CAJA COSTARRICENSE DE SEGURO SOCIAL
AUDITORIA NTERNA
Tel.: 2539-0821 - Fax.: 2539-0888
Apdo.: 10105

ATIC-45-2016
4-04-2016

RESUMEN EJECUTIVO

El presente estudio se realizó según el Plan Anual Operativo 2016 del Área de Tecnologías de Información y Comunicaciones de la Auditoría Interna, con el fin de evaluar el fortalecimiento de la gestión de la seguridad de la información, y así contribuir con el aseguramiento de la confidencialidad, integridad y disponibilidad de la información.

En este sentido, es necesario que la Institución valore la inversión de nuevas herramientas que ayuden a fortalecer la seguridad de la plataforma tecnológica, ya que según las métricas expuestas por la empresa Gartner, recomienda a las empresas invertir aproximadamente un 6% del presupuesto total destinado a tecnologías de información y comunicaciones.

Otro aspecto fundamental, es la necesidad de disponer del personal humano suficiente y competente que permita gestionar razonablemente los recursos destinados a la seguridad en TIC, por tanto, es importante indicar que un profesional especializado en seguridad informática, debe ser capaz de aplicar las metodologías, tecnologías y herramientas que existen en las distintas áreas involucradas, como lo es criptografía, modelos formales de seguridad informática, análisis forense, etc. , así como en las áreas en las que la seguridad informática tiene su aplicación: redes, sistemas operativos, aplicaciones. De igual forma deben también ser capaces de gestionar incidentes, riesgos y garantizar la continuidad del negocio, protegiendo los activos críticos de la Institución.

Adicionalmente, es importante que la Institución disponga de políticas de seguridad de la información acordes con las Normas Técnica para la Gestión de las Tecnologías de Información de la Contraloría General de la Repúblicas, así como otros estándares internacionales como el ISO27001, con el fin de articular la organización en cuanto a la seguridad de la información y brindando instrucciones claras a todos los funcionarios de las conductas esperadas y apropiadas, sirviendo como soporte para el logro de los objetivos de la Institución.

En este mismo orden de ideas, resulta relevante que la CCSS implemente indicadores que permitan alertar oportunamente cuando el límite de accesos a las aplicaciones es sobrepasado, detectar comportamientos irregulares en el uso de los sistemas de información, afectaciones al rendimiento de las herramientas tecnológicas, entre otros.

CAJA COSTARRICENSE DE SEGURO SOCIAL
AUDITORIA NTERNA
Tel.: 2539-0821 - Fax.: 2539-0888
Apdo.: 10105

ATIC-45-2016
4-04-2016

ÁREA TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES

ESTUDIO ESPECIAL REFERENTE AL FORTALECIMIENTO DE LA INFRAESTRUCTURA DE SEGURIDAD EN TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES

GERENCIA DE INFRAESTRUCTURA Y TECNOLOGÍAS

ORIGEN DEL ESTUDIO

La evaluación se efectúo de conformidad con el programa de estudios especiales contemplado en el Plan Anual Operativo 2016 del Área de Tecnologías de Información y Comunicaciones.

OBJETIVO GENERAL

Evaluar las acciones ejecutadas por la Administración para fortalecer la infraestructura de seguridad de las tecnologías de información y comunicaciones en la Caja Costarricense de Seguro Social.

OBJETIVOS ESPECÍFICOS

- Determinar las gestiones realizadas por el Área de Seguridad y Calidad Informática (ASCI) para garantizar la seguridad de las tecnologías de información y comunicaciones.
- Verificar la existencia de un marco que regule la confidencialidad, integridad y disponibilidad de la información en la Caja Costarricense de Seguro Social.

ALCANCE

Esta auditoría consideró la revisión de las acciones planificadas y ejecutadas por la Administración para garantizar la confidencialidad, integridad y disponibilidad de la información en la CCSS. El período de la evaluación se considera entre abril y mayo 2015.

El presente estudio se realizó cumpliendo los lineamientos establecidos en el Manual de Normas para el Ejercicio de la Auditoría Interna en el Sector Público.

METODOLOGÍA

Para lograr el cumplimiento de los objetivos se ejecutaron los siguientes procedimientos metodológicos:

- Solicitud de información a los encargados de las siguientes unidades:
  - Dirección de Tecnologías de Información y Comunicaciones

San José, Costa Rica. Ave. 2da, calles 5 y 7. Teléfono 2539-0821, Fax 2539-0888

CAJA COSTARRICENSE DE SEGURO SOCIAL
AUDITORIA NTERNA
Tel.: 2539-0821 - Fax.: 2539-0888
Apdo.: 10105

- Dirección SICERE
- Área de Seguridad y Calidad Informática

- Entrevista y reuniones con los siguientes funcionarios:
  - Lic. Ronald Lacayo Monge, Director del Sistema Centralizado de Recaudación.
  - Lic. Sergio Paz Morales, Subdirector de Tecnologías de Información y Comunicaciones a.i.
  - Licda. Mayra Ulate Rodríguez, Jefe Área de Seguridad y Calidad Informática.
  - Lic. Danilo Hernández Monge, Jefe Área Ingeniería en Sistemas.
  - Licda. Ana María Castro Molina, Jefe Subárea de Seguridad de Tecnologías de Información.
  - Lic. Alexander Angelini Mora, Jefe Subárea Sistemas Financieros Administrativos

MARCO NORMATIVO

- Ley General de Control Interno, 8292, setiembre 2002.
- Normas de Control Interno para el Sector Público. CGR, febrero 2009.
- Normas Técnicas para la Gestión y Control de Tecnologías de Información. CGR, junio 2007.

ASPECTOS NORMATIVOS A CONSIDERAR

Esta Auditoria, informa y previene al Jerarca y a los titulares subordinados, acerca de los deberes que les corresponden, respecto a lo establecido en el artículo 6 de la Ley General de Control Interno, así como sobre las formalidades y los plazos que deben observarse en razón de lo preceptuado en los numerales 36, 37 y 38 de la Ley 8292 en lo referente al trámite de nuestras evaluaciones; al igual que sobre las posibles responsabilidades que pueden generarse por incurrir en las causales previstas en el artículo 39 del mismo cuerpo normativo, el cual indica en su párrafo primero:

> *"Artículo 39.- Causales de responsabilidad administrativa. El jerarca y los titulares subordinados incurrirán en responsabilidad administrativa y civil, cuando corresponda, si incumplen injustificadamente los deberes asignados en esta Ley, sin perjuicio de otras causales previstas en el régimen aplicable a la respectiva relación de servicios. (…)"*

ANTECEDENTES

Esta Auditoría tuvo conocimiento del ataque informático[1] que sufrió el Sistema Centralizado de Recaudación (SICERE) por parte de personas ajenas a la Institución, cuyo propósito consistía en sustraer información de los trabajadores, como por ejemplo, historial de salarios, aportes patronales, entre otros.

[1] Un ataque informático es un método por el cual un individuo, mediante un sistema informático, intenta tomar el control, desestabilizar o dañar otro sistema informático(ordenador, red privada, etc.).

San José, Costa Rica. Ave. 2da, calles 5 y 7. Teléfono 2539-0821, Fax 2539-0888

CAJA COSTARRICENSE DE SEGURO SOCIAL
AUDITORIA NTERNA
Tel.: 2539-0821 - Fax.: 2539-0888
Apdo.: 10105

Sobre ese particular, a continuación se realiza un resumen de lo evidenciado por parte de la Administración Activa, que permitió detectar los casos que provocaron los accesos no autorizados a los sistemas de información institucionales:

Situación ocurrida el 13 de marzo del 2015:

a) A partir de las 7:20 a.m., los usuarios y encargados de los sistemas de información que contemplan el EDUS y SFA (aplicaciones web financieras como SICO, RCPI, Autogestión, Afiliación Oficina Virtual, entre otros), reportan diversos problemas relacionados con la disponibilidad para acceder a los sitios web de estas aplicaciones.

b) En virtud de lo anterior, los funcionarios de la Dirección de Tecnologías de Información y Comunicaciones (DTIC), proceden a realizar todas las revisiones pertinentes con el propósito de encontrar la causa que estaba provocando dicha problemática.

c) Con base en la revisión efectuada, la Administración evidenció que se habían registrado en las bitácoras de la aplicación Oficina Virtual del SICERE, solicitudes masivas de acceso a servicios de las aplicaciones web desde una dirección IP[2] ajena a la Institución, posteriormente lograron identificar que esta dirección pertenecía a una entidad financiera privada.

d) En un lapso de tiempo de 6:42 a.m. a 8:33 a.m., se contabilizaron un total de 37,974 peticiones de acceso a los servicios de la Oficina Virtual del SICERE.

e) Es importante indicar que, esta situación estaba provocando una sobrecarga de tareas en la plataforma tecnológica donde residen las aplicaciones, por lo tanto, daba como resultado que se presentara una lentitud o no disponibilidad de las aplicaciones del SFA y EDUS.

f) Según la Administración Activa, estas solicitudes masivas se dieron de la siguiente forma:

- Valiéndose de un usuario con el perfil de AFILIACION_TRAB (OV)3, lograron acceder a la aplicación de Oficina Virtual del SICERE.
- Posteriormente, utilizaron un software malicioso con el fin de obtener información de otros trabajadores.
- En total, lograron sustraer la información de 522,465 historiales laborales.

g) Como parte de las acciones ejecutadas por la Dirección de Tecnologías de Información y Comunicaciones, sobresalen las siguientes:

[2] La dirección IP (IP es un acrónimo para Internet Protocol) es una etiqueta numérica que identifica, de manera lógica y jerárquica, a una interfaz (elemento de comunicación/conexión) de un dispositivo (generalmente una computadora) dentro de una red que utilice el protocolo IP.
[3] El perfil AFILIACION_TRAB (OV) corresponde al perfil que se le asigna a los ciudadanos para que puedan consultar única y exclusivamente su información personal, por ejemplo: historial de salarios, cuotas, entre otros.

- Realizar el bloqueo en la infraestructura Tecnológica de la CCSS, con el propósito de evitar las solicitudes de acceso provenientes de la dirección IP externa.
- Efectuar las mejoras respectivas en la aplicación que permitieran fortalecer las vulnerabilidades detectadas por los funcionarios de la DTIC, cuya finalidad consistía en contrarrestar las acciones realizadas por el software malicioso.

Situación ocurrida el 26 de mayo del 2015:

a) Al igual que el caso ocurrido anteriormente, la alerta se da por la lentitud y no disponibilidad de las aplicaciones del EDUS y SFA.

b) Mediante la revisión efectuada por los funcionarios de la DTIC, nuevamente se registraron en las bitácoras de auditoría de la aplicación de Oficina Virtual del SICERE, solicitudes masivas de acceso a los servicios de las aplicaciones web a través de una dirección IP externa a la Institución; de igual forma se logró comprobar que pertenecía a la misma entidad financiera privada.

c) Se contabilizaron un total de 151,900 peticiones de acceso a los servicios de Oficina Virtual, utilizando mecanismos de acceso y autentificación diferentes a los establecidos.

d) Sobre este particular, la forma en que se dieron las solicitudes masivas fue muy diferente a las efectuadas en el caso anterior, tal y como se indica a continuación:

- Utilizando un usuario con un perfil de AFILIACION_OPC (OV)4, para el cual también es necesario el uso de un certificado de firma digital, consiguieron acceder a la aplicación de Oficina Virtual del SICERE.
- De igual forma, utilizaron un robot para consulta de información con el propósito de obtener datos del detalle de aportaciones patronales de otros trabajadores, independientemente de la operadora de pensiones a la que se encontraran afiliados.

e) Como parte de las acciones ejecutadas por la Dirección de Tecnologías de Información y Comunicaciones, resaltan las siguientes:

- Realizar el bloqueo en la infraestructura Tecnológica de la CCSS, con el propósito de evitar las solicitudes de acceso provenientes de la dirección IP externa.
- Efectuar las mejoras respectivas en la aplicación de la Oficina Virtual del SICERE que permitieran fortalecer las vulnerabilidades detectadas por los funcionarios de la DTIC, cuya finalidad consistía en contrarrestar las acciones ejecutadas por el software malicioso.

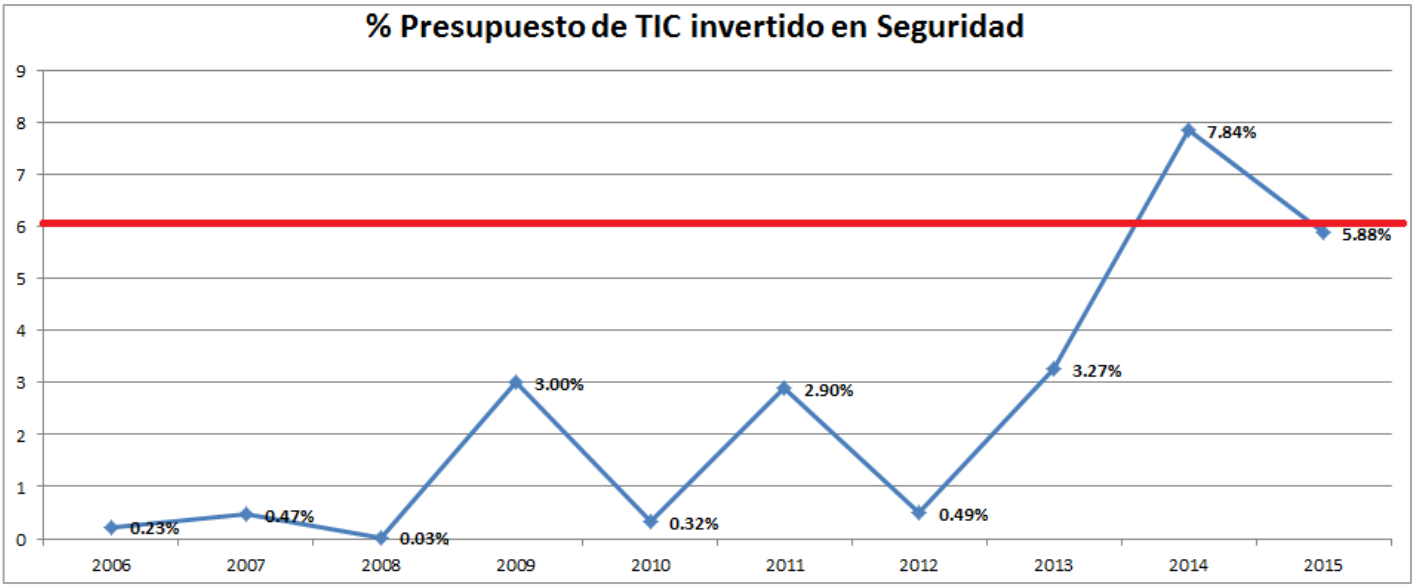
[4] El perfil AFILIACION_OPC (OV) corresponde al perfil que se le asigna a los funcionarios de las Operadoras de Pensiones para que puedan consultar única y exclusivamente la información de las personas que se encuentran afiliadas a la Operadora de Pensiones a la cual representan.

Sobre estos casos, es relevante indicar que la Administración Activa ha interpuesto una denuncia penal ante el Ministerio Público, así como una denuncia administrativa ante la Agencia de Protección de Datos, además la Dirección SICERE y DTIC han recomendado informar a la Superintendencia de Pensiones para que realicen una investigación de los hechos.

HALLAZGOS

1. REFERENTE A LA ASIGNACIÓN PRESUPUESTARIA PARA LLEVAR A CABO PROYECTOS DE SEGURIDAD INFORMÁTICA.

Según las métricas expuestas por la Gartner[5], recomienda a las empresas invertir aproximadamente un 6% del presupuesto total destinado a tecnologías de información y comunicaciones; no obstante, la situación de la Institución en materia de inversión de seguridad informática se representa en el siguiente gráfico:



Fuente: Análisis de datos presupuestarios, DTIC-ASCI-SSTI Setiembre 2015

Tal y como se observa en el gráfico anterior, en el periodo comprendido entre el año 2006 y 2015, el presupuesto asignado al tema de seguridad ha sido inferior con respecto a la métrica establecida por Gartner, a excepción del año 2014 donde hubo un incremento de aproximadamente 1.84%.

Las Normas de Control Interno para el Sector Público, de la Contraloría General de la República en el capítulo 5, Normas Sobre Sistemas de Información, en el apartado 5.9, indica:

[5] Gartner Inc. es una empresa consultora y de investigación de las tecnologías de la información

"El jerarca y los titulares subordinados, según sus competencias, deben propiciar el aprovechamiento de tecnologías de información que apoyen la gestión institucional mediante el manejo apropiado de la información y la implementación de soluciones ágiles y de amplio alcance (…)"

Igualmente, las Normas Técnicas para la Gestión y el Control de las Tecnologías de Información de la Contraloría General de la República, en el capítulo I, sobre Normas de Aplicación General, en el punto 1.4 sobre la gestión de la seguridad de la información, indica que:

"La organización debe garantizar, de manera razonable, la confidencialidad, integridad y disponibilidad de la información (…) Para ello debe documentar e implementar una política de seguridad de la información y los procedimientos correspondientes, asignar los recursos necesarios para lograr los niveles de seguridad requeridos y considerar lo que establece la presente normativa (…)"

Con respecto a la asignación presupuestaria realizada a la seguridad informática, la Licda. Mayra Ulate Rodríguez, Jefe del Área de Seguridad y Calidad Informática, indicó:

"Este es un tema que se planteó en el Plan de Acción para el fortalecimiento de la Infraestructura de Seguridad en TIC de la CCSS, en el cual se le pretende informar a la Junta Directiva de la CCSS lo que hemos invertido en materia de seguridad y lo que falta por invertir. Adicionalmente, es importante manifestarles que el presupuesto asignado a la seguridad informática está por debajo de acuerdo de lo recomendado por la industria indicado por diferentes empresas consultoras, como por ejemplo Gartner, indica que del presupuesto total asignado a las TIC, la organización debe asignar aproximadamente un 6.1% a la seguridad informática y de la información situación que no se ha cumplido en la CCSS.

Debido a la falta de recursos económicos y de acuerdo a la priorización que hemos realizado, se estableció que lográndose implementar para el año 2020 todo lo planificado en el Plan de Acción, estaría la institución a nivel de la industria en el tema de seguridad informática y de la información. Sin embargo, para lograr lo anterior dependemos de una adecuada asignación presupuestaria, así como dotación de recurso humano, que permita el cumplimiento del plan."

Si bien, la institución realiza los esfuerzos para lograr un uso adecuado de los recursos después de una crisis económica la cual provocó reportes sustanciales al contenido presupuestario de tecnologías de información y comunicaciones, preocupa a esta Auditoría que se estén dejando temas de seguridad y control sin presupuesto que puedan exponerla a riesgos relacionados a la disponibilidad de los sistemas, integridad de la información, confidencialidad de los datos y el cumplimiento de leyes y regulaciones, comprometiendo así la eficacia y eficiencia de los servicios.

2. REFERENTE A LOS PROFESIONALES ESPECIALISTAS EN SEGURIDAD INFORMÁTICA

Se evidenció la insuficiencia de profesionales especializados en diferentes áreas relacionadas con la seguridad informática, lo anterior contemplando que el Área de Seguridad y Calidad Informática dispone únicamente con 10 funcionarios, de los cuales solo 3 integran la Subárea de Seguridad de Tecnologías de Información, tal y como se muestra a continuación:

Cuadro 1. Cantidad de recursos del ASCI

Dependencia	Puesto	Funcionario	Grado Académico
Área de Seguridad y Calidad Informática	Jefatura de Área	Mayra Ulate Rodríguez	Maestría en Seguridad Informática
	Profesional 4	Rebeca Chaves Moya	Licenciatura Administración con énfasis en Contabilidad y Finanzas
	Secretaria	María Elizondo Zamora	Administración de Empresas (en proceso)
Subárea de Aseguramiento de la Calidad en TI	Jefatura de Subárea	Mario Vílchez Moreira	Maestría en Administración de Tecnologías de Información y Comunicaciones
	Analista Programador 4	Luis Camacho Barrantes	Licenciatura con énfasis en Gerencia de Proyectos
Subárea de Continuidad de la Gestión	Jefatura de Subárea	Leonardo Fernández Mora	Licenciatura en Ingeniería en Sistemas
	Analista Programador 4	Erick David Vindas Umaña	Licenciado en Ingeniería de Sistemas con énfasis en Redes y Telemática.
Subárea de Seguridad en Tecnologías de Información	Jefatura de Subárea	Ana María Castro Molina	Maestría en Seguridad Informática
	Analista Programador 4	Ericka Sánchez Solís	Maestría en Administración de Proyectos
	Analista Programador 4	Maikol González Alfaro	Licenciatura en Informática con énfasis en Gerencia de Proyectos
Total	**10**		

Fuente: Distribución de Recursos Humanos en el Área de Seguridad y Calidad Informática, ASCI noviembre 2015

Tal y como se mencionó anteriormente, la Subárea de Seguridad en Tecnologías de Información dispone únicamente de 3 funcionarios, los cuales tienen la responsabilidad de fomentar y velar por la seguridad en TIC en la Institución.

Adicionalmente, es importante manifestar que la Institución carece de profesionales especializados en áreas como análisis forense, delito informático, seguridad informática en redes de telecomunicaciones, entre otros; situación que impide aplicar conceptos, metodologías, herramientas, normativas y estándares existentes en estas materias, con el fin de brindar seguridad y protección a los activos de información de la CCSS.

Las Normas Técnicas para la Gestión y el Control de las Tecnologías de Información en su artículo 2.4 sobre la Independencia y recurso humano de la Función de TI establece que:

> *"(…) cuente con una fuerza de trabajo motivada, suficiente, competente y a la que se le haya definido, de manera clara y formal, su responsabilidad, autoridad y funciones."*

Así mismo, señalan en el inciso 3.1 "Consideraciones generales de la implementación de TI", lo siguiente:

> *"La organización debe implementar y mantener las TI requeridas en concordancia con su marco estratégico, planificación, modelo de arquitectura de información e infraestructura tecnológica. Para esa implementación y mantenimiento debe: (…)*
>
> *g. Tomar las previsiones correspondientes para garantizar la disponibilidad de los recursos económicos, técnicos y humanos requeridos. (…)"*

Sobre la insuficiencia de personal especializado, la Licda. Mayra Ulate Rodríguez, Jefe del Área de Seguridad y Calidad Informática, mencionó:

> *"Actualmente existe total disposición por parte del Área de Seguridad y Calidad Informática (ASCI) para aquellos funcionarios que deseen estudiar una maestría, de igual forma se deben realizar las coordinaciones correspondientes con el CENDEISSS para que le otorguen una beca al funcionario interesado. Sin embargo, esta gestión no depende únicamente del ASCI, ya que también debe existir interés, compromiso y disposición por parte del funcionario, máxime si se trata de una beca otorgada por la Institución.*
>
> *Nosotros como área podemos incentivar a los funcionarios para que estudien, inclusive a nivel del CENDEISSS se dispone de presupuesto institucional destinado para becas; sin embargo, no podemos obligar a los funcionarios a que se especialicen.*
>
> *Por otro lado, considero personalmente que sería más conveniente que los funcionarios pudieran obtener especializaciones a través de certificación en lugar de una maestría; por ejemplo: una certificación en ISO:27001, CISM Certified Information Security Manager, Certified Information Systems Auditor (CISA) Certified in the Governance of Enterprise IT (CGEIT) Certified in Risk and Information Systems Control (CRISC), Systems Security Certified Practitioner Certified Authorization Professional Certified Secure Software Lifecycle Professional Certified Cyber Forensics Professional HealthCare Information Security and Privacy Practitioner, ISO 22301, COBIT 5, entre otros. Lo anterior debido a que una certificación los convierte en especialistas de un tema determinado, lo cual resultaría más beneficioso al ASCI.*

El principal inconveniente con el tema de las certificaciones consiste en que su costo es muy elevado, cuestan más de $1000 (mil dólares americanos) y por ende deben gestionarse a través de una beca con el CENDEISSS; lo anterior conlleva una serie de trámites que complica matricular a tiempo a los funcionarios interesados (desde el momento en que se nos comunica la apertura de alguna certificación, iniciamos los trámites ante el CENDEISSS, sin embargo, dichos trámites no finalizan para el periodo de matrícula, lo cual nos obliga a descartar el curso).

Adicionalmente, es importante indicar lo cambiante que son las TIC y el hecho de que todos los años surgen nuevas certificaciones, lo cual implica que los funcionarios se mantengan certificados con el pasar el tiempo. Por lo tanto, esta situación se convierte en otra restricción que tenemos con el CENDEISSS, ya que dicho centro no puede dotar becas todos los años a los funcionarios para que se mantengan certificados."

Adicionalmente, como alternativa de solución a la problemática de la insuficiencia de personal, indicó:

"Actualmente estamos planificando una compra de "servicios profesionales 24x7", dicha compra nos permitirá garantizar que el proveedor dispone del personal suficiente y competente para atender diversos temas relacionados con la seguridad informática; asimismo, el proveedor deberá disponer de herramientas que fortalezcan nuestra plataforma tecnológica actual.

Uno de los objetivos consiste en que a través de las nuestras herramientas, así como las que el proveedor disponga, nos ayuden a monitorear la plataforma del CCSS, con el fin de evitar accesos no autorizados, virus informáticos, realizar análisis en línea, entre otros."

Con el incremento en el uso de las tecnologías de la información y las comunicaciones en la Caja Costarricense de Seguro Social, hace que la información y los recursos informáticos que la gestionan tengan un rol principal en la prestación de los servicios que ofrece la Institución. Asociado a este crecimiento es también cada vez mayor la cantidad de amenazas y ataques que se producen a las aplicaciones y recursos informáticos, es en este contexto que la información se convierte en un recurso crítico al que hay que proteger; por lo tanto, la seguridad informática se vuelve imprescindible como forma de garantizar la integridad, disponibilidad y confidencialidad de la información.

Ante este panorama, la CCSS debe estar preparada para proteger sus activos de información, esto implica conocer y aplicar de forma adecuada los conceptos, metodologías, herramientas, normativas y estándares existentes en esta materia, para lograr el objetivo de seguridad. Asimismo, para ello se requiere de recursos humanos profesionales debidamente capacitados y actualizados, que puedan aplicar de forma exitosa las metodologías y adaptarse rápidamente a los cambios tecnológicos y las exigencias de un área que está en constante evolución y cambio.

Un profesional especializado en seguridad informática, debe ser capaz de aplicar las metodologías, tecnologías y herramientas que existen en las distintas áreas involucradas, como lo es criptografía, modelos formales de seguridad informática, análisis forense, etc. , así como en las áreas en las que la seguridad informática tiene su aplicación: redes, sistemas operativos, aplicaciones. De igual forma deben también ser capaces de gestionar incidentes, riesgos y garantizar la continuidad del negocio, protegiendo los activos críticos.

Por tanto, la insuficiencia de personal podría ocasionar retrasos en la ejecución de proyectos, deterioro de servicios e impactar en la eficiencia y eficacia de las operaciones, así como la materialización de otros riesgos inherentes a las TIC, situación que podría comprometer la continuidad en la prestación de los servicios que brinda la CCSS, debido a que el crecimiento de la infraestructura y la capacidad de la Institución no se ajusta a la cantidad de recursos disponibles que respalden ese crecimiento.

3. REFERENTE A LA DISPOSICIÓN DE POLÍTICAS PARA LA PROTECCIÓN DE DATOS Y ADMINISTRACIÓN DE AMENAZAS Y VULNERABILIDADES

Esta Auditoría evidenció que la Institución no dispone de políticas que sirvan de guías para la apropiada protección de datos y la necesidad de un esquema de clasificación de la información, así como para la reducción de riesgos de explotación de vulnerabilidades técnicas. Lo anterior con el fin de disminuir en la medida de lo posible las amenazas contra los sistemas de información de la Institución.

Las Normas Técnicas para la Gestión y el Control de las Tecnologías de Información de la Contraloría General de la República, en el capítulo I, sobre Normas de Aplicación General, en el apartado 1.4 de la Gestión de la Seguridad de la Información, detalla:

> *"La organización debe garantizar, de manera razonable, la confidencialidad, integridad y disponibilidad de la información, lo que implica protegerla contra uso, divulgación o modificación no autorizados, daño o pérdida u otros factores disfuncionales.*
>
> *Para ello debe documentar e implementar una política de seguridad de la información y los procedimientos correspondientes, asignar los recursos necesarios para lograr los niveles de seguridad requeridos y considerar lo que establece la presente normativa en relación con los siguientes aspectos:*
>
> *- La implementación de un marco de seguridad de la información.*
> *- El compromiso del personal con la seguridad de la información.*
> *- La seguridad física y ambiental.*
> *- La seguridad en las operaciones y comunicaciones.*
> *- El control de acceso.*
> *- La seguridad en la implementación y mantenimiento de software e infraestructura tecnológica.*
> *- La continuidad de los servicios de TI.*

Además debe establecer las medidas de seguridad relacionadas con:

- El acceso a la información por parte de terceros y la contratación de servicios prestados por éstos.
- El manejo de la documentación.
- La terminación normal de contratos, su rescisión o resolución.
- La salud y seguridad del personal.

Las medidas o mecanismos de protección que se establezcan deben mantener una proporción razonable entre su costo y los riesgos asociados."

Adicionalmente, las mismas normas en el apartado 1.4.1 "Implementación de un marco de seguridad de la información", establece:

"La organización debe implementar un marco de seguridad de la información, para lo cual debe:

a. *Establecer un marco metodológico que incluya la clasificación de los recursos de TI, según su criticidad, la identificación y evaluación de riesgos, la elaboración e implementación de un plan para el establecimiento de medidas de seguridad, la evaluación periódica del impacto de esas medidas y la ejecución de procesos de concienciación y capacitación del personal.*
b. *Mantener una vigilancia constante sobre todo el marco de seguridad y definir y ejecutar periódicamente acciones para su actualización.*
c. *Documentar y mantener actualizadas las responsabilidades tanto del personal de la organización como de terceros relacionados."*

De igual forma, las normas ISO 27002:2013 contemplan un código de buenas prácticas para la gestión de seguridad de la información, por lo tanto, para este tema en particular es importante analizar los siguientes controles que fortalecen el aseguramiento de la confidencialidad, integridad y disponibilidad de la información, a saber:

*"…• **Seguridad en los accesos de terceras partes:***

<u>Objetivo:</u> Mantener la seguridad de que los recursos de tratamiento de la información y de los activos de información de la organización sean accesibles por terceros.

La seguridad de la información de la organización y las instalaciones de procesamiento de la información no deben ser reducidas por la introducción de un servicio o producto externo.

Debería controlarse el acceso de terceros a los dispositivos de tratamiento de información de la organización. Cuando el negocio requiera dicho acceso de terceros, se debería realizar una evaluación del riesgo para determinar sus implicaciones sobre la seguridad y las medidas de control que requieren.

Estas medidas de control deberían definirse y aceptarse en un contrato con la tercera parte.

(…)

- ***Clasificación de la Información:***

Objetivo: Asegurar un nivel de protección adecuado a los activos de información. La información debería clasificarse para indicar la necesidad, prioridades y grado de protección.

La información tiene grados variables de sensibilidad y criticidad. Algunos elementos de información pueden requerir un nivel adicional de protección o un uso especial. Debería utilizarse un sistema de clasificación de la información para definir un conjunto de niveles de protección adecuados, y comunicar la necesidad de medidas de utilización especial.

(…)

- ***Administración de Amenazas y Vulnerabilidades:***

Objetivo: Reducir los riesgos resultantes de la explotación de vulnerabilidades técnicas publicadas. La gestión de la vulnerabilidad técnica debe ser implementada de una manera efectiva, sistemática y respetable con medidas tomadas para confirmar su efectividad. Estas consideraciones deben incluir los sistemas operativos y otras aplicaciones en uso.

(…)

- ***Controles criptográficos:***

Objetivo: Proteger la confidencialidad, autenticidad o integridad de la información.

Se deberían usar sistemas y técnicas criptográficas para proteger la información sometida a riesgo, cuando otras medidas y controles no proporcionen la protección adecuada…"

Sobre la existencia de políticas para la protección de datos, administración de amenazas y vulnerabilidades, clasificación de datos, entre otros; la Licda. Mayra Ulate Rodríguez, Jefe del Área de Seguridad y Calidad Informática, mencionó lo siguiente:

"Con respecto a la política de clasificación de la información, es importante indicar que a raíz de una recomendación del informe ATIC-138-R-2009, se elaboró el Procedimiento para la Clasificación de la Información, el cual se pretende que sea de uso Institucional. Dicho procedimiento se hizo de conocimiento a todas las gerencias con el fin de que aportaran observaciones o sugerencias al documento, posteriormente atendidas todas las observaciones realizadas, se le entrego a la Gerencia de Infraestructura y Tecnologías para lo presentaran en el Consejo de Gerentes y así obtener su aprobación y oficialización; sin embargo, estamos a la espera de dicha aprobación.

Con respecto al procedimiento para la atención de incidentes, el Lic. José Manuel Zamora, Director a.i. de Tecnologías de Información y Comunicaciones, a raíz de los eventos presentados con el hackeo de SICERE, elaboró un documento para la atención de incidentes; sin embargo, también se encuentra a la espera de la aprobación y oficialización del Consejo de Gerentes.

En cuando a los documentos de la protección de datos y administración de amenazas y vulnerabilidades, se dispone de procedimientos que manejamos a lo interno del ASCI, ya que algunos documentos son muy técnicos y propios de la gestión que se realiza en esta área."

A fin de fortalecer la gestión integral de la seguridad de la información, y así contribuir con el aseguramiento de la confidencialidad, integridad y disponibilidad de la información asociada a los servicios que ofrece la Caja Costarricense de Seguro Social, es necesario disponer con una adecuada documentación de las políticas y normas de seguridad de la información. Por tanto, el no disponer de políticas relacionadas con temas como por ejemplo: clasificación de la información, encriptación de datos, vulnerabilidades de los sistemas de información, entre otros; podría generar incertidumbre al personal de la Institución sobre la forma de actuar ante un evento de estos.

4. REFERENTE AL ESTUDIO DE VULNERABILIDADES Y RIESGOS A LA SEGURIDAD EN TIC.

Se evidenció que actualmente la Institución no dispone de un estudio de vulnerabilidades debidamente oficializado, el cual permita detectar riesgos, oportunidades de mejora, entre otros aspectos relacionados con seguridad informática.

Sobre este particular, el último estudio de vulnerabilidades realizado en el Institución fue elaborado en el año 2007 por la empresa Pricewaterhouse Coopers, en el cual se evidenciaron una serie de debilidades a las que estaban expuestos algunos sistemas de información, la plataforma tecnológica, redes informáticas, entre otros; a raíz de lo anterior, se estableció un plan de acción que permitió mitigar el impacto de los riesgos detectados.

No obstante, es importante indicar que actualmente se está llevando a cabo un nuevo estudio de vulnerabilidades mediante la contratación 2014CD-000003-1150 “Servicios Profesionales para el análisis de vulnerabilidades y riesgos a la seguridad en TIC en la CCSS”, en el cual la empresa Deloitte es la responsable de realizar dicho estudio.

Según minuta TI-001-2014 del 18 de junio del 2014, se establece como fecha de finalización del estudio de vulnerabilidades para el 19 de febrero del 2015, sin embargo, a la fecha del presente informe, dicho estudio todavía se encuentra en proceso de ejecución. De acuerdo con lo indicado por la Administración Activa, el principal retraso que ha sufrido la elaboración de este análisis se debe a diferentes incumplimientos en la entrega de los productos por parte de la empresa contratada, por lo cual se le han aplicado las multas económicas correspondientes.

Las Normas Técnicas para la Gestión y Control de las Tecnologías de Información, establecen en su artículo 1.4.4 que:

> *“La organización debe implementar las medidas de seguridad relacionadas con la operación de los recursos de TI y las comunicaciones, minimizar su riesgo de fallas y proteger la integridad del software y la información.*
>
> *Para ello debe:*
>
> *a. Implementar los mecanismos de control que permitan asegurar la no negación, la autenticidad, la integridad y la confidencialidad de las transacciones y de la transferencia o intercambio de información.*
> *b. Establecer procedimientos para proteger la información almacenada en cualquier tipo de medio fijo o removible (papel, cintas, disco, otros medios), incluso los relativos al manejo y desecho de esos medios.*
> *c. Establecer medidas preventivas, detectivas y correctivas con respecto a software “malicioso” o virus.”*

Es importante indicar que en el estudio de vulnerabilidades realizado en el 2007, se le había recomendado a la Administración Activa lo siguiente:

> *“Dada la importancia de mantener la confidencialidad, integridad/autenticidad y no repudio de la información administrada a través de SICERE, se debe valorar la utilización de medio de encriptación que brinden el beneficio de proteger aquella información que haya sido clasificada como sensible o crítica (tanto la almacenada como la transmitida) en concordancia con la “Política de Clasificación de la Información”*

Referente a lo anterior, mediante oficio SFA-0774-06-N del 1 de noviembre del 2006, suscrito por el Lic. Alexander Angelini Mora, en aquel entonces coordinador de la Subárea de Sistemas Financieros Administrativos, indicó lo siguiente:

> *"…La encriptación de la información es una labor NO VIABLE, dado que se deben modificar todos los apps, no solo para SICERE, sino para todos los aplicativos integrados a dicho sistema, tales como: PEAS-SMM-GGCC-SPIC-Planilla Autogestión-RCPI-SICO-Retiro FCL-Facturas Médicas-Consulta Morosidad-SICERE Virtual, entre otras. Además, la siguiente versión del SICERE contempla el uso de certificados SSL de 128 bits en el servidor de aplicaciones y el bloqueo del acceso directo a la BD por parte del cliente; adicional fortalecimiento del esquema de seguridad indicado…"*

Sobre el estado de las recomendaciones indicadas en el estudio de vulnerabilidades realizado en el año 2007, la Licda. Mayra Ulate Rodríguez, Jefe del Área de Seguridad y Calidad Informática, indicó lo siguiente:

> *"Quedaron algunos aspectos relacionadas propiamente con soporte técnico, y esto se debió a que en ese periodo se estaba gestionando la migración de la plataforma tecnológica al DataCenter, razón por la cual algunos aspectos señalados en el informe quedaron sin efecto, o bien, se solventaron de otra forma.*
>
> *Es relevante indicar que aquellos aspectos que no se ejecutaron, se procedió a realizar la respectiva justificación, la cual se analizó con la empresa contratada en el seguimiento; muchas obedecieron al cambio de la plataforma, migración del DataCenter, limitaciones tecnológicas del momento, entre otras. Sin embargo, la mayoría de las recomendaciones quedaron cumplidas."*

Así mismo, sobre el estudio de vulnerabilidades que se está ejecutando actualmente en conjunto con la empresa Deloitte, la Licda. Ulate manifestó:

> *"Con la empresa Deloitte hemos tenido una serie de inconvenientes con la realización de este estudio, principalmente dicha empresa ha presentado retrasos en la entrega de los productos solicitados en el cartel, por lo que nos hemos vistos obligados a realizar las respectivas multas económicas por la entrega tardía de los productos.*
>
> *Actualmente, estamos a la espera de la entrega de algunos productos como por ejemplo: la fase de la ingeniería social, evaluación de equipos médicos, entre otros.*

Sin embargo, es difícil en estos momentos establecer una fecha de finalización, puesto que hemos alcanzado el límite de sanciones económicas a la empresa (en su momento era una forma para ejercer presión por la entrega de los productos), por lo que esta situación podría propiciar que la empresa contratada prolongue la entrega final del informe.

En estos momentos estamos en conversaciones con la empresa para finalizar el informe lo más pronto posible, ya que los resultados evidenciados son de suma importancia para nosotros."

La Administración al no disponer de un estudio de vulnerabilidades y riesgos a la seguridad en TIC, podría ocasionar que no haya certeza del estado actual de seguridad informática en la información que se administra, y por lo tanto se encontraría expuesta a eventuales accesos no autorizados, ataques o hackeo[6], así como exposición, alteración y/o pérdida de información sensible lo cual afectaría la continuidad de los servicios que presta la Institución.

5. REFERENTE A LA IMPLEMENTACIÓN DE SOLUCIONES TECNOLÓGICAS PARA LA SEGURIDAD DE LOS DATOS.

Se evidenció que la Institución presenta debilidades en la implementación de soluciones tecnológicas para garantizar razonablemente la seguridad de los datos almacenados, tales como análisis forense, criptografía, prevención de pérdida de datos, autentificación, seguridad en bases de datos, entre otros los cuales permitirían haber fortalecido la base de datos de SICERE ante ataques como los recibidos actualmente.

Las Normas Técnicas para la Gestión de Tecnologías de Información y Comunicaciones, establece en el artículo 2.3 "Infraestructura tecnológica", lo siguiente:

"La organización debe tener una perspectiva clara de su dirección y condiciones en materia tecnológica, así como de la tendencia de las TI para que conforme a ello, optimice el uso de su infraestructura tecnológica, manteniendo el equilibrio que debe existir entre sus requerimientos y la dinámica y evolución de las TI."

Adicionalmente, establece en el capítulo 3.3 "Implementación de la infraestructura tecnológica", lo siguiente:

"La organización debe adquirir, instalar y actualizar la infraestructura necesaria para soportar el software de conformidad con los modelos de arquitectura de información e infraestructura tecnológica y demás criterios establecidos…"

[6] Irrumpir o entrar de manera forzada a un sistema de cómputo o a una red.

Referente a la disponibilidad de las soluciones tecnológicas que fortalecen la seguridad informática en la Institución, la Licda. Mayra Ulate Rodríguez, Jefe del Área de Seguridad y Calidad Informática, indicó lo siguiente:

> *"Las soluciones tecnológicas incluidas en el Plan de Acción para el fortalecimiento de la Infraestructura de Seguridad en TIC se vienen planificando desde hace mucho tiempo, así lo pueden corroborar en el Mapa de Ruta elaborado por el ASCI en el año 2011 aproximadamente, lo que sucede es que no hemos podido ejecutar todas las soluciones principalmente por la falta de recurso humano, así como la falta de presupuesto para la compra de herramientas. Debido a lo anterior, hemos tenido que priorizar la implementación de dichas las soluciones con el fin de disponer de un esquema de seguridad lo suficientemente robusto.*
>
> *Es importante indicar que el Plan de Acción está alineado al Mapa de Ruta del ASCI."*

La ausencia de herramientas tecnológicas que fortalezcan la seguridad informática en la Institución podría generar una brecha que facilite diversos ataques informáticos, trayendo consigo graves consecuencias para la CCSS, como por ejemplo: robo de información sensible y confidencial, pérdida de datos, daños a la plataforma tecnológica, entre otros, lo cual además podría impactar negativamente en la imagen institucional.

6. REFERENTE A LA IMPLEMENTACIÓN DE MECANISMOS DE MONITOREO SOBRE LOS SISTEMAS DE INFORMACIÓN.

Se evidenció que la Institución presenta oportunidades de mejora en los servicios de monitoreo, propiamente en temas como la implementación de indicadores que permitan alertar oportunamente cuando el límite de accesos a las aplicaciones es sobrepasado, detectar comportamientos irregulares en el uso de los sistemas de información, afectaciones al rendimiento de las herramientas tecnológicas, entre otros.

Las Normas de Control Interno para el Sector Público, en su apartado 3.3 "Vinculación con la planificación estratégica", señalan respecto a los indicadores de gestión lo siguiente:

> *"La valoración del riesgo debe sustentarse en un proceso de planificación que considere la misión y la visión institucionales, así como objetivos, metas, políticas e indicadores de desempeño claros, medibles, realistas y aplicables, establecidos con base en un conocimiento adecuado del ambiente interno y externo en que la institución desarrolla sus operaciones, y en consecuencia, de los riesgos correspondientes.*

Asimismo, los resultados de la valoración del riesgo deben ser insumos para retroalimentar ese proceso de planificación, aportando elementos para que el jerarca y los titulares subordinados estén en capacidad de revisar, evaluar y ajustar periódicamente los enunciados y supuestos que sustentan los procesos de planificación estratégica y operativa institucional, para determinar su validez ante la dinámica del entorno y de los riesgos internos y externos".

Además, el compendio de buenas prácticas en tecnologías de información y comunicaciones COBIT 4.1, en su dominio de "*Planear y Organizar*", define:

"(…) Supervisión
(…) Implementar prácticas adecuadas de supervisión dentro de la función de TI para garantizar que los roles y las responsabilidades se ejerzan de forma apropiada, para evaluar si todo el personal cuenta con la suficiente autoridad y recursos para ejercer sus roles y responsabilidades y para revisar en general los indicadores clave de desempeño (…)".

Referente a los mecanismos de monitoreo que permitan detectar oportunamente usos irregulares de las aplicaciones informáticas, tal y como sucedió con el SICERE, la Licda. Mayra Ulate Rodríguez, Jefe del Área de Seguridad y Calidad Informática, mencionó lo siguiente:

"En el caso específico del hackeo de SICERE, el cual se produjo a través de mecanismos válidos (disponían de un usuario otorgado por la CCSS, utilizaron protocolos y medios de autentificación válidos, etc), es muy difícil que alguna herramienta pueda detectar este tipo de infiltraciones, ya que cumplen con todas las reglas para el acceso al sistema de información.

Actualmente los mecanismos de monitoreo se centran en detectar aquellos accesos no autorizados que intentan vulnerar a las aplicaciones de la CCSS, para ello la Institución ha realizado una importante inversión económica en la compra de herramientas que fortalecen la seguridad informática, como por ejemplo: IPS, correlacionar de eventos, Firewalls, antivirus, entre otros.

Ahora bien, la contratación de Tercerización de Servicios de Seguridad que se está gestionando, incluye el análisis de APT por sus siglas en inglés, (Advanced Persistent Threat), Amenazas Persistentes Avanzadas, que analiza entre otras cosas el tráfico para determinar si existe accesos realizados con herramientas especializadas, con el fin de alertar de algún posible uso irregular de los sistemas."

La insuficiencia de mecanismos de monitoreo podría ocasionar que en caso de materializarse algún evento que afecte la continuidad en la prestación de los servicios de la plataforma tecnológica, no se disponga de información que permita evidenciar la magnitud o intensidad de la situación o el grado de avance de su atención.

CONCLUSIONES

En la presente evaluación se determinó oportunidades de mejora en torno al fortalecimiento de la gestión de la seguridad de la información, y así contribuir con el aseguramiento de la confidencialidad, integridad y disponibilidad de la información.

En este sentido, es necesario que la Institución valore la inversión de nuevas herramientas que ayuden a fortalecer la seguridad de la plataforma tecnológica, ya que según las métricas expuestas por la empresa Gartner, recomienda a las empresas invertir aproximadamente un 6% del presupuesto total destinado a tecnologías de información y comunicaciones.

Otro aspecto fundamental, es la necesidad de disponer del personal humano suficiente y competente que permita gestionar razonablemente los recursos destinados a la seguridad en TIC, por tanto, es importante indicar que un profesional especializado en seguridad informática, debe ser capaz de aplicar las metodologías, tecnologías y herramientas que existen en las distintas áreas involucradas, como lo es criptografía, modelos formales de seguridad informática, análisis forense, etc. , así como en las áreas en las que la seguridad informática tiene su aplicación: redes, sistemas operativos, aplicaciones. De igual forma deben también ser capaces de gestionar incidentes, riesgos y garantizar la continuidad del negocio, protegiendo los activos críticos de la Institución.

Adicionalmente, es importante que la Institución disponga de políticas de seguridad de la información acordes con las Normas Técnica para la Gestión de las Tecnologías de Información de la Contraloría General de la Repúblicas, así como otros estándares internacionales como el ISO27001, con el fin de articular la organización en cuanto a la seguridad de la información y brindando instrucciones claras a todos los funcionarios de las conductas esperadas y apropiadas, sirviendo como soporte para el logro de los objetivos de la Institución.

En este mismo orden de ideas, resulta relevante que la CCSS implemente indicadores que permitan alertar oportunamente cuando el límite de accesos a las aplicaciones es sobrepasado, detectar comportamientos irregulares en el uso de los sistemas de información, afectaciones al rendimiento de las herramientas tecnológicas, entre otros.

CAJA COSTARRICENSE DE SEGURO SOCIAL
AUDITORIA NTERNA
Tel.: 2539-0821 - Fax.: 2539-0888
Apdo.: 10105

RECOMENDACIONES

A LA GERENCIA DE INFRAESTRUCTURA Y TECNOLOGÍAS

1. Brindar seguimiento al Plan de Acción para el Fortalecimiento de la Infraestructura de Seguridad en Tecnologías de Información y Comunicaciones, lo anterior con el propósito de garantizar un monitoreo integral de las acciones definidas por la Dirección de Tecnologías de Información y Comunicaciones (DTIC). **Plazo de cumplimiento 6 meses.**

2. Establecer una estrategia que permita solventar la problemática relacionada con la insuficiencia del recurso humano especializado en materia de seguridad informática, para lo anterior se podría valorar las siguientes opciones:

a. Dotar de plazas al Área de Seguridad y Calidad Informática, con el fin de contratar personal que disponga con los atestados académicos o especializaciones en seguridad informática, los cuales le permitan solventar las necesidades actuales de dicha área.
b. Definir un plan de capacitaciones acorde con las necesidades actuales del Área de Seguridad y Calidad Informática, cuyo propósito sea formar funcionarios con especialidades en materia de seguridad informática, los cuales aporten técnicas y conocimientos a los procesos que actualmente se ejecutan en la Institución.
c. Valorar la contratación de servicios profesionales, los cuales garanticen la disponibilidad de personal pertinente y competente, así como especialistas en diferentes temas relacionados con la seguridad informática.
d. Cualquier otra estrategia que la Administración Activa considere pertinente con el fin de garantizar la aplicación de los conceptos, metodologías, herramientas, normativas y estándares existentes en esta materia, cuyo fin sea fortalecer la seguridad informática en la Institución.

Sobre este tema, es importante indicar que un profesional especializado en seguridad informática, debe ser capaz de aplicar las metodologías, tecnologías y herramientas que existen en las distintas áreas involucradas, como lo es criptografía, modelos formales de seguridad informática, análisis forense, etc. , así como en las áreas en las que la seguridad informática tiene su aplicación: redes, sistemas operativos, aplicaciones. De igual forma deben también ser capaces de gestionar incidentes, riesgos y garantizar la continuidad del negocio, protegiendo los activos críticos de la Institución. **Plazo de cumplimiento: 6 meses**

3. Establecer un equipo de trabajo conformado por representantes de cada gerencia de la Institución, así como de la Dirección de Tecnologías de Información y Comunicaciones, con el fin de atender los siguientes aspectos:

San José, Costa Rica. Ave. 2da, calles 5 y 7. Teléfono 2539-0821, Fax 2539-0888

- Realizar un análisis de los sistemas de información institucionales que requieran fortalecer su esquema de seguridad, lo anterior basado en los siguientes aspectos: importancia de la información que almacena, exposición a usuarios externos a la CCSS, sensibilidad de los datos, entre otros que se consideren convenientes.

- En coordinación con los comités de usuarios de los sistemas de información que se seleccionen en el punto anterior, valorar la posibilidad de establecer parámetros que permitan generar alarmas cuando la cantidad de accesos permitidos son sobrepasados, lo anterior le permitiría a los administradores de los sistemas actuar oportunamente ante cualquier uso irregular de las aplicaciones informáticas de la CCSS y que pudieran afectar el rendimiento de la plataforma tecnológica.

- De igual forma, en coordinación con los comités de usuarios de los sistemas de información, realizar un análisis que permita definir la información sensible almacenada en las bases de datos, lo anterior con el propósito de implementar mecanismos de control que permitan incrementar la seguridad en su acceso, dentro del análisis podría valorarse la posibilidad de la encriptación de datos o cualquier otro que se considere pertinente.

  En caso de que los resultados de dicho análisis resulten factibles de implementar, elaborar un plan que incluya responsables, actividades, plazos, entre otros; orientados a la implantación de las medidas de seguridad que se consideren necesarias.

  Es importante indicar que para el cumplimiento de la presente recomendación se necesita la conformación de un equipo de trabajo formado por representantes de diferentes gerencias, por tanto el plan solicitado en el párrafo anterior podría ser elaborado para cada sistema de información, o bien, realizar un solo plan para un conjunto de sistemas de información que pertenecen a cada gerencia, tal y como el equipo de trabajo considere conveniente.

Es importante resaltar que los aspectos de coordinación con las demás unidades será responsabilidad de la Gerencia de Infraestructura y Tecnologías. **Plazo de cumplimiento 9 meses**

A LA DIRECCIÓN DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES

4. Considerando que el Área de Seguridad y Calidad Informática en conjunto con la empresa Deloitte se encuentran desarrollando un estudio de vulnerabilidades y riesgos a la seguridad en TIC, y debido a los retrasos en la entrega de los productos por parte de la empresa contratada, es importante que esta Dirección brinde seguimiento a la ejecución de dicho estudio, lo anterior con el propósito de evitar nuevos retrasos en la entrega de los resultados. Así mismo, es importante que se garantice el cumplimiento de la normativa en el proceso contractual.

Debido a los hechos presentados recientemente en relación con el hackeo al SICERE, es importante que la Institución disponga a la mayor brevedad posible de un estudio de vulnerabilidades de la seguridad en TIC, con el fin de establecer diversas medidas correctivas que le permitan subsanar todas las debilidades detectadas en dicho estudio. **Plazo de cumplimiento 12 meses**

5. Elaborar un marco normativo en relación con los siguientes temas:

- Administración de amenazas y vulnerabilidades.
- Protección de datos.
- Atención de incidentes.
- Clasificación de la información.
- Controles criptográficos.

Una vez elaborado dicho marco normativo, deberá enviarse a las instancias correspondientes con el propósito de proceder con la oficialización de los documentos.

Lo anterior, con el fin de fortalecer la gestión integral de la seguridad de la información, y así contribuir con el aseguramiento de la confidencialidad, integridad y disponibilidad de la información asociada a los servicios que ofrece la Caja Costarricense de Seguro Social. **Plazo de cumplimiento 6 meses.**

COMENTARIO

De conformidad con lo establecido en el artículo 45 del Reglamento de Organización y Funcionamiento de la Auditoría Interna, los resultados del presente estudio fueron comentados el 29 de febrero del 2016, con la presencia de los licenciados Jorge Porras Pacheco, Asesor de la Gerencia de Infraestructura y Tecnologías, Ana María Castros Molina, Jefe Subárea Seguridad de la Información y Manuel Montillano, funcionaria de la Dirección de Tecnologías de Información y Comunicaciones, en la cual se hicieron las siguientes observaciones:

"Referente a la recomendación 3 y 4, relacionadas con la coordinación con los comités de usuarios de los sistemas de información para el establecimiento de alarmas cuando la cantidad de accesos permitidos son sobrepasados, así como el análisis para definir la información sensible almacenada en las bases de datos y así fortalecer la seguridad en el acceso; la Administración considera conveniente dirigir estas recomendaciones a una instancia superior a la Gerencia de Infraestructura y Tecnologías, lo anterior debido a que existen sistemas de información que pertenecen a otras gerencias, tal es el caso del Sistema Institucional de Pensiones (SIP), Sistema Centralizado de Recaudación (SICERE), entre otros; por lo tanto, consideran que dicha instancia puede realizar las labores de coordinación y supervisión entre las gerencias.

CAJA COSTARRICENSE DE SEGURO SOCIAL
AUDITORIA NTERNA
Tel.: 2539-0821 - Fax.: 2539-0888
Apdo.: 10105

Respecto a la recomendación 5, sobre el seguimiento al estudio de vulnerabilidades desarrollado por la empresa Deloitte, la Licda. Castro Molina indica que parte del seguimiento que le podría brindar al desarrollo de este estudio, podría ser la elaboración de informes de avances gerenciales, los cuales presentaran el progreso en la ejecución del estudio. Asimismo, considera prudente incrementar el plazo de la recomendación en función de la disponibilidad de recursos de la Subarea de Seguridad en TI que sería la de que directamente tendrá que asumir este tema y de que en caso de requerirse presupuesto para materializar cualquier recomendación es de considerar que el planteamiento de dichos presupuestos es anual.

Finalmente, con respecto a la recomendación 6 relacionada con la elaboración y oficialización del marco normativo, la Licda. Castro Molina indica que es conveniente ajustar el texto de la recomendación, tal y como se muestra a continuación:
<u>Original:</u>
"…Una vez elaborado dicho marco normativo, deberá enviarse a la Gerencia de Infraestructura y Tecnologías con el propósito de proceder con la oficialización de los documentos…"
<u>Propuesta:</u>
"…Una vez elaborado dicho marco normativo, deberá enviarse a las instancias correspondientes con el propósito de proceder con la oficialización de los documentos…"
Lo anterior según el tipo de documento del marco normativo que se esté gestionando."

Con respecto a lo anterior, esta Auditoría se reunió el 16 de marzo del 2016 con la Lic. Rita Cubillo Jiménez, Asesora de la Presidencia Ejecutiva, con el propósito de comentarle las observaciones realizadas con respecto a las recomendaciones relacionadas con la implementación de alarmas en los sistemas de información cuando la cantidad de accesos son sobrepasados, así como el análisis de la información sensible almacenada en las bases de datos; en dicha reunión se acordó que una forma razonable de cumplir con estas recomendaciones consiste en la conformación por parte de la Gerencia de Infraestructura y Tecnologías, de un grupo de trabajo integrado por representantes de las gerencias, el cual se encargue de ejecutar las acciones correspondientes que les permitan acatar lo establecido por esta Auditoría.

ÁREA TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES

Firmado digitalmente por RANDALL ARAYA LUNA (FIRMA)
Fecha: 2016.04.12 11:15:37 -06'00'

Lic. Randall Araya Luna
ASISTENTE DE AUDITORÍA

RAFAEL ANGEL HERRERA MORA (FIRMA)
Firmado digitalmente por RAFAEL ANGEL HERRERA MORA (FIRMA)
Fecha: 2016.04.12 11:23:05 -06'00'

Lic. Rafael Herrera Mora
JEFE

RHM/RJAL/lba

San José, Costa Rica. Ave. 2da, calles 5 y 7. Teléfono 2539-0821, Fax 2539-0888