XXV ASAMBLEA GENERAL ORDINARIA DE LA ORGANIZACIÓN LATINOAMERICANA Y DEL CARIBE

DE ENTIDADES FISCALIZADORAS SUPERIORES

QUERÉTARO, MÉXICO, 23-28 NOVIEMBRE DE 2015

TEMA TÉCNICO 2

"LA IMPORTANCIA DEL USO DE BASES DE DATOS Y DE LA SEGURIDAD DE LA INFORMACIÓN PARA EL FORTALECIMIENTO DE LAS TICS EN EL EJERCICIO EFICIENTE DEL CONTROL"

PROPUESTA
INICIAL Y
DOCUMENTO GUIA

COLABORACIÓN
TÉCNICA

AUDITORIA SUPERIOR DE LA FEDERACIÓN
-MEXICO- AGOSTO
2015

I. BASES DE DATOS Y MINERÍA DE DATOS: HERRAMIENTAS Y TÉCNICAS EMPLEADAS POR LAS EFS

Con el fin de obtener conocimiento para examinar las condiciones en que las EFS se encuentran, se formulan las siguientes preguntas. La respuesta a cada una de ellas conforma el documento de "Colaboración técnica" elaborado y remitido por todas las EFS que participan, para el desarrollo del presente tema técnico en la Asamblea General.

1. ¿En la EFS el almacenamiento de las bases de datos de información misional o de negocio, se encuentra local, en la Nube o híbrido? El almacenamiento de las bases de datos de información misional o de negocio se encuentra de manera local.

2. ¿La EFS hace explotación de datos y/o extracción de información para transformar en conocimiento útil y ayudar en la toma de decisiones? ¿A través de qué medio y/o herramienta? Además de la información que se gestiona a través de los sistemas institucionales y los reportes que se obtienen de ellos, la Auditoría Superior de la Federación emplea herramientas de análisis de información y de Business Intelligence:

    - Las áreas auditoras emplean la herramienta ACL para análisis de grandes volúmenes de datos en apoyo a la realización de sus auditorías.
    - También se utiliza la herramienta QlikView, catalogada como software de Business Intelligence, para análisis de diversas fuentes de información, tanto de carácter administrativo como las relacionadas directamente con el trabajo sustantivo de la institución, las cuales sirven para crear nuevo conocimiento y apoyar la toma de decisiones.

    ¿La EFS ha tenido dificultades con respecto a la recolección de la información por la falta de estandarización en su presentación? ¿Cuáles? (por ejemplo: diferentes formas de presentación, formatos como Pdf, Excel, Word, texto plano, etc.) *Sí, es muy común que la información que recolectan tanto las áreas administrativas como las sustantivas provenga de muy variadas fuentes y en diversos formatos, incluyendo documentos impresos y texto libre no estandarizado.*

Algunos ejemplos de lo anterior lo constituye la información que se solicita a los entes auditados:

- *Estados de cuenta bancarios, que son proporcionados en forma impresa y que requieren digitalización y limpieza de datos.*
- *Bases de datos en formatos diversos como Access, SQL, csv (comma separated values), txt.*

3. ¿Se han presentado fallas en la seguridad sobre la información almacenada en los archivos de bases de datos? No tenemos evidencia de que se haya presentado algún tipo de incidente. No, no ha habido fallas en la seguridad de base de datos.

4. ¿La EFS tiene establecidos protocolos para garantizar la seguridad en la información almacenada? ¿Cuáles**?** En general, con respecto a los sistemas informáticos y en particular con el sistema sustantivo de gestión de información de las auditorías, el Sistema de Control y Seguimientos de Auditorías (SICSA), se aplican los siguientes protocolos de seguridad:

- *Para el acceso al sistema se hace una doble verificación:*
  - *Que el usuario esté dado de alta en el Directorio Activo, lo cual implica que es un empleado vigente de la institución.*
  - *Que el usuario cuente con permiso de acceso al SICSA.*
- *Por otra parte, se requiere un permiso para ingresar a cada módulo del sistema y un permiso para cada rol (elaborador, revisor, aprobador, etc.) dentro del mismo.*
- *Para impedir que los usuarios tengan acceso a toda la información de los sistemas, también se aplican permisos por centros de trabajo de manera que cada usuario sólo puede ver la información perteneciente a su área y nivel.*
- *Ningún usuario tiene acceso directo a las bases de datos; el sistema informático se encarga de gestionar las peticiones de lectura y escritura a las bases de datos y es el único que puede tener acceso directo a la información.*

Adicionalmente a lo anterior se puede comentar que: La ASF cuenta con diferentes mecanismos de seguridad con el fin de proteger la información almacenada en los servidores frente a daños accidentales o deliberados que puedan afectar a la disponibilidad, integridad o confidencialidad de la información o de los servicios prestados. Para logar esto se tienen implementados:

Los motores de Bases de datos con los que opera la ASF son Oracle y SQL Server en sus versiones 2008 y 2012 y las medidas de seguridad que se han implementado son las siguientes:

1. *Los servidores donde se almacenan las bases de datos se encuentran físicamente resguardados en sites con controles de acceso restringido.*
2. *Los servidores a nivel plataforma Windows se encuentran protegidos perimetralmente por la herramienta institucional de Deep Security de Trend Micro.*
3. *Las cuentas de administración SA quedan a resguardo exclusivo del Administrador de las Bases de datos y no son usadas para que las aplicaciones accesen a la base de datos.*
4. *Las cuentas de administración SA cuentan con un password robusto, mediante la combinación de caracteres que no tiene asociado un patrón o referencia alguna.*
5. *Se crean cuentas de administración con acceso restringido para las diferentes aplicaciones que hagan uso de la Base de datos*
6. *Se ha modificado el puerto de comunicaciones default para el acceso a la base de datos. El puerto default no es usado en aquellas en las que la funcionalidad lo ha permitido.*
7. *Se realiza una revisión periódica para evitar mantener tanto bases de datos como cuentas de usuario obsoletas o de prueba.*
8. *Se cuentan con un sistema de respaldos que respalda las bases de datos en caso de falla o pérdida de información.*

Además se tienen:

- Implementadas reglas de FW para cada servidor de base de datos, para bloquear los accesos no permitidos y de esta forma evitar modificaciones no autorizadas, maliciosos o accidentales.
- Sistema anti-virus y anti-spyware actualizado con el fin de evitar un incidente de seguridad en la red que ponga en peligro los datos almacenados en los servidores.
- Herramientas de detección de intrusos para evitar que trafico malicioso llegue a los servidores.
- Parcheo “virtual” para evitar que sean explotadas las vulnerabilidades en los servidores que alojan las Bases de datos.
- Monitoreo permanente de los servidores y aplicaciones con el fin de mantener su disponibilidad.
- Actualización de las herramientas de seguridad para la detección oportuna de nuevas amenazas.

- Respaldos periódicos (diarios y semanales, totales o incrementales según sea requerido) mediante el Sistema de Respaldo con el fin de en caso necesario recuperar la información.

5. ¿Qué aportes puede hacer la EFS, con relación al tema, desde su propia experiencia?

Cada día se desarrollan nuevos métodos que afectan la seguridad de la información por lo que se requiere contar con una estrategia completa de seguridad alineada con los objetivos de negocio. Con el fin de fortalecer la seguridad de la información, la ASF está empujando que las aplicaciones cumplan con el modelo SOA, mismo que establece que el acceso a la base de datos debe de ser solamente desde la capa aplicativa. Los accesos de usuarios a las bases de datos no son permitidos ni promovidos. De esta forma las aplicaciones conocidas como Cliente-servidor deben de ser en lo posible, sustituidas por aplicaciones conformes al modelo SOA.

II. SEGURIDAD INFORMÁTICA-SI

Con el fin de examinar el nivel de concientización que las EFS poseen en relación con el tema de seguridad de la Información, se formulan las siguientes preguntas. La respuesta a cada una de ellas conforma el documento de "Colaboración técnica" elaborado y remitido por todas las EFS que participan, para el desarrollo del presente tema técnico en la Asamblea General.

1. ¿En la EFS la información del proceso auditor se maneja digitalmente a través de expedientes electrónicos con niveles de seguridad como firmas electrónicas? No, se digitaliza solo evidencia pero no cuenta con ningún nivel de seguridad para su manejo.

2. ¿En la EFS se utiliza cifrado de datos para almacenamiento en bases de datos y/o transmisión de los mismos? No se utiliza cifrado en la base de datos ni el almacenamiento central. Los discos duros portátiles de los auditores de campo están cifrados y toda la comunicación y transmisión de información se realiza por medio de la VPN institucional.

3. ¿En la EFS a nivel de aplicaciones, qué seguridad se está aplicando? Para el sistema sustantivo de gestión de información de las auditorías, el Sistema de Control y Seguimientos de Auditorías (SICSA):

    a. Protección en los servidores, de tal forma que:
        i. Se cuenta con reglas para lograr que solo se acceda a los servidores desde direcciones IP autorizadas.
        ii. Se cuenta con reglas que evitan que sean explotadas las vulnerabilidades en los servidores, bloqueando las conexiones que se realicen con este fin.
        iii. Se analizan todos los archivos que se almacenan y ejecutan en el servidor con el fin de evitar una infección.
        iv. Se monitorizan servicios importantes para las aplicaciones en los servidores.

    b. Para el acceso al sistema se hace una doble verificación:
        i. Que el usuario esté dado de alta en el Directorio Activo, lo cual implica que es un empleado vigente de la institución.
        ii. Que el usuario cuente con permiso de acceso al SICSA.
        iii. Por otra parte, se requiere un permiso para ingresar a cada módulo del sistema y un permiso para cada rol (elaborador, revisor, aprobador, etc.) dentro del mismo.
    c. Para impedir que los usuarios tengan acceso a toda la información de los sistemas, también se aplican permisos por centros de trabajo de manera que cada usuario sólo puede ver la información perteneciente a su área y nivel.
    d. Ningún usuario tiene acceso directo a las bases de datos; el sistema informático se encarga de gestionar las peticiones de lectura y escritura a las bases de datos y es el único que puede tener acceso directo a la información.

4. ¿La EFS cuenta con procedimientos estandarizados para adquisición, desarrollo y/o mantenimiento de software, que garanticen niveles de seguridad de la(s) aplicación(es)? ¿Cuáles? La Dirección General de Sistemas (DGS) de la Auditoría Superior de la Federación tiene, entre otras atribuciones, las siguientes:

    a. Establecer las normas y emitir las políticas en materia de tecnologías de información, comunicaciones y seguridad informática

de la Auditoría Superior de la Federación, previa aprobación de su superior jerárquico.

b. Desarrollar e implantar los sistemas informáticos de la Auditoría Superior de la Federación y, en su caso, proponer la contratación de servicios externos complementarios;
c. Asesorar técnicamente a las unidades administrativas para que adquieran y administren directamente recursos informáticos, sistemas y licencias de software de aplicación específica, incluidos su mantenimiento y actualización;

Para el ejercicio de estas atribuciones, la DGS ha implementado un lineamiento para la solicitud de desarrollo o mantenimiento de sistemas y en general todo desarrollo informático que requieran las áreas usuarias de la institución. Este lineamiento prevé el llenado de un formato de solicitud en donde el requirente de un desarrollo o mantenimiento expone en términos generales su solicitud, especificando, entre otros aspectos administrativos, lo siguiente:

- Los objetivos del requerimiento.
- Descripción del problema que resuelve, la oportunidad de mejora o la necesidad que cubre el requerimiento.
- Descripción de los beneficios esperados del proyecto.
- Descripción de los riesgos en caso de no instrumentarse el requerimiento.
- Descripción general del requerimiento.
- Proporcionar los diagramas de flujo o diagrama de actividades que son la representación gráfica de los procesos principales. Un diagrama de actividades muestra el flujo de control general.
- Proporcionar la descripción de las posibles salidas o reportes para una consulta adecuada.
- Definición del responsable del seguimiento al requerimiento.

Las solicitudes que se hacen llegar a la DGS son analizadas internamente y evaluadas las posibles soluciones, analizados los riesgos y los costos de la solución. Una vez decidida la solución, se hace el desarrollo interno, la adquisición de software o la contratación de desarrollos externos. Independientemente de la vía de solución que se decida, en las especificaciones de la misma se incluyen todos los aspectos relativos a la seguridad de la información y de la operación de los sistemas. Ademas, Únicamente se pueden usar bases de datos SQL Server u Oracle, usándose solo las últimas 2 versiones que el fabricante del software soporte.

No se promueve el desarrollo de software basado en herramientas de tipo libre.

Las herramientas de software solo pueden ser adquiridas con el VoBo técnico de la Dirección General de Sistemas

5. ¿La EFS cuenta con mecanismos de seguimiento, evaluación y control al cumplimiento de los procedimientos definidos? Especifique. La ASF cuenta con un área interna que se encarga de realizar seguimiento puntual y coordinación a la gestión. Adicionalmente se cuenta con la Unidad de Evaluación y Control que depende de la Cámara de Diputados y que realiza auditorías periódicas a los diferentes procesos definidos. La ASF cuenta con certificación ISO9001-2008 por lo que periódicamente está sujeta a la recertificación por parte del despacho externo.

6. ¿Existen leyes nacionales para reglamentar la recolección, uso y procesamiento de la información personal? Si existen Leyes para la protección de datos personales. La ley que reglamenta la recolección, uso y procesamiento de la información personal es la Ley Federal de Protección de Datos Personales en Posesión de los Particulares y el encargado de asesorar y vigilar su cumplimiento es el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI).

7. ¿A nivel nacional existen leyes o códigos aplicables que contengan los requerimientos generales de seguridad para los proveedores de servicios de “hosting” de información digital y de nube? Por lo que se refiere a la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, incluye una disposición específica en su artículo 22, relativo a la excepción al consentimiento para proporcionar datos personales a terceros, cuya fracción V indica:

   “A terceros cuando se contrate la prestación de un servicio que requiera el tratamiento de datos personales. Dichos terceros no podrán utilizar los datos personales para propósitos distintos a aquéllos para los cuales se les hubieren transmitido.”

   Por su parte, el artículo 47 del Reglamento de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental establece que “los procedimientos para acceder a los datos personales que estén en posesión de las dependencias y entidades deben garantizar la protección de los derechos de los individuos, en particular, a la vida privada y a la intimidad, así como al acceso y corrección de sus datos personales, de

conformidad con los lineamientos que expida el Instituto y demás disposiciones aplicables para el manejo, mantenimiento, seguridad y protección de los datos personales".

Ref: "La nube: nuevos paradigmas de privacidad y seguridad para un entorno innovador y competitivo". (https://cidecyd.files.wordpress.com/2014/05/la-nube-nuevos-paradigmas-de-privacidad-y-seguridad-para-un-entorno-innovador-y-competitivo.pdf)

8. ¿Qué aportes puede hacer la EFS, con relación al tema, desde su propia experiencia? Debe desarrollarse un plan integral que inicie desde que una persona es contratada en la EFS hasta que se vuelva parte de su día con día, es decir se haga cultura.

   Para lo anterior siendo conceptos universales, se propone crear un grupo enfocado al desarrollo de materiales de concientización en Seguridad de la Información. (Guías, tutoriales, videos etc.)

III. BUENAS PRÁCTICAS DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

Con el fin de consolidar y compartir las buenas prácticas que las EFS poseen en relación con el tema, se formulan las siguientes preguntas. La respuesta a cada una de ellas conforma el documento de "Colaboración técnica" elaborado y remitido por todas las EFS que participan, para el desarrollo del presente tema técnico en la Asamblea General.

1. ¿Existe una Política de seguridad adoptada institucionalmente por la EFS? ¿Desde qué año? Desde hace más de 6 años se inició. A nivel interno, la EFS ha desarrollado su propia Normativa institucional, en la cual hay lineamientos acerca de los siguientes temas:
   - Uso de bienes informáticos
   - Soporte Técnico
   - Uso de Internet
   - Uso de software
   - Gestión de la infraestructura tecnológica
   - Uso de servicios de comunicación electrónica

2. ¿La EFS cuenta con una metodología para gestión de incidentes de seguridad? ¿Cuál? No se cuenta con una metodología.

3. ¿La EFS cuenta con una metodología para el análisis de vulnerabilidades y gestión de riesgo? ¿Cuál? No se cuenta con una metodología, sin embargo de manera periódica se realiza un escaneo de vulnerabilidades con las herramientas Qualys Guard y Deep Security para la aplicación de los parches virtuales y/o físicos. Para la evaluación de riesgos se utiliza la herramienta Modulo Risk Management que automatiza el proceso de análisis de riesgo por medio de la identificación, análisis, evaluación y tratamiento de los riesgos detectados.

4. ¿La EFS ha realizado pruebas de la efectividad del Plan de Continuidad del Negocio y recuperación de desastres? Se cuenta con un sistema de respaldo y recuperación, y un sitio alterno con el que se han realizado pruebas para la restauración de las aplicaciones y de la información. Actualmente se está trabajando para establecer el sitio alterno de operación para ASF esté hospedado en una instalación alterna (diferente a edificios de la ASF) dentro un marco de un acuerdo de mutua cooperación.

5. Según las pruebas de la pregunta 4. ¿En la EFS cuál es el tiempo promedio para restablecer la operación de la infraestructura tecnológica y dar continuidad al Negocio? Promedio de 6 horas para restablecer la operación de la aplicación sustantiva principal. Otras aplicaciones a restaurar están por ser definidas.

6. ¿La EFS tiene clasificada la información producida y recibida (Confidencial, publica, etc.)?

   La información no se encuentra clasificada.

7. ¿La EFS cuenta con Acuerdos de privacidad, niveles de servicio (NDA, SLA), etc.? Sí, y los mismos se muestran plasmados en los contratos que se tienen firmados con los proveedores de servicio.

8. ¿La EFS tiene establecido un Plan de respuesta a incidentes? No se cuenta con un plan de respuesta a incidentes.

9. ¿En la EFS se realiza auditoría externa/interna a la gestión de incidentes de seguridad informática?. No se tiene un proceso formal para la gestión de incidentes de seguridad.

10. ¿Existe el compromiso de la alta dirección de la EFS con respecto a la seguridad de la información? Sí. La ASF tiene implementadas medidas técnicas que permiten la protección de la información y de los sistemas del acceso, uso, divulgación, interrupción o destrucción no autorizada.

11. ¿Qué aportes puede hacer la EFS, con relación al tema, desde su propia experiencia? El usuario es el eslabón más débil de la seguridad, por lo que si no se cuenta con un programa de concientización en seguridad, no existirá herramienta capaz de proteger la información. La Alta Dirección, por el tipo de información que maneja, es la más vulnerable, por lo que se requiere de su compromiso y ejemplo para fortalecer la seguridad en todos los niveles.

IV. EQUIPO DE RESPUESTA A INCIDENTES DE SEGURIDAD INFORMÁTICA (CSIRT-COMPUTER SECURITY INCIDENT & RESPONSE TEAM)

Con el fin de compartir y evaluar el avance que las EFS poseen en relación con el tema, se formulan las siguientes preguntas. La respuesta a cada una de ellas conforma el documento de “Colaboración técnica” elaborado y remitido por todas las EFS que participan, para el desarrollo del presente tema técnico en la Asamblea General.

1. ¿La EFS cuenta con personal especializado en seguridad informática? Sí. El personal encargado de la seguridad de la ASF cursó un Diplomado en Seguridad Informática y se encuentra capacitado en la administración de las herramientas de seguridad con las que cuenta actualmente la ASF. Adicionalmente se cuenta con personal certificado en *Comptia Security Certified* y en las herramientas de seguridad de *Trend Micro*. La Dirección General de Sistemas, promueve la actualización en tema de seguridad de su personal

2. ¿Se encuentra implementado un grupo de seguridad de la información para realizar monitoreo y/o atención de incidentes? No existe un grupo creado con ese objetivo: monitorear y atender los incidentes de información.

3. ¿Se encuentra institucionalizado el grupo de seguridad de la EFS? No, no está institucionalizado.

4. ¿Qué plataformas se utilizan para seguridad perimetral, monitoreo y/o correlación de eventos de seguridad de la información? Para la seguridad perimetral, se trabaja con la tecnología Palo Alto Networks a través de su solución PA-3020. La iniciativa para adquirir una herramienta de correlación de eventos está en análisis.

5. ¿La infraestructura de monitoreo y seguridad que posee la EFS se encuentra: tercerizada, en la nube, local, otra (Especifique)? La infraestructura se encuentra instalada y operando de forma local, aunque se cuenta con algunos servicios administrados específicamente para la herramienta Deep Security (seguridad de servidores WINTEL), mismos que operan 7x24, y atienden todos los incidentes de seguridad relacionados con los 93 servidores de la EFS.
6. ¿La EFS cuenta con un equipo de respuesta a incidentes de seguridad Informática (CSIRT- Computer Security Incident & Response Team)? No.

7. ¿Se tienen identificados los servicios que va a prestar el CSIRT? No.

8. ¿Se tiene identificado el entorno y el grupo de clientes que atenderá el CSIRT? No

9. En caso de no contar con un equipo de respuesta a Incidentes de Seguridad Informática, ¿la EFS cuenta con procedimientos de monitoreo a incidentes de Seguridad Informática? Sí, y el mismo está implementado y se apoya en las consolas de monitoreo de las herramientas de seguridad informática con las que cuenta la EFS (Antivirus Trend Micro, Firewall Palo Alto, Filtrado de contenido web Websense, Filtrado de e-mail IMSVA).

10. ¿Se realiza seguimiento a los incidentes de seguridad que se han presentado en la EFS? Sí, para los servidores se cuenta con el monitoreo de las herramienta de seguridad Deep Security, el firewall, la herramienta de filtrado web y el antivirus institucional. En caso de detectar violaciones de seguridad, se realiza la investigación y se aplican acciones correctivas que surjan de este proceso. Se continúa con el monitoreo hasta su solución.

Para el caso de los equipos de los usuarios que llegan a presentar algún incidente de virus y en caso de que internamente la herramienta de antivirus no lo pueda solucionar, se obtienen muestras del equipo para que sean analizadas por el fabricante y obtener el patrón que resuelve el incidente. Una vez liberado el patrón, se manda la actualización a todos los equipos de la ASF. Es importante mencionar que los equipos del usuario final reciben hasta tres actualizaciones al día.

11. ¿Se toman acciones preventivas a los incidentes de seguridad registrados en la EFS? Si, y del análisis de la causa raíz del incidente, se desprenden políticas, lineamientos o mejoras en la operación. Algunos casos específicos son:
    a. Se realizan verificaciones periódicas del estado de la plataforma de seguridad para analizar nuevas vulnerabilidades y brechas de seguridad.
    b. En los servidores se aplican los parches virtuales que los protegen de nuevas vulnerabilidades, para posteriormente realizar la aplicación física de los mismos.
    c. Para los equipos de los usuarios finales, se mantienen actualizados los patrones antivirus para mantenerlos protegidos de códigos maliciosos.

12. ¿La información de los incidentes de seguridad es reportada a nivel de la Alta Dirección en la EFS? Sí. Se emiten reportes mensuales que se presentan a la Alta Dirección.

13. ¿La EFS cuenta con la figura de Oficial de Seguridad Informática? No se encuentra establecido de manera formal.

14. ¿Existe en el país una estrategia o política pública para implementar un mecanismo de ciberseguridad / ciberdefensa? Existe una estrategia a nivel Gobierno Federal, administrada por el comité de Seguridad Nacional, el cuan contempla una estrategia para el manejo de posibles crisis de ciberseguridad, también delinea los pasos a seguir para prevenir un incidente y que hacer en caso de un ataque serio.

15. ¿Existe a nivel nacional un equipo de respuesta a incidentes de seguridad informática (CSIRT)? Sí, conformado por diferentes entidades de la Administración Pública Federal bajo un comité de Seguridad Nacional.

V. MECANISMOS DE SEGURIDAD PARA INTERCAMBIO DE INFORMACIÓN

Con el fin de compartir y evaluar mecanismos de seguridad implementados por las EFS, para intercambiar información interna o externamente, se formulan las siguientes preguntas. La respuesta a cada una de ellas conforma el documento de “Colaboración técnica” elaborado y remitido por todas las EFS que participan, para el desarrollo del presente tema técnico en la Asamblea General.

1. A efectos de evitar la acción de amenazas ocasionadas por la proliferación de software malicioso como virus, malware, troyanos, spam, etc., ¿qué medidas de prevención, ha adoptado o implementado la EFS?
    a. Protección en el correo electrónico:
        i. Los correos externos lleguen sin virus al buzón del usuario.
        ii. Solo se acepten correos cuyo destinatario sea un usuario del dominio de ASF.
        iii. No se acepten desde su conexión, correos basura o no solicitados.
        iv. Se puedan filtrar aquellos correos con contenido difamatorio o que dañen la reputación de la ASF.

    b. Protección en los servidores:
        i. Se cuenta con reglas para lograr que solo se acceda a los servidores desde direcciones IP autorizadas.
        ii. Se cuenta con reglas que evitan que sean explotadas las vulnerabilidades en los servidores, bloqueando las conexiones que se realicen con este fin.
        iii. Se analizan todos los archivos que se almacenan y ejecutan en el servidor en busca de virus o código malicioso, con el fin de evitar una infección.
        iv. Se cuenta con herramientas para detección de tráfico inválido
        v. Se monitorizan servicios importantes para las aplicaciones en los servidores.
    c. Antivirus en los equipos de cómputo:
        i. Detección y limpieza de código malicioso.
        ii. Protección que evita la ejecución de archivos desde unidades de almacenamiento USB.
        iii. Protección que evita la modificación de archivos del sistema o de configuraciones en el Internet Explorer.

iv. Detección y bloqueo de conexiones maliciosas hacia servidores de comando y control.
v. Bloqueo de URLs maliciosas.
vi. Monitoreo para asegurar que todos los equipos cuenten con antivirus.

2. ¿La EFS realiza intercambio de información sensible a través de la red de datos interna o web Institucional? En la red de datos interna y en algunas aplicaciones en web viaja información sensible, por ejemplo, en la web está el sistema de Línea Ética de Denuncia que registra información sensible.

   También hay un sistema en web para el registro de información que cargan las Entidades de Fiscalización de las 32 entidades federativas del país. En ambos casos se utiliza un protocolo seguro de transferencia de hipertexto (https) para establecer un canal cifrado.

3. ¿Se ha concientizado al usuario final interno y externo de la EFS sobre la seguridad en Internet? Se emiten cápsulas informativas concientizando sobre los riesgos de seguridad., a través de boletines informativos que llegan al usuario a través del correo electrónico o por medio de las pantallas de difusión de información para empleados.

4. ¿Conoce el usuario final interno y externo de la EFS sobre las diferentes modalidades de robo de datos o de información a través de la WEB? Si, a través de boletines informativos que llegan al usuario a través del correo electrónico o por medio de las pantallas de difusión de información para empleados. Existe una cultura de seguridad informática al interior de la EFS? No, pero se está trabajando en ello.

5. ¿Qué aportes puede hacer la EFS, con relación al tema, desde su propia experiencia? En la ASF se han instrumentado sistemas en arquitectura web y se ha hecho una combinación de uso de protocolo https, registro a través de usuario y contraseña y en algunos casos, encriptado de datos. En sistemas donde el usuario debe enviar un formulario solicitando información, se ha instrumentado también la solicitud de ingresar algún código mediante el mecanismo captcha. Con estos mecanismos no hemos tenido contratiempos de seguridad.

VI. CONVENIOS DE COOPERACIÓN O INTERADMINISTRATIVOS DE INTERCAMBIO DE INFORMACIÓN ENTRE ENTIDADES DE CONTROL DEL PAÍS O NORMATIVIDAD PARA REGLAMENTAR EL TEMA.

Conocer qué se ha hecho y cómo, qué se tuvo en cuenta en su realización, con qué propósito, que lineamientos se tienen, con qué normatividad se cuenta, etc., son inquietudes que surgen con el desarrollo del tema de seguridad; es por ello que se formulan las siguientes preguntas con el fin de compartir y evaluar el avance que las EFS poseen en relación con el tema. La respuesta a cada una de ellas conforma el documento de "Colaboración técnica" elaborado y remitido por todas las EFS que participan, para el desarrollo del presente tema técnico en la Asamblea General.

1. ¿Existen convenios interadministrativos para el intercambio de información entre Entidades de Control en el país? Si existen, por ejemplo el Acuerdo por el que se establece el Esquema de Interoperabilidad y de Datos Abiertos de la Administración Pública Federal, con el objetivo siguiente:

   El Esquema de Interoperabilidad y de Datos Abiertos de la Administración Pública Federal, tiene por objeto determinar las bases, principios y políticas que deberán observar las dependencias, las entidades y la Procuraduría General de la República, para la integración de los procesos relacionados con servicios digitales, así como para compartir y reutilizar plataformas y sistemas de información, a fin de incrementar la eficiencia operativa de la Administración Pública Federal y su relación con la sociedad.

   Referencia: Diario Oficial de la Federación, del 6 de septiembre de 2011: http://dof.gob.mx/nota_detalle.php?codigo=5208001&fecha=06/09/2011

2. ¿Existe normatividad que reglamente el tema de intercambio de información entre las entidades de Control del país? Si existen, y esa normatividad es emitida por entidades como la Unidad de Gobierno Digital, cuyo objetivo es instrumentar, fomentar y promover la utilización de las Tecnologías de la Información y Comunicaciones en los procesos de la Administración Pública Federal, para fortalecer la gestión pública y mejorar la entrega de servicios a la sociedad.

Además, existe la Comisión Intersecretarial para el Desarrollo del Gobierno Electrónico (CIDGE), que es un órgano estratégico para el Desarrollo del

Gobierno Electrónico. Su objetivo es: Promover y consolidar el uso y aprovechamiento de las Tecnologías de la Información y Comunicaciones (TIC´s) en la Administración Pública Federal.

3. ¿La EFS de su país realiza intercambio de información almacenada en base de datos con **otras EFS**? ¿De qué tipo? Existen algunos sitios web en los que se registra y consulta información por parte de otras EFS. Esta información reside en bases de datos protegidas.

La ASF de México como presidencia del Grupo de Trabajo sobre el Valor y Beneficio de las EFS de INTOSAI, y previamente como presidencia de la Task Force sobre la base de datos con información de las EFS, tuvo el mandato de la INTOSAI para crear una base de datos con información actualizada y específica sobre las EFS del mundo. Estas informaciones abarcan, entre otras, la estructura de organización, criterios de administración y gestión, mandatos, atribuciones legales e información relevante acerca de los métodos de auditoría.

El objetivo de esta herramienta, fácil de utilizar para todos los miembros de la INTOSAI y el público, consiste en demostrar las similitudes y diferencias de todas las EFS del mundo.

En OLACEFS, 19 EFS respondieron un cuestionario electrónico cuya fecha límite fue el 30 de noviembre de 2013, el cual fue el medio de recopilación de la información que conforma el sitio: www.intosai-database.org.mx

Es un sitio web público, pero para efectos de carga de información de los cuestionarios, cada EFS cuenta con su propio usuario y contraseña para el acceso a la herramienta.

4. ¿La EFS de su país realiza intercambio de información almacenada en base de datos **con otros organismos internacionales**? ¿De qué tipo? Existen algunos sitios web en los que se registra y consulta información por parte de otras EFS. Esta información reside en bases de datos protegidas.

Con organismos internacionales aún no hay colaboración para generar una base como tal, sin embargo existe en
Ejemplos son el sitio del Grupo de Trabajo sobre Deuda Pública, del INTOSAI (http://www.wgpd.org.mx) y el Glosario en Línea con Terminología de Fiscalización de la INTOSAI (http://www.intosaiglossary.org.mx/Main.aspx

5. ¿Existe intercambio de información sensible de la EFS desde/hacia entidades gubernamentales? ¿De qué tipo? Hasta el momento la información sensible no se intercambia mediante mecanismos electrónicos. Se maneja a través de papel o mediante discos digitales físicos (CD, DVD).

6. ¿Qué aportes considera que la EFS puede hacer, con relación al tema, desde su propia experiencia? Se está analizando un proyecto para incorporar a la ASF en la plataforma de interoperabilidad de la Oficina Postal Electrónica (OPE), que busca la integración de los Sistemas Automatizados de Control de Gestión de las Dependencias Federales, permitiendo así el intercambio de oficios electrónicos legalmente válidos y garantizando el control de flujo de todos los mensajes de interoperabilidad del control de gestión.