CONTRALORIA GENERAL DE LA REPÚBLICA
DE COSTA RICA

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"

Elaborado por:

Jorge Garnier Roviera
Joaquín Gutiérrez Gutiérrez
Jorge León Rodríguez
Javier Brenes Arrieta

Junio, 2015

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?

Las bases de datos de información misional o de negocio, en el caso de nuestra EFS están locales en servidores ubicados en el centro de cómputo.

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?

Se cuenta con personal que hace uso de datos internos y externos para transformarlos en conocimiento que se utilizan en la toma de decisiones. Por ejemplo se cuenta con información de 10 años sobre presupuestos públicos, datos sobre los procedimientos de contratación de entidades fiscalizadas para los últimos 8 años, información sobre gestión de las municipalidades, datos de las declaraciones juradas de bienes presentadas ante la CGR, bases de datos externas para realizar controles cruzados, entre otros.
Para realizar estas funciones se utilizan tanto herramientas compradas como aplicaciones desarrolladas a lo interno. Entre las herramientas especializadas están: IDEA, QlikView, Oracle BI y MS SQL.

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.)

Se presentan problemas con información recibida de otras entidades públicas, entre otras cosas: inconsistencias en los datos y falta de normalización. No existe una estandarización a nivel de entidades públicas con relación a la presentación de los datos, lo cual hace que en la práctica se tenga que recibir la información en el formato que el productor establezca, debiendo el receptor hacer los ajustes que correspondan.

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

Pese a que nuestros dispositivos de seguridad detectan constantes intentos de ataque hacia nuestros equipos, a la fecha no se ha materializado ningún evento que haya comprometido la información almacenada en nuestras bases de datos.

Contraloría General de la República
T: (506) 2501-8000, F: (506) 2501-8100 C: contraloria.general@cgr.go.cr
http://www.cgr.go.cr/ Apdo. 1179-1000, San José, Costa Rica

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

La CGR cuenta con un documento de políticas de seguridad en el uso de las tecnologías de información, mediante el cual se dan lineamientos de acatamiento obligatorio relacionados con las buenas prácticas en el uso de las TICs.

Se establecen en este documento lineamientos relacionados con:

- Uso adecuado de contraseñas
- Control de malware
- Control físico y ambiental del centro de cómputo
- Uso de la telefonía IP
- Conexiones inalámbricas
- Conexiones a terceros
- Uso del Internet
- Uso del correo electrónico y de herramientas colaborativas
- Manejo de información sensible
- Manejo de información institucional oficial.

De igual manera cabe indicar que existen una serie de procedimientos almacenados en la base de datos, para la recuperación de servicios; sin embargo aún no se cuenta con protocolos formales de atención de incidentes y recuperación de los servicios como tales. Este proceso se lleva a cabo en forma reactiva ante la ocurrencia de un evento.

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

La CGR, como un mecanismo para recibir información de entidades fiscalizadas, ha desarrollado sus propios sistemas y web services, tendientes a que los datos nos queden registrados localmente con una mayor usabilidad, de manera tal que facilite las posteriores labores de minería de datos.

A nivel país hace falta que un ente rector en materia de TICs, formule estándares que faciliten el intercambio de información entre las entidades públicas.

En esta era, la información representa un activo vital que permite y agiliza, la toma de decisiones y de paso, permite que las instituciones con mayor capacidad de manejar información, puedan ser expeditas en sus funciones y efectivas en sus actividades diarias.

Contraloría General de la República
T: (506) 2501-8000, F: (506) 2501-8100 C: contraloria.general@cgr.go.cr
http://www.cgr.go.cr/ Apdo. 1179-1000, San José, Costa Rica

En el caso de las EFS, con procesos de información importantes entre sus instituciones fiscalizadas y con diferentes plataformas para el manejo de datos, ofrecen todo un reto tecnológico y procedimental, que obliga a promover un enfoque muy puntual con respecto a la información que se desea procesar. Esto conlleva a que siempre se deba contar con un presupuesto que permita a la EFS, llevar delantera y liderazgo en esta materia, por encima de las instituciones fiscalizadas, contando además con herramientas que faciliten la minería, análisis estadísticos y procesamiento de los datos; y que promuevan un adecuado uso de la tecnología entre el personal de la EFS a través de un presupuesto que facilite la implementación, capacitación y uso de la misma, por medio de una política institucional que tienda a valorar el dato y en consecuencia la información.

INFORMACIÓN PUBLICADA EN INTERNET O COMPARTIDA ENTRE EFS.

1. ¿La EFS publica información misional a través de Internet?

La CGR procura publicar a través de su sitio en internet, información misional que es útil, tanto para usuarios externos como internos, otras entidades públicas y privadas; además en busca de potenciar el conocimiento y el accionar del ciudadano interesado en el manejo de la Hacienda Pública. Como ejemplos de estas publicaciones, en nuestro sitio web se encuentra:

- Información sobre la gestión de las municipalidades.
- Conozca en qué se gasta su dinero (información sobre cómo se gastan los recursos públicos por parte de las instituciones, dirigido al ciudadano)
- Ingresos, gastos y resultados de los presupuestos públicos.
- Compras realizadas con fondos públicos.
- Registro de funcionarios públicos sancionados.
- Normativa para la fiscalización.
- Pronunciamientos de la CGR.
- Informes de fiscalización emitidos.
- Autorizaciones de compra directa, resoluciones de objeciones al cartel y apelaciones, refrendos de contratos.
- Plan de adquisiciones de la CGR.

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

Se ofrecen servicios web para informar al ciudadano sobre cómo hacer trámites ante la CGR, se provee un sistema automatizado para el registro de las declaraciones juradas de bienes, se cuenta con un web service y un sistema en línea para que las entidades reporten datos

Contraloría General de la República
T: (506) 2501-8000, F: (506) 2501-8100 C: contraloria.general@cgr.go.cr
http://www.cgr.go.cr/ Apdo. 1179-1000, San José, Costa Rica

sobre los procedimientos de contratación que realizan, se cuenta con una aplicación en línea para que se puedan presentar denuncias ante la CGR, las consultas pueden ser planteadas directamente ante un sistema en línea, existe un sitio para facilitar la capacitación virtual dirigida a los funcionarios públicos y se tiene un sistema para el trámite de la aprobación presupuestaria en línea.

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

A la fecha se han controlado todos los incidentes de seguridad detectados por nuestros equipos; sin embargo, se ha actuado de forma reactiva ante la presentación del incidente, careciendo de protocolos de acción formalmente definidos para la atención de estos.
Hace falta renovar dispositivos y programas de seguridad que ya no son efectivos contra ataques de última generación, situación que se va enfrentando de acuerdo con la disponibilidad presupuestaria. La falta de estos elementos compromete y limita la detección de nuevos ataques, imposibilitando tomar acciones mitigantes.

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

En la CGR se aplican protocolos de seguridad física para el acceso a las instalaciones donde se maneja información sensible, se cuenta con políticas para la gestión segura de la información y además, se cuenta con un contrato de servicios mediante el cual una empresa especializada en el tema de seguridad, realiza anualmente un estudio de vulnerabilidades sobre nuestra plataforma. En dicho estudio se analizan las diferentes situaciones relacionadas al antes, durante y después, de un incidente de seguridad informática. Las recomendaciones de esos estudios orientan nuestro plan de acción en materia de seguridad en TICs.

Se trabaja, con las limitantes presupuestarias, en mejorar la continuidad y la seguridad de la TI a nivel institucional.

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

El Ministerio de Ciencia, Tecnología y Telecomunicaciones, emitió el 24 de mayo del año 2013, la directriz **Nº 049-MICITT** tendiente a que todas las entidades del sector público implementen el protocolo IPv6. Al respecto la CGR viene desarrollando con éxito un proyecto para lograr que nuestras instalaciones y servicios operen con dicho protocolo.

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

Contraloría General de la República
T: (506) 2501-8000, F: (506) 2501-8100 C: contraloria.general@cgr.go.cr
http://www.cgr.go.cr/ Apdo. 1179-1000, San José, Costa Rica

Las EFS deben buscar mecanismos tecnológicos que posibiliten a los interesados (entes públicos, privados o ciudadanos en general), a acceder a los datos de una forma “cruda”, y que puedan procesar de acuerdo con sus necesidades, los datos que maneja la institución y reflejen el estado de los fiscalizados.

Es importante considerar la seguridad informática como un proceso permanente y mantener los dispositivos y programas de seguridad dentro de un umbral tecnológico, que posibilite a la organización sostener un nivel de seguridad directamente proporcional al valor de los datos que administra. Así mismo, establecer una normativa que regule y capacite a los funcionarios de la institución como actores primordiales del proceso de seguridad en TIC.

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?

La CGR ha venido en un proceso de aplicación de una política de cero papeles desde el año 2012, con lo cual las auditorías vienen siendo aplicadas con el uso del expediente electrónico, donde, tanto los oficios como los papeles de trabajo son firmados digitalmente, tanto por su realizador como por el correspondiente revisor. Los documentos que son recibidos en el proceso auditor, son escaneados e incorporados a cada expediente electrónico, mismo que luego es almacenado en un CD con documentos debidamente hipervinculados, donde queda en definitiva el expediente de cada auditoría.

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

Para la transmisión de los datos se utiliza el protocolo https, con el fin de darle mayor seguridad a este trasiego de información por Internet, además se utilizan redes virtuales privadas (VPN) para la comunicación de los usuarios remotos. En cuanto al cifrado de datos en la BD, es posible, pero no en todos los casos se utiliza.

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

A nivel de aplicaciones el manejo de la seguridad hereda la gestión de seguridad de la base de datos, ampliada con procedimientos y políticas relativas a las claves de usuarios. Contamos con un sistema de gestión de los roles y privilegios que tienen los usuarios para el uso de las aplicaciones internas. Manejamos un esquema de claves robustas, cuyo cambio es obligatorio acorde a las políticas de seguridad vigentes, tenemos ambientes separados de desarrollo, pruebas y producción, utilizamos protocolo https para proteger la información y las

Contraloría General de la República
T: (506) 2501-8000, F: (506) 2501-8100 C: contraloria.general@cgr.go.cr
http://www.cgr.go.cr/ Apdo. 1179-1000, San José, Costa Rica

claves de usuario y contamos con equipos especializados de seguridad para la protección de nuestros sitios web, mediante los cuales nuestros usuarios acceden a las aplicaciones..

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 CGR ha venido dándole prioridad al desarrollo interno en lugar de la adquisición de aplicaciones. En ese contexto contamos con una metodología de desarrollo de proyectos de TIC estandarizada y promulgada a nivel institucional. Contamos con ambientes separados para el desarrollo y prueba de nuestras aplicaciones y con un procedimiento formal de pase a producción, tanto de nuevas aplicaciones como de ajustes a éstas. En la metodología anteriormente indicada y en el procedimiento institucional de Gestión de Soluciones Tecnológicas, se establece que luego de un análisis de requerimientos, en la determinación de la solución, se analizan opciones de adquisición de la aplicación, en tanto el análisis de ésta determine que satisface los requerimientos establecidos por el usuario.

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

En el caso del desarrollo de nuestras aplicaciones se realiza un seguimiento de los puntos de control establecidos en la metodología de desarrollo de proyectos de TIC. En el caso de los procedimientos relacionados con la gestión de la infraestructura tecnológica, se cuenta con puntos de control que son verificados en el caso de procedimientos rutinarios. Adicionalmente contamos con programas y consolas que permiten verificar bitácoras en busca de comportamientos anómalos en los servicios.

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

En nuestro país aplica la Ley No. 8968, Ley de Protección de la Persona frente al tratamiento de sus Datos Personales, publicada el 5 de setiembre de 2011.

Esta ley es de aplicación a los datos personales que figuren en bases de datos automatizadas o manuales, de organismos públicos o privados, y a toda modalidad de uso posterior de estos datos. El régimen de protección de los datos de carácter personal que se establece en esta ley no será de aplicación a las bases de datos mantenidas por personas físicas o jurídicas con fines exclusivamente internos, personales o domésticos, siempre y cuando estas no sean vendidas o de cualquier otra manera comercializadas. En dicha ley se regula la autodeterminación informativa, el principio de consentimiento informado, el principio de calidad de la información, los derechos que asisten a la persona con respecto a sus datos

Contraloría General de la República
T: (506) 2501-8000, F: (506) 2501-8100 C: contraloria.general@cgr.go.cr
http://www.cgr.go.cr/ Apdo. 1179-1000, San José, Costa Rica

personales y las excepciones a la autodeterminación informativa del ciudadano. Aplica criterios con relación a la seguridad y confidencialidad del tratamiento de los datos personales, así como lo relacionado a la transferencia de esos datos.

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?

No existe normativa al respecto.

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

Se puede optar por soluciones en la nube que cumplan con los aspectos de seguridad requeridos y que le permitan a la organización beneficiarse de estos esquemas, ya sea de software o de infraestructura como servicio, disminuyendo costos de manera considerable y agilizando la obtención de soluciones tecnológicas para la organización. Las máximas autoridades deben conocer, para luego apoyar, estas opciones tecnológicas y a nivel país promoverse una legislación que oriente y posibilite el uso de estas opciones, con economías de escala que beneficien la Hacienda Pública.

BUENAS PRÁCTICAS DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

1. ¿Existe una Política de seguridad adoptada institucionalmente por la EFS? ¿Desde qué año?

La CGR cuenta con políticas de seguridad adoptadas institucionalmente desde el año 2007. Con el fin de que estas políticas mantengan su vigencia técnica, el documento es revisado de manera periódica y a la fecha se han emitido 2 actualizaciones, una en el año 2012 y la última emitida formalmente por el Despacho Contralor el pasado 29 de enero de 2015.

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

No se cuenta con una metodología formalmente establecida, pero sí se cuenta con guías operacionales específicas para el diagnóstico y prevención de los incidentes, así como para la recuperación de los servicios.

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

Periódicamente se realizan estudios de vulnerabilidades por parte de una entidad externa, con el propósito de identificar y administrar riesgos asociados a la seguridad informática.

Contraloría General de la República
T: (506) 2501-8000, F: (506) 2501-8100 C: contraloria.general@cgr.go.cr
http://www.cgr.go.cr/ Apdo. 1179-1000, San José, Costa Rica

Pese a esto, requerimos documentar una metodología y formalizarla. Igualmente requerimos de más recursos para atender algunas de las vulnerabilidades detectadas.

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

No contamos con un plan de continuidad del negocio.

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?

No aplica.

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

En un sistema institucional que gestiona la información recibida y producida, el usuario la clasifica como confidencial o pública; esto a partir de lineamientos de cada jefatura o por la aplicación de restricciones legales.

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

No contamos con acuerdos de servicio (SLA) y para el caso de los contratos con externos se establecen cláusulas de privacidad y de confidencialidad de la información.

8. ¿La EFS tiene establecido un Plan de respuesta a incidentes?

Anualmente se planifican actividades y se separan recursos presupuestarios para la atención de incidentes. Contamos con contratos de soporte para la atención de incidentes y un contrato con una empresa que evalúa anualmente nuestra gestión de respuesta a incidentes y nos hace recomendaciones a aplicar. Para la aplicación de dichas recomendaciones se necesitan recursos (humanos, materiales y monetarios), así como documentar y consolidar planes y procedimientos.

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

Contamos con un contrato con una empresa especializada en seguridad informática, que anualmente evalúa nuestra gestión para atender el antes, el durante y el después de un incidente de seguridad informática. Las recomendaciones emitidas son analizadas y priorizadas, para atenderlas según la disponibilidad de recursos y tiempo del personal de la CGR.

Contraloría General de la República
T: (506) 2501-8000, F: (506) 2501-8100 C: contraloria.general@cgr.go.cr
http://www.cgr.go.cr/ Apdo. 1179-1000, San José, Costa Rica

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

Existen una serie de recomendaciones y solicitudes presupuestarias que se realizan año con año, no obstante, las limitaciones financieras que enfrenta el país reducen la capacidad ejecutiva para solventar las necesidades planteadas. Ante estas circunstancias, la alta dirección promueve un compromiso constante, pero limitado por lo anteriormente indicado.

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

La gestión de la seguridad informática no es un problema de índole técnico, sino de tipo presupuestario, donde las tecnologías que soportan y gestionan la seguridad evolucionan constantemente, enfrentando ataques de nueva generación. Sin embargo, estas tecnologías son costosas y el personal debe actualizar sus conocimientos de manera permanente. Se deben tomar acciones que minimicen el riesgo de desactualización del personal técnico en la materia de seguridad informática y otros campos relacionados. Igualmente, la gestión de la seguridad informática involucra directamente a los usuarios de las tecnologías de información y debe promoverse la cultura institucional y las competencias de nuestro personal en estos campos.

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

1. ¿La EFS cuenta con personal especializado en seguridad informática?

La CGR cuenta con personal capacitado en temas relativos a la seguridad informática y cuyas labores principales son atender los elementos que soportan esta área. Se han recibido cursos de “hackeo” ético, administración de riesgos de TIC, Continuidad del Negocio y Continuidad de la TI, ITIL, operación de equipos de seguridad, entre otros.

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

Las labores de monitoreo y/o atención de incidentes es realizada con personal de la Unidad de Tecnologías de Información, sin que exista un grupo de seguridad formalmente establecido. Por falta de personal, estos funcionarios no realizan únicamente estas funciones y esto dificulta la realización de un proceso de análisis tan exhaustivo como deseáramos realizar.

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

Contraloría General de la República
T: (506) 2501-8000, F: (506) 2501-8100 C: contraloria.general@cgr.go.cr
http://www.cgr.go.cr/ Apdo. 1179-1000, San José, Costa Rica

No se encuentra un grupo de seguridad instaurado institucionalmente.

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

Utilizamos routers con funciones de firewall, firewall especializados en protección de sitios web, equipo para apoyo en las labores de seguridad. El monitoreo se realiza de forma independiente por equipo. En cuanto a correlación de eventos no contamos con plataformas de apoyo.

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

La plataforma de seguridad con que contamos se encuentra local.

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

No se cuenta con un equipo CSIRT a nivel de la EFS, se atiende con personal de la Unidad de Tecnologías de Información.

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

No se tienen identificados.

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

No se tiene identificado.

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?

Se cuenta con procedimientos independientes de monitoreo del comportamiento de los eventos que podrían amenazar la seguridad informática y que son atendidos de conformidad a como se presenten.

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

Sí se realiza seguimiento a los incidentes, se registran en un sistema y se le da análisis y atención hasta darlo por cerrado.

Contraloría General de la República
T: (506) 2501-8000, F: (506) 2501-8100 C: contraloria.general@cgr.go.cr
http://www.cgr.go.cr/ Apdo. 1179-1000, San José, Costa Rica

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

Se cuenta con un contrato con una empresa externa que ejecuta, en conjunto con personal de la Unidad de Tecnologías de Información, actividades preventivas tendientes a minimizar los riesgos asociados a la seguridad informática. Dicha Unidad ejecuta también una serie de actividades relacionadas con la atención preventiva a eventos de seguridad relativa a los servicios y recursos con que cuenta la CGR.

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

Los ataques de mayor relevancia son reportados a la Jefatura de la Unidad de Tecnologías de Información y al Gerente de la División de Apoyo. La bitácora de eventos de seguridad está registrada en un sistema de información, posibilitando su consulta y análisis en línea, por parte de los funcionarios encargados, supervisor y jefatura de TI.

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

No se tiene dicha figura formalmente establecida, sin embargo, se cuenta con un funcionario de nivel fiscalizador que desempeña funciones similares, sin que estas sean sus únicas funciones.

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

A nivel nacional el Ministerio de Ciencia, Tecnología y Telecomunicaciones (MICITT), como ente rector en esta materia, tiene a su cargo la definición de una estrategia pública.

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

A nivel nacional el Ministerio de Ciencia, Tecnología y Telecomunicaciones (MICITT), implementó un CSIRT Nacional, promoviendo la integración con enlaces de la diferentes entidades públicas.

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

Las EFS deben promover y coadyuvar a que se establezca a nivel del sector público, una estrategia o política pública tendiente a que las entidades refuercen los mecanismos de mitigación a los riesgos de seguridad informática, fortaleciendo de esta manera el control

Contraloría General de la República
T: (506) 2501-8000, F: (506) 2501-8100 C: contraloria.general@cgr.go.cr
http://www.cgr.go.cr/ Apdo. 1179-1000, San José, Costa Rica

interno en las Instituciones. Por otra parte, la consciencia de que atender los aspectos de seguridad informática es fundamental hoy en día, debe conllevar a que se otorguen más recursos presupuestarios, humanos y de capacitación, para que puedan fortalecerse estas acciones a lo interno de las EFS.

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?

La CGR ha implementado software antivirus en todos los equipos, se cuenta con equipos especializados a nivel perimetral para la detección de malware, nuestro correo electrónico filtra spam y malware, además existen políticas de seguridad dirigidas al personal que orientan sobre el uso adecuado de las TICs.

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

La CGR sí realiza intercambio de información sensible a través de la red de datos, ya sea por el uso interno de los sistemas de información o por el acceso a nuestro sitio web institucional.

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

Se realiza la concientización a los usuarios mediante correos, charlas y políticas de seguridad formalmente promulgadas.
A nivel externo se ha comunicado sobre los cuidados mínimos que se deben tener y sobre el cuidado en cuanto a no revelar sus password y que la CGR no solicita esos datos mediante correos electrónicos.

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?

Mediante campañas periódicas de sensibilización y programas de divulgación apoyadas en las herramientas institucionales. Cada vez que sucede algún tipo de amenaza se le informa al usuario y se le reitera sobre la importancia de tener los cuidados mínimos para no ser víctima de algún robo de datos o de información, aportándole ejemplos y formas de actuar concretos.

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

Contraloría General de la República
T: (506) 2501-8000, F: (506) 2501-8100 C: contraloria.general@cgr.go.cr
http://www.cgr.go.cr/ Apdo. 1179-1000, San José, Costa Rica

Producto de las campañas anteriormente descritas el personal tiene una cultura de seguridad informática. Además en el proceso de inducción a nuevos funcionarios se da una charla sobre aspectos de seguridad informática y buen uso de las tecnologías, que todo funcionario debe aplicar. Finalmente, la Unidad de Tecnologías de Información promueve que las políticas de seguridad y buen uso de las TICs, se mantengan vigentes ante cambios tecnológicos o nuevas herramientas que se utilicen.

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

Nos parece importante recalcar que unido a los lineamientos y políticas que a nivel interno se puedan tener y que son de aplicación obligatoria para todo el personal, se cuente con un esquema sancionatorio por el incumplimiento comprobado y negligente que algún funcionario cometa.
Por otra parte, pese a los esfuerzos que se realicen en promover la cultura en materia de seguridad informática, siempre existirá la dificultad con aquellos usuarios que tienen el pensamiento de que "*a mí nunca me va a pasar*", con lo cual muchas medidas de prevención no son aplicadas.

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?

No se cuenta con ese tipo de convenios.

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

No se cuenta con normativa al respecto.

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

No se realiza intercambio de información almacenada en nuestras bases de datos con otras EFS.

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

Contraloría General de la República
T: (506) 2501-8000, F: (506) 2501-8100 C: contraloria.general@cgr.go.cr
http://www.cgr.go.cr/ Apdo. 1179-1000, San José, Costa Rica

No se tiene intercambio de información con otros organismos internacionales.

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

Entre entidades gubernamentales y con la finalidad de realizar acciones propias del sistema de pagos, se realizan intercambios de información sensible.
Por otra parte, la mayoría de la información de la CGR es pública y se dispone para ser consultada mediante nuestro sitio web.
Con el fin de aprovechar a nivel interno bases de datos que tienen otras entidades gubernamentales, se cuenta con convenios debidamente formalizados. Entre estos podemos citar convenios para obtener información de la Asamblea Legislativa, el Registro Nacional, Tribunal Supremo de Elecciones, Migración y Extranjería, Poder Judicial, Instituto Nacional de Seguros, etc.

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

Es importante contar con convenios con otras EFS o entidades de control del país, que permitan el intercambio de experiencias, buenas prácticas e información útil para la ejecución de los propios procesos institucionales.

Contraloría General de la República
T: (506) 2501-8000, F: (506) 2501-8100 C: contraloria.general@cgr.go.cr
http://www.cgr.go.cr/ Apdo. 1179-1000, San José, Costa Rica