AUDITORIA JUDICIAL

Informe de Auditoría para el mejoramiento del control interno relativo a la seguridad de las bases de datos sensibles de llamadas confidenciales y Protección a Víctimas y Testigos

Sección de Auditoría de Tecnologías de Información

Noviembre, 2016

AUDITORIA JUDICIAL
TELEFONO: 2295-3238
FAX: 2257-05-85
APARTADO: 79-1003 SAN JOSE

N° 1222-80-SATI-2016

17 de noviembre de 2016

Licenciado
Elpidio Calderón Chaves, Jefe
Unidad Tecnológica Informática
Organismo de Investigación Judicial

Estimado señor:

De conformidad con lo dispuesto en el Artículo 36 de la Ley General de Control Interno, le remito el estudio efectuado por la Sección de Auditoría de Tecnología de Información del Despacho a mi cargo denominado **"*Evaluación de las Bases de Datos sensibles de Protección a las Víctimas y Testigos y de las llamadas confidenciales*".**

En el informe de referencia, se logran determinar importantes oportunidades de mejora donde se denota la necesidad de desarrollar un nuevo sistema de información para el Centro de Información Confidencial del OIJ.

Cabe resaltar, la conveniencia de fortalecer los controles para desarrollar, formalizar y poner en práctica una aplicación que permita de manera integral, ágil y segura, la recopilación de la información suministrada mediante las llamadas confidenciales. Estas condiciones mencionadas incrementan el riesgo de una inadecuada recopilación de la información, lentitud en la atención y posibles pérdidas de información sensible.

Por otra parte, la base de datos de Protección de las Víctimas y Testigos, es administrada mediante el Sistema Costarricense de Gestión de Despachos Judiciales y el Escritorio Virtual, para los cuales se lleva a cabo un nuevo desarrollo, el cual será evaluado oportunamente por esta Auditoría.

No omito indicar que con la implementación de las recomendaciones emitidas se pretende minimizar el riesgo de que en el futuro se presenten las debilidades detectadas. Además, es relevante señalar que de conformidad con lo establecido en la Ley General de Control Interno, esta Auditoría efectuará en su momento un seguimiento, para asegurarse de que las acciones establecidas por las instancias competentes, se hayan implementado eficazmente y dentro de los plazos definidos en cada caso.

Atentamente,

Carlos Castro Hernández
Subauditor Judicial

maal

c: Consejo Superior
Oficina de Planes y Operaciones del OIJ
Sección Auditoría Tecnología de Información
Archivo.-

TABLA DE CONTENIDO

Evaluación de las Bases de Datos Sensibles de llamadas confidenciales y Protección a Víctimas y Testigos

1 INTRODUCCIÓN

1.1 Trámite de los informes de auditoría según la Ley General de Control Interno.

El artículo 36 de la Ley General de Control Interno, establece el tratamiento que los titulares subordinados encargados de las áreas evaluadas, deben dar a los informes de fiscalización que emite la Auditoría Interna, el cual incluye, la orden de implementación de las recomendaciones vertidas en el informe o el planteamiento de discrepancia ante el Jerarca, en el plazo de diez días hábiles a partir de la fecha de recibido el documento.

A su vez, el artículo 39 de la citada Ley advierte de la responsabilidad administrativa o civil que puede acarrear sobre los responsables, la inobservancia de las recomendaciones emitidas por la Auditoría Interna.

1.2 Origen del estudio

Estudio no programado realizado de conformidad con las competencias que son atinentes a esta Auditoría, establecidas en el artículo 22 de la Ley General de Control Interno.

1.3 Objetivo general

Evaluar si la información contenida en las bases de datos empleadas para las llamadas confidenciales y para la Protección de las Víctimas y Testigos, posee controles de seguridad acordes con la normativa vigente.

1.4 Alcance y naturaleza

Esta evaluación comprendió el análisis de los controles de acceso a la información y medios de almacenamiento para determinar la adecuada conservación de su integridad y confidencialidad.

Para llevar a cabo este estudio, se analizó el Sistema de Información Confidencial (SIC) del Centro de Información Confidencial (CICO) del OIJ y el Sistema de Información empleado para la Protección a las víctimas y testigos en el Poder Judicial.

El estudio comprendió la situación encontrada al momento de la auditoría, con fecha de corte al 12 de octubre del 2016.

1.5 Equipo de Trabajo

El estudio fue desarrollado por el máster Miguel Ángel Azofeifa Lizano, bajo la coordinación de la Msc. Alicia Sancho Brenes, jefe de la Sección de Auditoría de Tecnología de Información.

1.6 Normativa técnica aplicada

Para la ejecución de este estudio se observaron las Normas Generales de Auditoría para el Sector Público (R-DC-064-2014) y las Normas de control interno para el Sector Público (N-2-2009-CO-DFOE, ambos promulgados por la Contraloría General de la República.

1.7 Difusión verbal de los resultados

Este estudio fue puesto en conocimiento del área auditada mediante informe en borrador No. 1106-76-SATI-2016 del 27 de octubre del 2016, y conferencia final efectuada el 09 de noviembre del 2016.

En dicha reunión participaron de la Unidad Tecnológica Informática:

- Lic. Roger Martínez Ruiz.

Y por parte de la Auditoría:

- Msc. Alicia Sancho Brenes.
- Master. Miguel Ángel Azofeifa Lizano.

Para la redacción de este informe se consideraron las observaciones de la administración.

2 RESULTADOS DEL ESTUDIO

Como producto de la auditoría realizada a la base de datos utilizada para la Protección de las Víctimas y Testigos, se determinó que es administrada mediante el Sistema Costarricense de Gestión de Despachos Judiciales y el Escritorio Virtual, los cuales, si bien al momento de nuestra intervención presentan aspectos de mejora relacionados con la seguridad de la información, también se pudo constatar que se lleva a cabo un nuevo desarrollo en dichos sistemas, en cuya plataforma se solventarán los riesgos detectados. Este desarrollo será evaluado posteriormente por esta Auditoría, cuyos resultados se comunicarán oportunamente.

En relación con la base de datos de llamadas confidenciales, se determinaron algunos aspectos susceptibles de mejora, los cuales se detallan a continuación:

2.1 Conveniencia de desarrollar un nuevo sistema de información para el Centro de Información Confidencial del Organismo de Investigaciones Judiciales (OIJ)

El Sistema de Información Confidencial (SIC) que es utilizado por el Centro de Informaciones Confidenciales (CICO), se encuentra desarrollado en un lenguaje de programación obsoleto, con un motor de base de datos sin soporte del proveedor, mediante este sistema se registra la información de las llamadas que ingresan al OIJ a través del número 800-8000-OIJ, para ellos se dispone de un grupo de 4 servidores judiciales que en turnos rotativos reciben las denuncias que provienen de todas partes del país.

Es importante indicar, que el sistema inicialmente fue una plantilla hecha en el software aplicativo MS-Access y posteriormente se desarrolló bajo el mismo esquema en la base de datos en la que se encuentra actualmente. Cabe resaltar, que los informáticos del OIJ están conscientes de esta deficiencia, pero aducen que a pesar del riesgo identificado no hay un proyecto para desarrollarla en una nueva plataforma tecnológica.

En visita de esta Auditoría al CICO, el coordinador de esta Unidad mencionó que en algún momento se pretendió que con el módulo de denuncias del Sistema de Expediente Criminal Único (ECU) se solventaría la necesidad de crear un nuevo sistema, no obstante, dicho módulo no es práctico ni reúne las características de diseño para atender las llamadas que se originan en este despacho.

El sistema de referencia actualmente está desarrollado mediante objetos de conexiones conocidos como "ODBC" a la Base de Datos por medio de un usuario y clave única, lo cual incrementa el riesgo de la seguridad de la información, pues sería vulnerable fácilmente al no manejar claves y perfiles por usuario, cuenta con una bitácora de transacciones que registran todos los eventos, no obstante, no se registra el nombre del usuario que las efectúa, lo que registra la bitácora es la dirección y el nombre de la computadora desde donde se accede al sistema.

Otra limitante que se pudo observar en cuanto al uso del sistema de referencia, es que no cumple con todos los requisitos necesarios por parte de los usuarios para almacenar la información de las llamadas de denuncias y archivos aportados por los informantes, su diseño es limitado en cuanto a la facilidad de recopilar la información aportada, pues se carece de campos que registren de una forma detallada la información suministrada en un evento acontecido.

Al respecto el numeral 1.4 de las Normas Técnicas para la gestión y el control de las Tecnologías de Información (N-2-2007-CO-DFOE) de la Controlaría General de la República, indican lo siguiente:

> "*1.4 Gestión de la seguridad de la información*
> *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."*

Además, el numeral 3.2 de las mismas normas supra citadas al referirse al diseño de los sistemas indica lo siguiente:

> "3.*2 Implementación de software*
> *La organización debe implementar el software que satisfaga los requerimientos de sus usuarios y soporte efectivamente sus procesos."*

La causa por la cual no se ha desarrollado un nuevo sistema de referencia, es debido a que no se ha denotado la prioridad requerida para la actualización del sistema de información de llamadas confidenciales, por parte de la Administración del OIJ.

Dentro de los riesgos que existen al no contar con un sistema informático que cumpla con los requerimientos de diseño y seguridad de la información se pueden detallar:

- Inadecuada recopilación de la información brindada por el denunciante debido a que el sistema no cumple con los requerimientos deseados para el almacenamiento de la información. Esto dificulta asegurar la solicitud de toda la información relevante, así como dificulta la extracción de información para reportes o estadísticas, para la mejora continua del control interno del proceso, así como para obtener información de análisis criminal.

- Lentitud o prolongación del tiempo que requiere el operador que recibe las llamadas debido al inadecuado diseño de la aplicación.

- Pérdida, alteración o divulgación de la información, lo cual se puede presentar por personas con acceso autorizado al sistema, sin que haya posibilidad de establecer responsabilidades debido a la falta de identificación única de los usuarios, o por acceso no autorizado mediante malware[1] debido a la falta de soporte del software por parte del proveedor, lo cual produce que no se corrijan las debilidades de seguridad detectadas.

Ante la materialización de este riesgo se pueden presentar las siguientes situaciones:

  - Detrimento de la calidad del trabajo de investigación, por la ausencia de información valiosa aportada al caso.

  - Posibles efectos negativos contra el personal judicial y la ciudadanía en general, en caso de que algún individuo que se sienta afectado por alguna denuncia, decida tomar represalias contra un denunciante, alertado por la divulgación de la información contenida en este sistema.

  - Pérdida de la imagen de la institución en caso de que se materialice el riesgo relacionado con la divulgación o pérdida de datos que dificulten la resolución exitosa de casos.

[1] Malware: es la abreviatura de "Malicious software", término que engloba a todo tipo de programa o código informático malicioso cuya función es dañar un sistema o causar un mal funcionamiento.

3 CONCLUSIONES DEL ESTUDIO

La información contenida en las bases de datos empleadas para las llamadas confidenciales se administra mediante el sistema "SIC" del Centro de Informaciones Confidenciales y presenta un riesgo importante en cuanto a la seguridad de la información por la obsolescencia del software y el diseño de una clave genérica de conexión para todos los usuarios. Además que no cumple con los requerimientos de los usuarios en cuanto al registro y consulta de información.

Por otra parte, la base de datos utilizada para la Protección de las Víctimas y Testigos administrada por el Sistema de Gestión y el Escritorio Virtual, también tiene falencias de seguridad de la información, sin embargo, se espera que un nuevo desarrollo que se lleva a cabo solvente dicho riesgo.

4 RECOMENDACIONES DEL ESTUDIO

A LA UNIDAD TECNOLOGICA INFORMÁTICA DEL OIJ

4.1 Desarrollar un nuevo Sistema de Información para el Centro de Información Confidencial del OIJ, con el fin de facilitar las labores de captura, almacenamiento y administración de la información que se suministra mediante las llamadas anónimas y confidenciales de los denunciantes que se originan en todo el país.

Es de suma importancia que este sistema contemple los niveles de seguridad requeridos, a fin de proporcionar razonablemente la confidencialidad, integridad y disponibilidad de la información, tal y como lo dictan las normas que lo rigen y las mejores prácticas internacionales en dicha materia.

Plazo de cumplimiento: Noviembre del 2017

5 OTRAS OBSERVACIONES DE LA ADMINISTRACIÓN

En reunión de comunicación de resultados el representante de la UTI señaló que el 26 y 27 de octubre del 2016, se realizaron reuniones con el propósito de obtener recursos y establecer los requerimientos, a fin de desarrollar un nuevo módulo dentro del ECU para atender las llamadas confidenciales, lo cual será corroborado posteriormente por esta Auditoría para considerarla como una solución alterna a la recomendación.