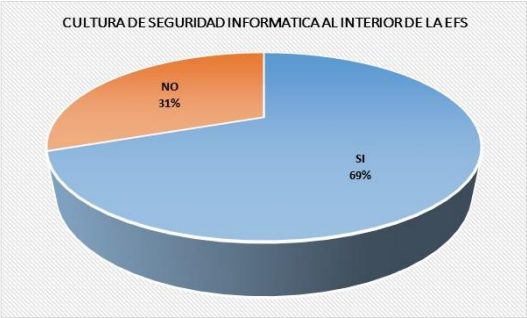
Encuesta Intercambio Información



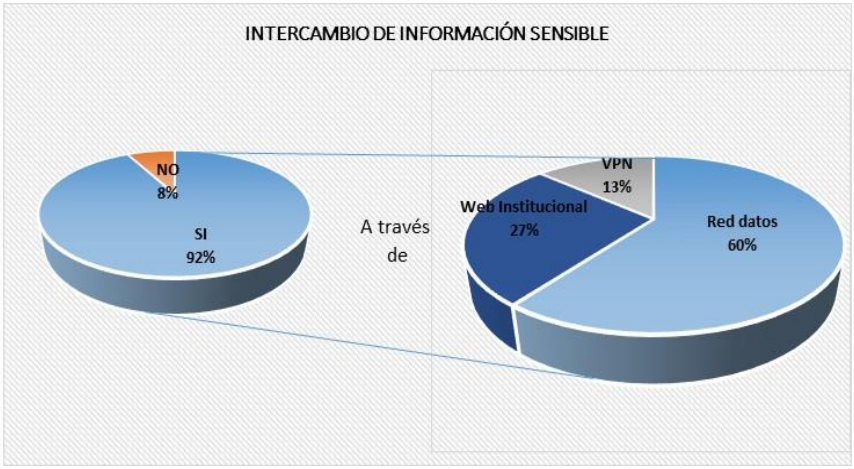






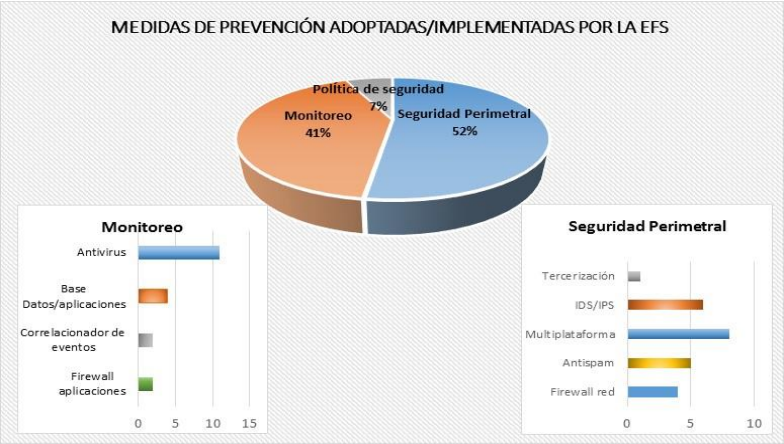
Encuesta Intercambio Información	
	

Las EFS realizan intercambio de información sensible a través de la red de datos interna o web Institucional. Se encontró que el 92% de las Entidades Fiscalizadoras Superiores realizan el intercambio a través de la red de datos, de la web institucional y en casos muy puntuales se emplean redes privadas virtuales (VPN)



Fuente: EFS colaboradoras para la desarrollar el tema Técnico No. 2

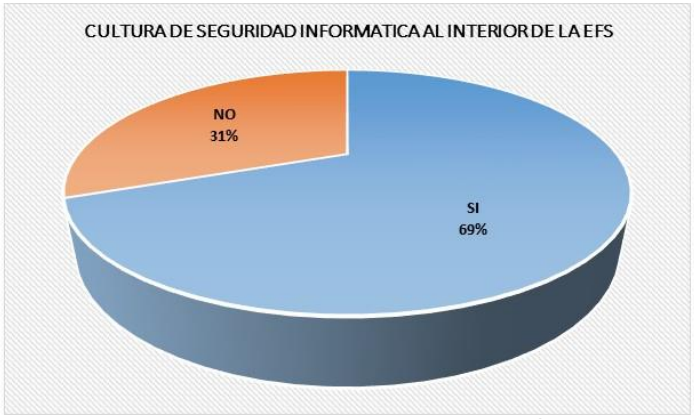
Con el fin de compartir y evaluar mecanismos de seguridad implementados por las EFS, para intercambiar información interna o externamente, evitar la acción de amenazas ocasionadas por la proliferación de software malicioso como virus, malware, troyanos, spam, etc., se realizó un sondeo de las medidas de prevención adoptadas o implementadas por las EFS.



Fuente: EFS colaboradoras para la desarrollar el tema Técnico No. 2

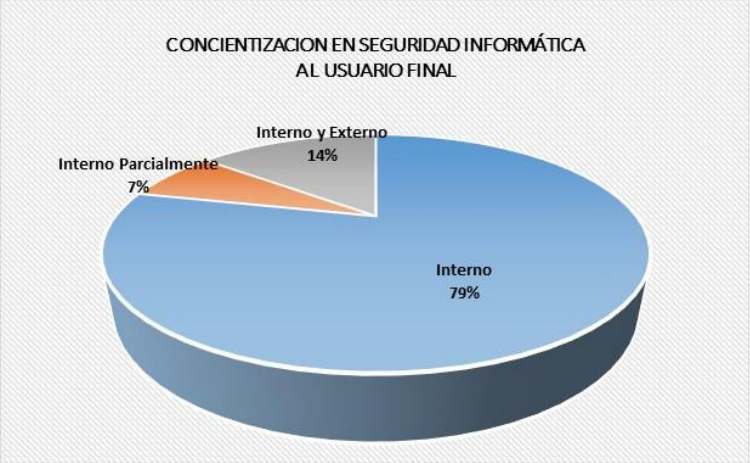
Las medidas de prevención adoptadas o implementadas por las EFS fueron agrupadas en tres categorías o grupos de trabajo: políticas de seguridad implementada por el 7% de las EFS, Monitoreo (implementación y uso de antivirus, monitoreo de aplicaciones y bases de datos, correlacionador de eventos y aseguramiento mediante uso de firewall de aplicaciones) empleada por el 41%; y 52% reporta existencia de infraestructura de seguridad perimetral (firewall de red, anti spam, IDS e IPS, tercerización de la seguridad del perímetro de red, entre otras).

La evaluación permitió determinar la existencia de una cultura de seguridad informática al interior de las EFS del 69% (9 EFS respondieron afirmativamente); también que el usuario final ha sido concientizado en el tema de seguridad informática, haciendo mayor énfasis en el usuario interno, lo cual le ha permitido tener conocimiento de las diferentes modalidades de robo de información a través de Internet (web) a que se encuentra expuesto.



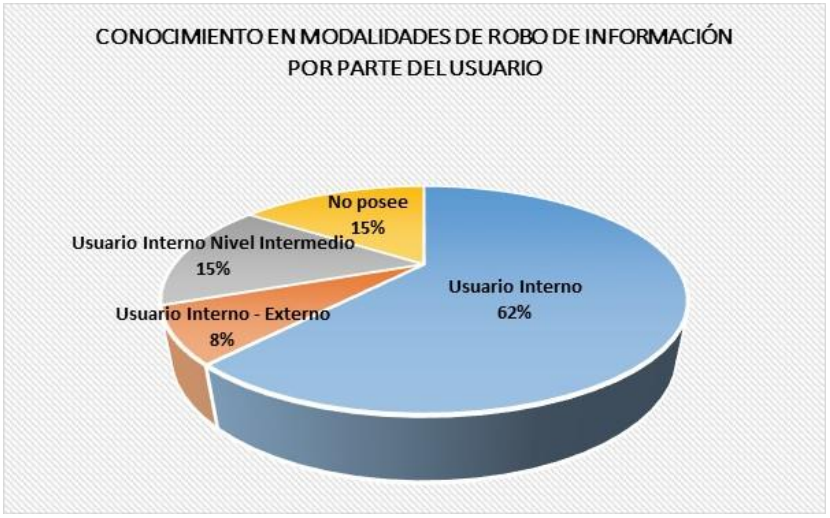
Fuente: EFS colaboradoras para la desarrollar el tema Técnico No. 2

De otra parte, se evidenció que el 79 % de los usuarios finales internos ha sido concientizado con la seguridad informática, otro 14%, reporta que se ha concientizado a los usuarios tanto internos como externos, mientras que el 7% manifiesta que solo ha concientizado parcialmente a su usuarios internos.



Fuente: EFS colaboradoras para la desarrollar el tema Técnico No. 2

En la siguiente gráfica se muestra que el 62% de los usuarios internos de las EFS tiene conocimiento de las modalidades de robo de información, mientras el 15% no posee conocimiento.



Fuente: EFS colaboradoras para la desarrollar el tema Técnico No. 2

Conclusiones

Haciendo un análisis de las recomendaciones del estándar ISO 27001:2013 y la información proporcionada en las encuestas por EFS colaboradoras, se observa un interés general en el tema de seguridad de la información, en cuanto a la aplicación de buenas prácticas y controles de seguridad en la plataforma tecnológica de TI; por tanto debería trabajarse definiendo una política maestra de seguridad de la información para alinear la estrategia de seguridad de la OLACEFS y las EFS. Igualmente, una política de Gobierno de TI para intercambio de información, que facilite aunar esfuerzos para garantizar la seguridad de la información y definir normas para su intercambio.

Por tanto todas la acciones deben estar encaminadas a propender por la seguridad de la información recolectada, procesada, analizada y compartida, de tal manera que ésta

pueda ser accedida por quien debe hacerlo y en el momento permitido para ello, observar aspectos relevantes a considerar en la elaboración de políticas de seguridad y para la definición de herramientas de seguridad a emplear. Lo anterior, sin perder de vista el enfoque integrado de seguridad de la información como un proceso sistemático permanente, cuyo costo debe ser proporcional al valor de los activos de información que protege.

La alta dirección debe tomar conciencia que por el tipo de información estratégica que posee, se vuelve más vulnerable al convertirse en blanco de los delincuentes informáticos, por lo que requiere de mayor compromiso y ejemplo para fortalecer la seguridad en todos los niveles de la organización; por ello, es importante que este comprometida a encaminar sus esfuerzos para implementar el Sistema Gestión de Seguridad de la Información – SGSI; para ello deberá conocer opciones de desarrollo tecnológico y legislar sobre el tema con el fin de generar capacidades institucionales para la gestión integral y sostenibilidad del proyecto de seguridad.

Igualmente, es importante la implementación del Centro de Respuesta a Incidentes (CSIRT o CERT) con el fin de generar reglas para los usuarios de TICs en las EFS, desarrollando relaciones de confianza y un punto de contacto confiable dentro de la entidad para el manejo de incidentes de seguridad de la información. Con la coordinación apropiada se promoverá la adecuada utilización de la infraestructura tecnológica basados en las buenas y mejores prácticas,

Los usuarios deben esperar que el CSIRT les preste los servicios que describen, pero es preciso enfatizar que sin la participación activa de ellos, la eficacia de los servicios y su operatividad podrá verse disminuida considerablemente, igualmente que sin el respaldo y apoyo de la alta dirección en la implementación y funcionamiento, el grupo de respuesta a incidentes no podrá mostrar sus verdaderos beneficios. La sensibilización general que provee el CSIRT sobre aspectos de seguridad entre los usuarios no sólo mejora el grado de entendimiento de estos sobre el tema, sino que además ayuda a reducir el número de ataques exitosos y aumenta la probabilidad que se detecten y reporten oportunamente, lo que redunda en que los tiempos de recuperación disminuyan y las pérdidas se minimicen o tiendan a desaparecer. El manejo oportuno y proactivo de los incidentes de seguridad se verá reflejado en reducción de costos, aumento de la seguridad de la información con base en la gestión y mejora de los procesos que se desarrollan y de los servicios que se ofrecen.

Es muy útil tener un CSIRT estructurado dado que en este se concentra personal especializado, equipos de gestión y monitoreo, alertas y recomendaciones de seguridad, de tal manera que las EFS estarán en capacidad de participar y compartir experiencias con otros equipos similares y proveedores de servicios de seguridad de la información, mejorarán su conocimiento estratégico en el manejo de incidentes de seguridad de forma global. Es importante compartir información de alertas o de amenazas avanzadas, con el fin de fortalecer la seguridad de la información entre EFS; adicionalmente, se podrá contar con una metodología de gestión de la seguridad estructurada para reducir riesgos por pérdida o robo de la información; identificando debilidades del sistema y de las áreas

a mejorar; además, proporcionará de forma expedita los procedimientos para restablecer la continuidad a las operaciones de la Entidad tras la ocurrencia de incidentes graves.

Es importante sensibilizar al usuario final sobre la importancia de tener conocimiento de seguridad informática y de aspectos relevantes de la seguridad de la información como integridad, disponibilidad, confidencialidad, gestión de incidentes, medidas no invasivas, protección de la información y políticas de acceso a la información, dado que el eslabón más débil en la implementación de la cadena de procesos de la seguridad, de lo contrario no habrá herramienta de seguridad capaz de proteger la información. Se debe implementar estrategias de sensibilización periódicamente, dirigida a actualizar conocimientos de seguridad al personal y capacitar a los nuevos ingresantes.

Cabe resaltar la importancia que tiene contar con convenios que permitan el intercambio de experiencias, buenas prácticas e información útil para la ejecución de los procesos institucionales en cuanto a seguridad de la información; compartir experiencias del proceso de implantación de plataformas de seguridad, como herramientas de Gestión de incidentes con una visión de Inteligencia de Negocios, que permita minimizar al máximo los falsos positivos (incidentes que generan alarmas que no comprometen los sistemas) además, compartir experiencias del proceso de implementación de la confidencialidad en la red de datos, información que ayuda a relacionar la situación actual de cada EFS y compararla para mejorar el entorno de seguridad y gobernanza de tecnología de la información.

Por último, no sobra resaltar que no existe un sistema “totalmente seguro” y que independientemente de las medidas y controles aplicados y del conocimiento del riesgo, este siempre estará presente y por tanto la seguridad absoluta no es posible, por lo que se debe trabajar sobre alcanzar niveles aceptables de seguridad.

RECOMENDACIONES

En cuanto a la implementación de buenas prácticas, se sugiere compartir experiencias de su proceso de atención a incidentes de seguridad, fortalecer la respuesta a incidentes mediante la conformación de equipos especializados e institucionales permanentes, para promover y coadyuvar a que se establezca una política pública que se refuerce los mecanismos de mitigación de riesgos de seguridad informática. Además, conocer el apoyo que brinda las diferentes EFS, con el fin de simplificar trámites para evitar duplicidad de información, estandarización de plataformas tecnológicas.

Se sugiere a todas las EFS implementar el equipo de respuesta de incidentes informáticos (CSIRT / CERT) propendiendo por la adopción e implementación de estándares de tal forma que en el momento de enfrentar un incidente informático que generé pérdida de información se cuente con medidas que garanticen contar con respaldos o backups, con planes de continuidad y recuperación de desastres, que permitan restablecer la operación y dar continuidad del negocio en el menor tiempo posible.

Dado que la información disponible de las entidades, constituye un insumo determinante en el éxito de sus labores y son el factor más importante para la creación de sinergias encaminadas a consolidar una gestión pública transparente, eficiente y honesta; se debe trabajar en tener sitios web seguros, de fácil acceso, que permitan publicar la información generada como producto de las operaciones realizadas al interior de las EFS para demostrar trasparencia, divulgar la información, dar a conocer los resultados de su trabajo y ofrecer servicios a la ciudadanía.

Antes de publicarse nuevos servicios, deben realizarse pruebas de penetración/test de vulnerabilidades que las determinen, en aras de subsanarlas antes de su publicación en internet.

Se sugiere que para asegurar la información producida y compartida por las EFS, el intercambio de ella en cualquier instancia se realice en modo cifrado e impulsar el uso del certificado electrónico o firma electrónica, aprovechado las ventajas de la infraestructura de clave pública (PKI) de cada país.

Si no existe una política de gobierno para el intercambio de información, las entidades se deben poner de acuerdo y aunar esfuerzos para garantizar la seguridad de la información y establecer normativas para su intercambio.

CREDITOS Y AGRADECIMIENTOS

La Contraloría General de la República de Colombia, agradece la contribución realizada por los siguientes miembros de la Organización, que hicieron sus aportes de forma oportuna y permitieron elaborar un diagnóstico de la situación actual y del avance logrado mediante el uso de las TIC, quienes nos permitieron a través de la aplicación de la encuesta, realizar el análisis del tema técnico para esta Asamblea:

1. Controlaría General de la República de Cuba
2. Auditoría Superior de la Federación de México
3. Contraloría General de la República de Nicaragua
4. Contraloría General de la República Bolivariana de Venezuela
5. Contraloría General de la República de Chile
6. Auditoría General de la Nación de Argentina
7. Controlaría General de la República de Panamá
8. Cámara de Cuentas de la República Dominicana
9. Tribunal Superior de Cuentas de la República de Honduras
10. Oficia del Contralor del Estado Libre Asociado de Puerto Rico
11. Contraloría General de la República Perú
12. Contraloría General de la República de Costa Rica
13. Contraloría General de la República de Colombia