Documento de colaboración técnica – CGR Nicaragua

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.

Junio, 2015

Introducción

Como ha escrito Umberto Eco[1] "*Toda información es importante si está conectada a otra*". Nuestras EFS son organizaciones por las cuales fluye mucha información y nuestros esfuerzos deben estar dirigidos a que ésta genere conocimiento, sea oportuna, ayude en la gestión y cumplimiento misional. Pero, sin obviar todo lo concerniente a la seguridad de la misma y su uso adecuado.

Las tecnologías de la información y las comunicaciones son parte importante para lograr esa meta, sin embargo se requiere de inversión y desarrollo de capacidades técnicas.

Actualmente, la CGR Nicaragua se encuentra iniciando un proceso de incorporación de las TICs de una manera más conveniente, útil y moderna. Orientando el trabajo hacia obtener un área de tecnologías de la información que sea un apoyo significativo en la gestión de la CGR incorporando tecnologías acordes con el quehacer y que faciliten los procesos de recolección, procesamiento, análisis, intercambio y publicación de información de forma ágil y segura.

En el presente, damos respuesta de acuerdo a nuestra situación actual como EFS – Nicaragua, a las interrogantes planteadas en el documento propuesta inicial y documento guía remitido por la Oficina de Capacitación, Producción de Tecnología y Cooperación Técnica Internacional de la Contraloría General de la República de Colombia.

[1] Alessandria, Italia, 5 de enero de 1932. Es un escritor y filósofo italiano. Miembro del Foro de Sabios de la Mesa del Consejo Ejecutivo de la Unesco.

Preguntas formuladas

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 hibrido?**

   Respuesta: Local. Los Sistemas Gestores de Bases de Datos que manejan la información se encuentran en servidores ubicados en las instalaciones centrales de la CGR.

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?**

   Respuesta: Actualmente no se utiliza ninguna herramienta para realizar minería de datos. Cada sistema de información desarrollado incluye los reportes de dirección requeridos para la toma de decisiones y remisión a la máxima autoridad.

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.)**

   Respuesta: Si. La que se menciona, diferentes formatos de presentación en los orígenes de los datos.

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

   Respuesta: No. A la fecha no se ha reportado ningún tipo de falla de seguridad en las bases de datos, ni se han encontrados fallas en la integridad de la información.

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

   Respuesta: En el ámbito de los sistemas de información se han establecido mecanismos de seguridad, tales como: roles y perfiles de usuarios con el objetivo de garantizar que a través de la autentificación e identificación solamente los usuarios permitidos accedan a las aplicaciones. Así también se manejan registros de eventos y pistas de auditoría que permiten indagar sobre cualquier anomalía que se pudiera presentar en el registro y procesamiento de los datos.

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

   Respuesta: La oportunidad de la información y del conocimiento que ésta genera es realmente relevante, por lo que, además de incorporar herramientas de análisis y minería de datos, se debe también mejorar los tiempos de recolección y procesamiento de datos procurándolos más cortos, incorporando por ejemplo, sistemas móviles y/o web que

permitan que de una manera más sencilla y ágil se puedan obtener los resultados esperados. Esto conlleva a un análisis particular de tecnologías, recursos humanos y capacidades internas para su implementación.

INFORMACIÓN PUBLICADA EN INTERNET O COMPARTIDA ENTRE EFS

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

   Respuesta: Sí. A través del sitio web institucional, la Oficina de Acceso a la Información Pública de la CGR da a conocer a la población en general la información pertinente.

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

   Respuesta: Actualmente no. En un corto plazo tenemos previsto la incorporación gradual de algunos servicios.

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

   Respuesta: No en su totalidad. La EFS cuenta con un Software de Gestión Unificada perimetral que ayuda a controlar la mayoría de los aspectos a nivel de seguridad en una red de datos, sin embargo se carece de dispositivos más avanzados para tener un mejor control.

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

   Respuesta: Sí. El Centro de Procesamiento de Datos cuenta con dispositivos de acceso físico (reconocimiento de huella digital), teniendo al personal mínimo requerido con acceso al mismo. En las instalaciones destinadas para los gabinetes de comunicación un 65% se encuentran resguardado con llave para uso exclusivo de personal de infraestructura, no así el restante 35% ya que los gabinetes se encuentran compartiendo espacio con las oficinas de los funcionarios.

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

   Respuesta: No que tengamos conocimiento.

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

   Respuesta: La publicación de información en el sitio web es un aspecto de gran importancia, ya que ésta es una de las formas de comunicación que la EFS tiene con la población y dar así a conocer su trabajo, su legislación, etc. Se debe trabajar sí, por tener sitios web seguros, de fácil acceso, que ofrezcan servicios a la población y esto implica tomar en cuenta aspectos técnicos como:

   - ✓ Sistemas operativos estables con configuraciones endurecidas.
   - ✓ Versiones de manejadores de contenido (o seguridad en el desarrollo interno).
   - ✓ Vulnerabilidad en las versiones de software utilizados (plan de actualización).

- ✓ Cifrado de comunicaciones con el uso de certificados digitales.
- ✓ Habilitar registros y eventos de seguridad para detectar inconvenientes.
- ✓ Implementación de software para detección de ataque, capa 3 y 7.
- ✓ Limitar accesos a lugares según rol.

SEGURIDAD INFORMÁTICA

1. **¿En la EFS la información del proceso auditor se maneja digitalmente a través de expedientes electrónicos con niveles de seguridad como firmas electrónicas?**

   Respuesta: El expediente completo de cada proceso de auditoría se lleva de forma manual. Sin embargo en los sistemas se registra parte de esa información, pero no con niveles de seguridad como firmas electrónicas.

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

   Respuesta: Únicamente las contraseñas de usuarios almacenadas en las bases de datos son encriptadas. Los sistemas expuestos al internet corren bajo el protocolo http sin certificado digital.

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

   Respuesta: La seguridad aplicada en las aplicaciones es a través del establecimiento de controles de autentificación, autorización, registro de eventos y pistas de auditoría.

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?**

   Respuesta: No. Se está en el proceso de estandarización de dichos procedimientos, los cuales definirán entre otras cosas, niveles de seguridad en todo el ciclo de vida del desarrollo de sistemas.

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

   Respuesta: No. Como se menciona en el punto anterior, la EFS está en proceso de definición de los procedimientos y por ende de los mecanismos de control y seguimiento.

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

   Respuesta: Ley 476, Ley de Servicio Civil. Sistema de Información del Servicio Civil (SISEC).

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?**

   Respuesta: No.

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

   Respuesta: No se trata únicamente de recolectar, procesar, analizar y compartir información. Sino también de darle seguridad a la misma, de garantizar que es accedida por quien debe hacerlo y en el momento permitido para ello. Por lo que, todo lo concerniente a políticas y herramientas de seguridad son aspectos de relevancia que se deben considerar:

   - ✓ Contar con herramientas para clasificación de la información que permitan identificar/evitar fuga y robo de información.
   - ✓ Aplicar medidas de control de acceso a todos los niveles.
   - ✓ Incorporar técnicas de encriptación y de firma digital.
   - ✓ Contar con herramientas de correlación de eventos para tener un mejor panorama de todo lo que sucede dentro de la entidad.
   - ✓ Contar con herramientas que permitan evaluar ciertas medidas de seguridad para estar "compliant" con las políticas de la organización.
   - ✓ Mantener una constante vigilancia tecnológica para conocer cómo actúan las nuevas infecciones de seguridad y estar mejor preparados ante ataques.

BUENAS PRÁCTICAS DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

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

   Respuesta: Actualmente no. La CGR está entrando a un proceso de estandarización de los recursos informáticos, con el objetivo de establecer normativas, procedimientos y políticas de seguridad para el uso correcto de los recursos.

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

   Respuesta: No. Conocemos de algunos marcos de trabajo como ITIL donde abarcan temas respecto a la gestión de incidentes de seguridad de la información, siendo la idea en un mediano plazo apegarnos a una determinada metodología.

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

   Respuesta: No. Se está considerando realizar análisis de vulnerabilidades a través del uso de software de escaneo para ese fin, igualmente con ayuda de proveedores externos.

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

   Respuesta: No. La CGR no cuenta con un Plan de Continuidad del Negocio y Recuperación de Desastres. Actualmente, se carece de la Infraestructura Tecnológica (a nivel hardware y software) en las instalaciones de la EFS, ni tampoco se cuenta con un Centro Alterno de Operaciones necesario para asegurar la continuidad del negocio. Solamente se realizan pruebas de recuperación de respaldos de bases de datos.

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?**

   Respuesta: No se han determinado a nivel de tecnología los tiempos de recuperación (RTO) ni la cantidad máxima de información que podría perderse (RPO).

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

   Respuesta: La clasificación solamente se realiza de manera manual pero no a través de una herramienta (por ejemplo, prevención de pérdida de información) que permita ciertos niveles de acceso, copia, impresión, y demás formas de bloqueo según su clasificación.

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

   Respuesta: Los acuerdos de niveles de servicios actuales son únicamente para los servicios de Internet y Correo Electrónico, los que son provistos por proveedores externos.

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

   Respuesta: No. En un corto plazo se dará inicio a una implementación de servicios para los cuales se definirán los planes de respuestas a incidentes.

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

   Respuesta: No. La CGR no dispone de auditorías informáticas.

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

    Respuesta: Sí. La alta dirección de la EFS está consciente de la importancia de la seguridad de la información y se ha comprometida con la implementación de herramientas y servicios necesarios que garanticen la misma.

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

    Respuesta: En términos de gestión es importante conocer lo siguiente:
    - ✓ Establecer la confidencialidad de la información
    - ✓ Asegurar la integridad de la información
    - ✓ Disponer de la información cuando se requiera
    - ✓ Políticas de acceso a la información
    - ✓ Gestión de los incidentes, para tratar de siempre conocer qué pasó, qué podemos hacer, cómo podemos seguir mejorando
    - ✓ Informar al usuario final que es el componente más vulnerable en temas de seguridad

- ✓ Implementar medidas no invasivas a los procesos de los usuarios, pero siempre tratando de proteger la información

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

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

   Respuesta: No. Actualmente dentro de los funcionarios que integran la División de Tecnologías de la Información no se cuenta con un especialista en seguridad informática.

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

   Respuesta: No. Falta de personal dedicado a tal fin.

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

   Respuesta: No.

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

   Respuesta: El dispositivo que se utiliza actualmente es una plataforma de UTM para proteger, registrar y monitorear todos los eventos de seguridad que puedan ocasionarse en la red de datos a lo interno y a lo externo. Sin embargo, se necesita de herramientas especializadas que analicen otros tipos de eventos.

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

   Respuesta: Local. Se posee una solución de UTM para temas de seguridad, pero se ha iniciado la implementación de otras herramientas para conocer el estado de los servicios en general y a detalle de la red institucional. No obstante, las distintas herramientas no forman parte de una solución integral e interrelacionada.

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

   Respuesta: No.

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

   Respuesta: No.

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

   Respuesta: 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?**

   Respuesta: Parcialmente. Actualmente, el trabajo se ha enfocado en identificar a mayor detalle los equipos que forman parte de la red institucional de la entidad, con el objetivo de establecer estrategias de monitoreo y por ende incrementar tiempos de respuesta a incidentes de seguridad tratando de mitigar al máximo, porque el riesgo debe ser detectado y administrado.

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

    Respuesta: Si. Una vez se ha identificado el problema inmediatamente se buscan adoptar las medidas correctivas y preventivas relacionadas al caso con el fin de evitar otra situación similar en un futuro cercano.

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

    Respuesta: Si. Se realiza con apoyo de los proveedores de servicios tratando de buscar mejores prácticas en cuanto a la configuración para prevención de incidentes, y tratando de estar en las últimas versiones de software estables (mejoras en métodos de detección) para un mejor aprovechamiento de las herramientas.

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

    Respuesta: Sí. La alta dirección está siempre informada de los incidentes, de las acciones tomadas y de las repercusiones.

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

    Respuesta: No.

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

    Respuesta: No.

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

    Respuesta: No.

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

Respuesta: La definición de un equipo de respuesta a incidentes de seguridad informática permitirá concientizar a todo el personal a atenuar y prevenir incidentes graves de seguridad, así como dirigir de forma centralizada la respuesta a los incidentes de seguridad que puedan ocurrir para ayudar a proteger la información.

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?**

Respuesta: Se han aplicado varios niveles de protección: perimetral implementando filtrado web con clasificación de sitios, análisis de virus, detección de ataques e intrusos, cortafuegos de aplicaciones web, entre otros; a nivel de usuario final se han instalado antivirus con la variante de un escaneo heurístico ante amenazas, el cual es manejado centralmente para el despliegue de políticas de manera global y dando al usuario los privilegios mínimos requeridos para su trabajo; con el proveedor de servicio de correo se ha solicitado el endurecimiento de las políticas de filtrado de correos, listas negras, entre otros aspectos.

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

Respuesta: Sí. La EFS hace uso de un Sistema Administrativo y Financiero que es común para todas las entidades públicas del país, para lo cual la institución a cargo de dicho sistema realizó un proyecto al contratar enlaces privados para la interconexión de las entidades, sobre los cuales se implementaron redes virtuales privadas cuyas conexiones son administradas por nuestro cortafuegos perimetral.

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

Respuesta: Parcialmente. El mecanismo ha sido que al detectar ingeniería social a través de correos vulnerados de otras instituciones, se informa masivamente para evitar comprometer credenciales de usuario que puedan poner el nombre de la institución en riesgo. Así también se les ha dado conocer sobre la importancia de un uso adecuado del internet y se han aplicado restricciones a sitios categorizados como ocio o que pueden representar riesgo para la EFS.

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?**

Respuesta: Parcialmente. A través del correo institucional se les informa sobre casos detectados así como noticias del acontecer de la seguridad de la información con el objetivo de advertirles de los problemas y riesgos, pero no así a manera de talleres informativos.

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

   Respuesta: No. La falta de implementación de mecanismos de seguridad ha conllevado a un poco de descuido por parte de los funcionarios en el uso de los recursos tecnológicos. Sin embargo, con la implementación de los nuevos servicios se iniciará por concientizar en el uso de las contraseñas, permisos de usuarios, resguardo de información, privacidad, entre otros, logrando gradualmente incrementar la cultura respecto a la seguridad de la información.

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

   Respuesta: Para el intercambio de información de manera segura se deben considerar:
   - ✓ Realizar redes virtuales privadas con medidas estrictas de acceso
   - ✓ Definición de redes para el aislamiento de los servidores involucrados en el intercambio.
   - ✓ Accesos por credenciales de usuario, tokens, certificados.
   - ✓ Documentarse en temas de seguridad e intercambio de información.

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?**

   Respuesta: Con la Contraloría General de Chile y Contraloría General del Ecuador. Comunicaciones con la contraloría de cuentas de Guatemala y México para firma de convenio.

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

   Respuesta: No. Los primeros pasos serán respecto a firma digital para asegurar la identidad de los funcionarios, servicios o entidades del país.

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

   Respuesta: Ninguno. La información contenida en las bases de datos de la EFS es hasta el momento de uso exclusivo de la misma.

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

   Respuesta: Ninguno.

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

   Respuesta: No. Como parte de nuestros procesos está verificar los bienes de los funcionarios públicos que forman parte de su declaración de probidad, pero actualmente se hace de forma manual y no a través de un sistema de información.

6. **¿Qué aportes considera que la EFS puede hacer, con relación al tema, desde su propia experiencia?**
   Respuesta: El intercambio de información entre entidades permite entre otras cosas agilizar procesos, reducir costos y dar respuestas oportunas a diversos servicios. Sin embargo las organizaciones involucradas en el intercambio, si es que no existiera una política de gobierno, deben ponerse de acuerdo y aunar esfuerzos para garantizar la seguridad de esa información y establecer normativas claras y prácticas para el intercambio de la misma.