República de Panamá

Contraloría General de la República

Panamá, 25 de junio de 2015

Nota Núm.637-15-DCC-UAI

Doctor
EDGARDO MAYA VILLAZÓN
Contralor General de Colombia
Presidente de la Comisión de Tecnologías de la
Información y las Comunicaciones de la OLACEFS
E. S. D.

Señor Contralor:

Tengo el agrado de dirigirme a usted a fin de referirme al oficio 2015EE0053344, por medio del cual se solicitó el envío de colaboraciones para el desarrollo del **Tema Técnico N° 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"**, que será abordado en la XXV Asamblea General Ordinaria, a desarrollarse en la ciudad de Querétaro, México.

Al respecto, nos complace remitirle nuestros aportes al citado tema, esperando que dicha información enriquezca el Documento Guía que ha preparado su distinguida Entidad Fiscalizadora Superior, en calidad de Presidencia de la Comisión de Tecnologías de la Información y las Comunicaciones.

Hago propicia la ocasión para expresarle nuestras muestras de consideración y estima.

Atentamente,

FEDERICO A. HUMBERT
Contralor General

REPÚBLICA DE PANAMÁ
DESPACHO DEL CONTRALOR
CONTRALORÍA GENERAL DE LA REPÚBLICA

REPÚBLICA DE PANAMÁ
CONTRALORÍA GENERAL DE LA REPÚBLICA DE PANAMÁ

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

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

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 base de datos se encuentra 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?
En estos aspectos nos encontramos en una fase incipiente.

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.)
Contamos con diferentes plataformas, y las estaciones de trabajo a nivel institucional mantienen licencias de diferentes versiones.

4. ¿Se han presentado fallas en la seguridad sobre la información almacenada en los archivos de bases de datos?
No se tienen conocimientos de fallas hasta el momento.

5. ¿La EFS tiene establecidos protocolos para garantizar la seguridad en la información almacenada? ¿Cuáles?
Se cuentan con respaldos diarios de la información en el caso de las Bases de Datos y periódicos con respecto a información de servidores de datos.

6. ¿Qué aportes puede hacer la EFS, con relación al tema, desde su propia experiencia?
Se negocia con herramientas a nivel del Estado con la Autoridad de Innovación Gubernamental de Panamá, para poder elaborar estándares.

B. INFORMACIÓN PUBLICADA EN INTERNET O COMPARTIDA ENTRE EFS.

1. ¿La EFS publica información misional a través de Internet?
La información institucional es publicada en la página WEB.

2. ¿La EFS ofrece servicios web a través de su propio portal de Internet?
Se ofrecen servicios como el acceso de aplicaciones para colaboradores y el trámite de certificado de trabajo a los ciudadanos.

3. ¿La EFS considera tener controlados todos los incidentes de seguridad que han ocurrido en la red de datos?
En este aspecto nos encontramos en desarrollo. Estamos tratando de estar al día.

4. ¿La EFS propende por el correcto y seguro funcionamiento de las instalaciones de procesamiento de la información y medios de comunicación?
Estamos anuentes de la necesidad de reforzar constantemente los procedimientos actuales.

5. ¿Existe un plan a nivel nacional para ingreso a IPv6 en la que esté involucrada la EFS?
Actualmente no. Tampoco la Red Multiservicio desarrollada por la Autoridad de Innovación Gubernamental de Panamá, está orientada a IPV6.

6. ¿Qué aportes puede hacer la EFS, con relación al tema, desde su propia experiencia?
Actualmente, estamos abiertos a recibir recomendaciones de las EFS que tengan mayor experiencia en el tema.

C. SEGURIDAD INFORMÁTICA-SI

1¿En la EFS la información del proceso auditor se maneja digitalmente a través de expedientes electrónicos con niveles de seguridad como firmas electrónicas?
El proceso fiscalizador cuenta con un Sistema de Seguimiento, Control, Acceso y Fiscalización de Documentos (SCAFID); y no maneja firmas electrónicas.

2. ¿En la EFS se utiliza cifrado de datos para almacenamiento en bases de datos y/o transmisión de los mismos?
Para almacenamiento en base de datos sólo se utilizan las contraseñas.
En ciertas aplicaciones publicadas en la web (las que tienen que ver con aplicaciones en línea), se utiliza el cifrado.

3. ¿En la EFS a nivel de aplicaciones, qué seguridad se está aplicando?
Se cuenta con el Sistema de Seguridad para Aplicaciones para aplicaciones Externas – SSAE; el cual permite el acceso a diferentes aplicaciones a través de una única cuenta de usuario (cédula) y contraseña, verifica el acceso y la asignación de Roles.

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?
A través del Sistema de Gestión de Calidad ISO 9001:2008, se manejan dos grandes mapas de procesos. Los procedimientos estandarizados para el punto 7. Realización del Servicio, sustentan al mapa de Diseño, Desarrollo e Implementación de Soluciones Tecnológicas.

5. ¿La EFS cuenta con mecanismos de seguimiento, evaluación y control al cumplimiento de los procedimientos definidos? Especifique.
A través de las Auditorías Internas de Calidad, sustentadas en el punto 8.2.2 del Manual de Calidad.

6. ¿Existen leyes nacionales para reglamentar la recolección, uso y procesamiento de la información personal?
Ley 83 del 9 de noviembre de 2012, sobre trámites Gubernamentales y Medios Electrónicos.

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?
La Resolución 14 del 10 de febrero de 2015 de la Autoridad de Innovación Gubernamental lo regula.

8. ¿Qué aportes puede hacer la EFS, con relación al tema, desde su propia experiencia?
A nivel Institucional, se cuenta con:

- Políticas informáticas para la seguridad de la Información.

A nivel de Infraestructura, se cuenta con:

- Dispositivos firewall con servicios de antivirus, Web filtering y control de aplicaciones a nivel WEB.
- Algunas aplicaciones web cuentan con cifrado para la transmisión de datos.
- Se utilizan mecanismos de VPN sitio a sitio y clientes VPN en sitios remotos.

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

1. ¿Existe una Política de seguridad adoptada institucionalmente por la EFS? ¿Desde qué año?
Se cuenta con Políticas y Guías Generales de Seguridad de la Información para Usuarios Finales, con fecha de Marzo 2010.

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

3. ¿La EFS cuenta con una metodología para el análisis de vulnerabilidades y gestión de riesgo?
¿Cuál?
Actualmente no.

4. ¿La EFS ha realizado pruebas de la efectividad del Plan de Continuidad del Negocio y recuperación de desastres?
Solo se cuenta con un Plan de contingencia en la aplicación que tiene que ver con el Pago de la Planilla Gubernamental.

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?
Con respecto al proceso de pago de la planilla gubernamental, en promedio 4 horas.

6. ¿La EFS tiene clasificada la información producida y recibida (Confidencial, publica, etc.)?
No se cuenta con clasificación de la información.

7. ¿La EFS cuenta con Acuerdos de privacidad, niveles de servicio (NDA, SLA), etc.?
Si cuenta con acuerdos, sólo con algunos proveedores.

8. ¿La EFS tiene establecido un Plan de respuesta a incidentes?
No lo tiene establecido.

9. ¿En la EFS se realiza Auditoría externa/interna a la gestión de incidentes de seguridad informática?
No se realizan.

10. ¿Existe el compromiso de la alta dirección de la EFS con respecto a la seguridad de la información?
Si existe, y se reconoce la situación desventajosa en que nos encontramos.

11. ¿Qué aportes puede hacer la EFS, con relación al tema, desde su propia experiencia?
En estos momentos nos encontramos en una etapa temprana de Buenas Prácticas.

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

1¿La EFS cuenta con personal especializado en seguridad informática?
Actualmente no cuenta con dicho personal especializado.

2. ¿Se encuentra implementado un grupo de seguridad de la información para realizar monitoreo y/o atención de incidentes?
Actualmente no cuenta con dicho grupo.

3. ¿Se encuentra institucionalizado el grupo de seguridad de la EFS?
Actualmente no se encuentra institucionalizado dicho grupo.

4. ¿Qué plataformas se utilizan para seguridad perimetral, monitoreo y/o correlación de eventos de seguridad de la información?
A nivel de seguridad perimetral: plataforma de Fortinet y a nivel de monitoreo de equipos de telecomunicaciones: WhatsUP.

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

6. ¿La EFS cuenta con un equipo de respuesta a incidentes de seguridad Informática (CSIRTComputer Security Incident & Response Team)?
Actualmente no.

7. ¿Se tienen identificados los servicios que va a prestar el CSIRT?
No, hemos solicitado consultorías para orientarnos en este sentido.

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

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?
No cuenta.

10. ¿Se realiza seguimiento a los incidentes de seguridad que se han presentado en la EFS?
Si se da seguimiento, cuando se presenta el caso.

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

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

13. ¿La EFS cuenta con la figura de Oficial de Seguridad Informática?
No cuenta.

14. ¿Existe en el país una estrategia o política pública para implementar un mecanismo de ciberseguridad / ciberdefensa?
La Autoridad de Innovación Gubernamental de Panamá (AIG) cuenta con un departamento para monitorear y advertir de vulnerabilidades. CSIRT Panamá.

15. ¿Existe a nivel nacional un equipo de respuesta a incidentes de seguridad informática (CSIRT)?
CSIRT Panamá creado en el año 2011, tiene como compromiso dar respuestas de incidentes de seguridad informática.

16. ¿Qué aportes puede hacer la EFS, con relación al tema, desde su propia experiencia?
Estamos en conversaciones con DDRH de Contraloría, con respecto a la necesidad de establecer en el organigrama institucional dicha figura.

F. MECANISMOS DE SEGURIDAD PARA INTERCAMBIO DE INFORMACIÓN

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?

Cerrar puertos a nivel de equipos de seguridad perimetral, aplicar control de aplicaciones a nivel WEB y reforzar la seguridad a nivel de antivirus en la Institución.

2. ¿La EFS realiza intercambio de información sensible a través de la red de datos interna o web Institucional?
Se remite información a otra entidad para el pago de la planilla gubernamental.

3. ¿Se ha concientizado al usuario final interno y externo de la EFS sobre la seguridad en Internet?
A través de las Políticas y Guías Generales de Seguridad de la Información para Usuarios Finales, publicadas en el 2010.

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?
No se le ha instruido ni diseminado dicho conocimiento.

5. Existe una cultura de seguridad informática al interior de la EFS?
No existe.

6. ¿Qué aportes puede hacer la EFS, con relación al tema, desde su propia experiencia?
Pese a que no se cuenta con personal o Departamento que vea la parte de Seguridad en particular; se cuenta con plataformas que pueden reducir los riesgos a nivel de Seguridad de la Información.

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

1¿Existen convenios interadministrativos para el intercambio de información entre Entidades de Control en el país?
2. ¿Existe normatividad que reglamente el tema de intercambio de información entre las entidades de Control del país?
3. ¿La EFS de su país realiza intercambio de información almacenada en base de datos con otras EFS? ¿De qué tipo?
4. ¿La EFS de su país realiza intercambio de información almacenada en base de datos con otros organismos internacionales? ¿De qué tipo?
5. ¿Existe intercambio de información sensible de la EFS desde/hacia entidades gubernamentales? ¿De qué tipo?
6. ¿Qué aportes considera que la EFS puede hacer, con relación al tema, desde su propia experiencia?

El intercambio de información actualmente se da a través de acuerdos y solicitudes puntuales entre las entidades. Como visión del gobierno de Panamá, es que la Autoridad de Innovación Gubernamental – AIG, desarrolle una plataforma de Interoperabilidad que actualmente se encuentra en fase de planificación. Esto permitiría la gestión de la información común de las entidades del Estado para cualquier propósito a través de dicho organismo.