APORTES TEMA TECNICO N°2
EFS CONTRALORÍA GENERAL DE LA REPÚBLICA DE COLOMBIA
XXV ASAMBLEA GENERAL ORDINARIA - OLACEFS

1. 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?

   R. Almacenamiento 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?

   R. Si. En base de datos, herramientas como IDEA, SPSS Modeler, ArcGIS

3. ¿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.)

   R. Si. Falta de estandarización en formatos

4. ¿Se han presentado fallas en la seguridad sobre la información almacenada en los archivos de bases de datos?

   R. Disponibilidad

5. ¿La EFS tiene establecidos protocolos para garantizar la seguridad en la información almacenada? ¿Cuáles?

   R. Autenticación, Autorización, Replicación, políticas de seguridad, aplicación de parches de software y seguridad física.

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

2. INFORMACIÓN PUBLICADA EN INTERNET O COMPARTIDA ENTRE EFS.

Con el fin de conocer el tipo y categorías de información que las EFS hacen pública a través de Internet o la que es compartida por este mismo medio o por canales privados, 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 publica información misional a través de Internet?

   R. Si. Misional sobre los resultados del proceso auditor, Plan estratégico, misión, visión institucionales, presupuestal y financiera nacional, capacitación y contratación.

2. ¿La EFS ofrece servicios web a través de su propio portal de Internet?

   R. Si. Certificaciones, denuncias y contratación

3. ¿La EFS considera tener controlados todos los incidentes de seguridad que han ocurrido en la red de datos?

   R. Si. Controles preventivos gestionados a través de la plataforma SOC

4. ¿La EFS propende por el correcto y seguro funcionamiento de las instalaciones de procesamiento de la información y medios de comunicación?

   R. Si. Normas y Procedimientos

5. ¿Existe un plan a nivel nacional para ingreso a IPv6 en la que esté involucrada la EFS?

   Si. Liderado por el Ministerio de Tecnologías de Información y las Comunicaciones- MinTIC.

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

3. 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?

   R. Si. Expediente electrónico asegurado mediante firma digital

2. ¿En la EFS se utiliza cifrado de datos para almacenamiento en bases de datos y/o transmisión de los mismos?

   R. Se utiliza cifrado de datos en la transmisión, mediante uso del protocolo SSH

3. ¿En la EFS a nivel de aplicaciones, qué seguridad se está aplicando?

   R. Autenticación. Autorización y Auditoria - AAA, monitoreo de puertos y protección perimetral

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?

   R. Se cuenta con manual contratación y procedimiento para desarrollo y mantenimiento de software.

5. ¿La EFS cuenta con mecanismos de seguimiento, evaluación y control al cumplimiento de los procedimientos definidos? Especifique.

   R. Si. Verificación de cumplimiento de requerimientos y auditorias de control interno.

6. ¿Existen leyes nacionales para reglamentar la recolección, uso y procesamiento de la información personal?

   R. Ley de protección de datos personales, Comercio electrónico

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?

R. Se desconoce

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

4. 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?

   R. Si. Política de seguridad aprobada en Comité Directivo el 29 de mayo de 2013.

2. ¿La EFS cuenta con una metodología para gestión de incidentes de seguridad? ¿Cuál?

   R. Si. CSISO

3. ¿La EFS cuenta con una metodología para el análisis de vulnerabilidades y gestión de riesgo? ¿Cuál?

   No. Pero se siguen algunos procedimientos sugeridos en las ISO 31000 e ISO 27000

4. ¿La EFS ha realizado pruebas de la efectividad del Plan de Continuidad del Negocio y recuperación de desastres?

   R. Si. En diciembre de 2014.

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?

   R. 7 horas

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

   Si. Clasificación de los documentos como confidenciales o públicos

7. ¿La EFS cuenta con Acuerdos de privacidad, niveles de servicio (NDA, SLA), etc.?

Si. NDA y SLA

8. ¿La EFS tiene establecido un Plan de Respuesta a Incidentes?

   R. Si

9. ¿En la EFS se realiza Auditoría externa/interna a la gestión de incidentes de seguridad informática?

   R. No

10. ¿Existe el compromiso de la alta dirección de la EFS con respecto a la seguridad de la información?

    R. Si. Alto compromiso Institucional y nacional. Fue creada la Unidad de Seguridad y Aseguramiento Tecnológico mediante la expedición de la Ley 1474 de 2011.

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

5. 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?

   Si. Entre 2012 y 2014 se formaron como especialistas 27 profesionales, de diferentes dependencias de la CGR de Colombia.

2. ¿Se encuentra implementado un grupo de seguridad de la información para realizar monitoreo y/o atención de incidentes?

   Si. La dependencia especializada en el tema es la Unidad de Seguridad y Aseguramiento Tecnológico. Además, la Oficina de Sistemas e Informática cuenta con el grupo de trabajo Security Operation Center – SOC (Centro de Operaciones de Seguridad).

3. ¿Se encuentra institucionalizado el grupo de seguridad de la EFS?

   Si. A través de la Ley 1474 de 2011

4. ¿Qué plataformas se utilizan para seguridad perimetral, monitoreo y/o correlación de eventos de seguridad de la información?

   Fortinet, Imperva, Alient Vault, Fsecure, PCsecure.

5. ¿La infraestructura de monitoreo y seguridad que posee la EFS se encuentra: tercerizada, en la nube, local, otra (Especifique)?

   R. Local

6. ¿La EFS cuenta con un equipo de respuesta a incidentes de seguridad Informática (CSIRT-Computer Security Incident & Response Team)?

   R. No, pero se cuenta con la Unidad de Seguridad y Aseguramiento Tecnológico y con el grupo SOC de la Oficina de Sistemas

7. ¿Se tienen identificados los servicios que va a prestar el CSIRT?

   R. Si.

8. ¿Se tiene identificado el entorno y el grupo de clientes que atenderá el CSIRT?

   R. Si. Se tiene identificación de los stakeholders internos y externos.

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?

   R. Si. Establecidos en la Metodología CSISO

10. ¿Se realiza seguimiento a los incidentes de seguridad que se han presentado en la EFS?

    R. Si

11. ¿Se toman acciones preventivas a los incidentes de seguridad registrados en la EFS?

    R. Si.

12. ¿La información de los incidentes de seguridad es reportada a nivel de la Alta Dirección en la EFS?

    R. Si. Mensualmente se generan informes del SOC, sobre monitoreo e incidentes de seguridad. Los informes se remiten a solicitud y trimestralmente a la Oficina de Planeación de la CGR de Colombia.

13. ¿La EFS cuenta con la figura de Oficial de Seguridad Informática?

    R. No

14. ¿Existe en el país una estrategia o política pública para implementar un mecanismo de ciberseguridad / ciberdefensa?

    Si. Liderada por el ColCERT Colombia, la Cámara Colombiana de Informática y Telecomunicaciones y el MinTIC, para que sea implementada en todas las entidades del sector gobierno.

15. ¿Existe a nivel nacional un equipo de respuesta a incidentes de seguridad informática (CSIRT)?

    Si. ColCERT administrado por la Policía Nacional.

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

6. 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?

   R. La Entidad cuenta con Política de Seguridad implementada. A nivel de red, se tiene implementada la plataforma de seguridad perimetral mediante firewall, IDS, IPS; además, se cuenta con la plataforma de monitoreo y gestión de seguridad donde se hace monitoreo y seguimiento a amenazas o incidentes que se presentan sobre la infraestructura de la red de datos. Se monitorean bases de datos, aplicaciones y a nivel de PC's se hace detección y prevención mediante el uso de antivirus y antispam. Adicionalmente se cuenta con herramienta que impide la ejecución de programas no autorizados institucionalmente.

2. ¿La EFS realiza intercambio de información sensible a través de la red de datos interna o web Institucional?

   R. Si. A través de la red de datos (SIIF Nación)

3. ¿Se ha concientizado al usuario final interno y externo de la EFS sobre la seguridad en Internet?

   R. Si. El Ministerio de Tecnologías de Información y Comunicaciones permanentemente hace campañas de prevención dirigida a toda la población, sobre uso de Internet Seguro. Además, se cuanta con portales dirigidos a la población infantil.

   Internamente, se publican tips de seguridad, bien sea a través de las carteleras, de correo electrónico o por la Intranet.

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?

   R. Mediante las campañas institucionales y por la divulgación que hace el Gobierno Nacional por los diferentes medios de comunicación, si se tiene conocimiento.

5. Existe una cultura de seguridad informática al interior de la EFS?

   R. SI. Con la divulgación de políticas institucionales y gubernamentales.

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

7. 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?

   R. Si. Realizados para la ejecución de procesos de Investigaciones, Juicios Fiscales y Jurisdicción Coactivo.

2. ¿Existe normatividad que reglamente el tema de intercambio de información entre las entidades de Control del país?

   R. No.

3. ¿La EFS de su país realiza intercambio de información almacenada en base de datos con otras EFS? ¿De qué tipo?

   R. No.

4. ¿La EFS de su país realiza intercambio de información almacenada en base de datos con otros organismos internacionales? ¿De qué tipo?

   R. No.

5. ¿Existe intercambio de información sensible de la EFS desde/hacia entidades gubernamentales? ¿De qué tipo?

   R. Si. Se hace intercambio de información de tipo financiero, fiscal, bancaria, de activos, entre otros.

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

CONTRALORÍA
GENERAL DE LA REPÚBLICA

Proyectó: Eliana Zamora Caro
Zoila Emperatriz Calderón Padilla

Revisó: