02 de diciembre de 2016
AI-396-2016

Doctor
Alberto López Chaves, MBA
Gerente

Asunto: Remisión de Informe AI-C-014-2016

Estimado señor:

Se remite el Informe N° AI-C-14-2016, en el cual se consignan los resultados de la auditoría de cumplimiento sobre la gestión de las bases de datos institucionales.

El objetivo del estudio consistió en evaluar la administración de las bases de datos institucionales por parte del Departamento de TI, con el fin de comprobar el cumplimiento de las políticas y procedimientos establecidos y los marcos de referencia de las mejores prácticas de TI.

El día 30 de noviembre de 2016 la Auditoría Interna expuso los resultados, la conclusión y las recomendaciones obtenidas del estudio a la Gerencia y al responsable de poner en práctica las recomendaciones.

Según el artículo No. 36 de la Ley General de Control Interno, se recuerda el plazo de hasta diez días hábiles, contados a partir de la fecha de recibido el informe con que cuenta la Administración, para ordenar la implantación de las recomendaciones.

Las recomendaciones se emiten al amparo del artículo 35 de la Ley Orgánica del Instituto, la competencia que facultan los artículos 22, 35 y 36 de la Ley General de Control Interno.

Atentamente,

FERNANDO JOSE RIVERA SOLANO (FIRMA)

Firmado digitalmente por FERNANDO JOSE RIVERA SOLANO (FIRMA)
Nombre de reconocimiento (DN): serialNumber=CPF-03-0226-0040, sn=RIVERA SOLANO, givenName=FERNANDO JOSE, c=CR, o=PERSONA FISICA, ou=CIUDADANO, cn=FERNANDO JOSE RIVERA SOLANO (FIRMA)
Fecha: 2016.12.02 16:44:45 -06'00'

Fernando Rivera Solano
Auditor Interno

FRS/kbm

C. Lic. Sergio Lira Valdivia
Jefe Departamento de TI
Licda. Milena Moreno Rojas
Gerencia
Consecutivo

INFORME N° AI-C-014-2016

AUDITORÍA INTERNA
INSTITUTO COSTARRICENSE DE TURISMO

“INFORME DE AUDITORÍA DE CUMPLIMIENTO SOBRE LA GESTIÓN DE LAS BASES DE DATOS INSTITUCIONALES”

Diciembre, 2016

Instituto Costarricense de Turismo
Auditoría Interna
Tel. (506) 2299-5800
Fax (506) 2291-5721

CONTENIDO

RESUMEN EJECUTIVO DEL ESTUDIO

La auditoría se realizó en cumplimiento del Plan Anual de Trabajo y con el objetivo de evaluar la administración de las bases de datos institucionales por parte del Departamento de TI, con el fin de comprobar el cumplimiento de las políticas y procedimientos establecidos y los marcos de referencia de las mejores prácticas de TI.

El estudio determinó oportunidades de mejora en los siguientes aspectos:

- Herramientas de auditoría en las bases de datos.
- Gestión de las actualizaciones de las bases de datos.
- Esquema de clasificación de datos.
- Servicio de escucha (listener).
- Personal clave de TI.

Producto de los resultados obtenidos se generaron recomendaciones referentes a:

- Implementar las funciones de seguridad en las bases de datos institucionales, con el fin de contar con una herramienta que registre y detecte incidentes potenciales relacionados con las operaciones que realiza el DBA y otros funcionarios con privilegios.
- Establecer un procedimiento de mantenimiento periódico de la bases de datos (gestión de parches, estrategias de actualización, riesgos, análisis de vulnerabilidades y requerimientos de seguridad), con la finalidad de minimizar los riesgos por vulnerabilidades a las bases de datos Institucionales.
- Establecer un esquema de clasificación de datos, el cual según COBIT 4 y 5 debe contener al menos:
    - información sobre la criticidad o seguridad de la información,
    - asignación de la propiedad y custodia de los datos;
    - controles de seguridad apropiados para cada una de las clasificaciones de datos que requieran protección.
- Implementar las medidas necesarias para la protección del “listener” con el fin de resguardar y prevenir ataques a las bases de datos Institucionales y que se analice la posibilidad de cambiar el puerto 1522 a otro fuera de los rangos 1521-1550 y 1600-1699.

- Implementar un plan de respaldo del personal que realiza funciones críticas, con la finalidad de minimizar la dependencia de la Institución hacia funcionarios que podrían afectar la continuidad del negocio.

AI-C-014-2016

"INFORME SOBRE LA AUDITORÍA DE CUMPLIMIENTO SOBRE LA GESTIÓN DE LAS BASES DE DATOS INSTITUCIONALES"

1. INTRODUCCIÓN

1.1 Origen del estudio

La auditoría se realizó en cumplimiento del Plan Anual de Trabajo de la Auditoría Interna del año 2016

1.2 Objetivo general de la auditoría

Evaluar la administración de las bases de datos institucionales por parte del Departamento de TI, con el fin de comprobar el cumplimiento de las políticas y procedimientos establecidos y los marcos de referencia de las mejores prácticas de TI.

1.3 Alcance de la auditoría

Con la finalidad de cumplir con el objetivo planteado, se revisó la administración de las bases de datos Oracle y Windows SQL Server relacionas con:

- Actualizaciones
- Seguridad y monitoreo
- Acceso y autorización
- Respaldo y recuperación
- Encriptación de datos
- Seguridad de la red relacionada con las bases de datos
- Ambiente de control

El periodo revisado comprendió de enero a octubre de 2016.

1.4 Normas técnicas de la auditoría

El estudio se realizó de acuerdo con la normativa aplicable al ejercicio de la Auditoría Interna, así como lo establecido en las "Normas Generales de Auditoría para el Sector Público".

1.5 Marco legal

La normativa consultada en el estudio es la siguiente:

- Normas Técnicas para la gestión y el control de las TI emitidas por la CGR. (en adelante NTGCTI)

- Como mejor práctica:
    - COBIT[1] 4.1 en español
    - COBIT[2] 5.0 en español Procesos Catalizadores
    - www.oracle.com/technetwork
        - Whitepaper Seguridad: Opciones de Seguridad de la BD Oracle 10g R2 (Oracle Database Vault, Oracle Advanced Security Option y Oracle DataMasking), Abril 2009
        - Oracle Database Security Checklist, Junio 2008
        - Recommendations for Leveraging the Critical Patch Update and Maintaining a Proper Security Posture, Noviembre 2010
    - https://support.microsoft.com/es-es
        - Cómo determinar la versión y la edición de SQL Server y sus componentes[3]
    - https://technet.microsoft.com
        - Security Best Practices Checklist, Mayo, 2003
    - The Center for Internet Security (en adelante CIS)[4]
    - Integrigy[5]
        - WHITE PAPER: Oracle Database Listener Security Guide. Abril 2007

---

[1] - [2] Objetivos de Control para la Información y la Tecnología Relacionada" y conocido por sus siglas en inglés como COBIT. Este documento es desarrollado por la Information Systems Audit and Control Association (ISACA) y el IT Governance Institute (ITGI)

[3] https://support.microsoft.com/es-es/kb/321185

[4] Es una organización dedicada a mejorar la preparación y la respuesta de la seguridad cibernética entre las entidades del sector público y privado. Utilizando sus fuertes asociaciones industriales y gubernamentales, CIS combate la evolución de los retos de seguridad cibernética en una escala global y ayuda a las organizaciones a adoptar las mejores prácticas clave para lograr las defensas inmediatas y eficaces contra los ataques cibernéticos.

[5] Innovador líder en soluciones de seguridad para aplicaciones empresariales de misión crítica.

1.6 Limitación

No hubo ninguna limitación en el desarrollo del estudio.

1.7 Comunicación verbal de los resultados de la auditoría

En reunión celebrada el día 30 de noviembre de 2016 a las 2:00 p.m. en la sala de reuniones de la Auditoría Interna, se expusieron los resultados, conclusiones y recomendaciones (incluyendo los plazos probables de la ejecución de estas últimas) del presente informe al MBA. Alberto López Chaves, Gerente y al Lic. Sergio Lira Valdivia, Jefe del Departamento de TI.

1.8 Análisis realizado de las observaciones recibidas de la Administración

No hubo observaciones

2. RESULTADOS

2.1 HERRAMIENTAS DE AUDITORÍA EN LAS BASES DE DATOS

El Departamento de TI no ha activado la herramienta de auditoría en las bases de datos para controlar las operaciones que realizan el DBA y otros funcionarios con privilegios en las mismas.

Al respecto, la norma 1.4.5 “control de acceso” de las NTGCTI, indica que se debe establecer procedimientos para la definición de perfiles, roles y niveles de privilegio, y para la identificación y autenticación para el acceso a la información, tanto para usuarios como para recursos de TI, así como el establecimiento de los mecanismos necesarios que permitan un adecuado y periódico seguimiento al acceso a las TI.

Además, la práctica de gestión DSSO5.07 “Supervisar la infraestructura para detectar eventos relacionados con la seguridad” de COBIT 5 (p. 195) establece que se deben usar herramientas de detección de intrusiones, supervisar la infraestructura para detectar accesos no autorizados y asegurar que cualquier evento esté integrado con la supervisión general de eventos y la gestión de incidentes.

Por otra parte, Oracle en su documento "Whitepaper Seguridad: Opciones de Seguridad de la BD Oracle 10g R2 (Oracle Database Vault, Oracle Advanced Security Option y Oracle DataMasking)[6], así como, “Security Best Practices Checklist” para SQL[7], indican que las opciones de seguridad de la base de datos Oracle, dan cumplimiento a un amplio rango de regulaciones y normativas, como es la herramienta de auditoría de bases de datos.

El motivo por el cual no se ha activado la herramienta de auditoría en las bases de datos institucionales, es porque la Jefatura de TI la consideraba como un control de registros de todas las transacciones que se realizan en los sistemas -lo cual, según él, implica un alto consumo de recursos técnicos- y no solo para las que ejecuta el DBA y otros funcionarios con privilegios.

Por su parte, el DBA manifestó que la razón fundamental por la que no se ha activado el Audit Trail (pistas de auditoría), es porque los eventos sobre los datos Oracle están quedando registrados en bitácoras propias de las tablas de transacciones y que no conoce las características actuales del Audit Trail en función del registro de eventos y que en el caso de SQL Server, por ser paquetes

[6] www.oracle.com/technetwork/es/documentation/317541-esa.pdf

[7] https://technet.microsoft.com/library/Cc966456

de terceros las actividades de bitácoras quedan supeditadas al paquete correspondiente (bitácoras que traen los sistemas).

Lo indicado por el DBA se refiere a los movimientos que realizan los usuarios en los sistemas, éstos quedan en las bitácoras señaladas, pero, no se refirió a los registros de las operaciones por él realizadas como DBA y las efectuadas por funcionarios con privilegios que son las que no están quedando guardadas.

Al no estar activa la herramienta de auditoría en las bases de datos institucionales, no se dispone de información sobre las operaciones realizadas por el DBA y otros usuarios con privilegios especiales, lo que no permite que se puedan identificar posibles actividades sospechosas o maliciosas, que no se puedan prevenir ataques y detectar potenciales intrusos y, por lo tanto, no se tomen las soluciones pertinentes.

De acuerdo con lo identificado en este punto se recomienda a la Gerencia:

1. Instruir al Departamento de TI para que en un plazo de dos meses, implemente las funciones de seguridad en las bases de datos institucionales, con el fin de contar con una herramienta que registre las operaciones que realiza el DBA y otros funcionarios con privilegios y poder detectar posibles incidentes que pudieran afectar la información almacenada en las mismas.

2.2 GESTIÓN DE LAS ACTUALIZACIONES DE LAS BASES DE DATOS

En la verificación realizada sobre la versión actual de las de bases de datos Institucionales, se determinó que algunas no presentan la última actualización disponible, a continuación se detalla:

Nombre del Software de Base de Datos	Versión Actual en el ICT	Última Versión del Proveedor
Oracle Database 10 g	10.2.0.1	10.2.0.5
Microsoft SQL Server 2005	9.0.3042.00 (Service Pack 2)	9.0.5000.00 (Service Pack 4)
Microsoft SQL Server 2008 R2	10.50.1600.1	10.50.6000.34 (Service Pack 3)

Al respecto, la norma 1.4.1 “Seguridad en la implementación y mantenimiento de software e infraestructura tecnológica” de las NTGCTI, establece que la organización debe mantener la integridad de los procesos de implementación y mantenimiento de software e infraestructura tecnológica y evitar el acceso no autorizado, daño o pérdida de información, por lo que debe de contar con procedimientos claramente definidos para el mantenimiento y puesta en

producción del software e infraestructura. Asimismo, el mismo cuerpo normativo establece en la norma 4.1 “Administración y operación de la plataforma tecnológica”, que la organización debe mantener la plataforma tecnológica en óptimas condiciones y minimizar su riesgo de fallas por lo que debe establecer y documentar los procedimientos y las responsabilidades asociados con la operación de la plataforma.

Al respecto se tiene como buena práctica de referencia el COBIT en su versión 5, que establece en la práctica de gestión BAI03.10 “Mantener soluciones” (p. 138), que se debe desarrollar y ejecutar un plan para el mantenimiento de los componentes de la solución que incluya revisiones periódicas respecto a las necesidades de negocio y requerimientos operacionales tales como la gestión de parches, estrategias de actualización, riesgos, análisis de vulnerabilidades y requerimientos de seguridad.

Por otra parte, tanto Oracle[8], Microsoft[9] y la CIS[10] en sus parámetros de configuración de seguridad[11-12-13] recomiendan instalar la última versión de las bases de datos

El motivo por el cual algunas bases de datos institucionales no se encuentran actualizadas, es porque el Departamento de TI no cuenta con un procedimiento de mantenimiento periódico de las bases de datos (gestión de parches, estrategias de actualización, riesgos, análisis de vulnerabilidades y requerimientos de seguridad).

En entrevista con el jefe del Departamento de TI y el DBA, este último indicó que no hay un procedimiento para las revisiones y aplicación de los parches, sino que se mantiene una cuenta para el DBA en el sitio Oracle donde se consultan y donde nos envían información relacionada con la seguridad y aplicación de parches. Los parches se bajan directamente de este sitio para su aplicación posterior. Asimismo, el jefe del Departamento indicó que en el sistema queda registrada la última versión o la versión que está en operación por lo que con esto se puede determinar si se requiere alguna actualización.

---

[8] http://www.oracle.com/us/support/assurance/leveraging-cpu- wp- 164638.pdf?ssSourceSiteId=otnen

[9] https://technet.microsoft.com/library/Cc966456

[10] The Center for Internet Security

[11] https://benchmarks.cisecurity.org/tools2/sqlserver/CIS_SQL2005_Benchmark_v1.1.pdf

[12] https:// benchmarks.cisecurity.org/tools2 /sqlserver/ CIS_Microsoft_SQL_Server_2008 R2_Database _Engine_Benchmark_v1.0.0.pdf

[13] https://benchmarks.cisecurity.org/tools2/sqlserver/CIS_SQL2005_Benchmark_v1.1.pdf

No obstante lo anterior, las acciones indicadas por el Departamento de TI, no han sido suficientes para garantizar que la Institución cuente con todas las bases de datos actualizadas.

El no contar con un procedimiento de mantenimiento periódico de las bases de datos (gestión de parches, estrategias de actualización, riesgos, análisis de vulnerabilidades y requerimientos de seguridad) podría ocasionar que:

- No se corrijan a tiempo fallos de seguridad creando vulnerabilidades que pueden afectar la confidencialidad y disponibilidad de la información institucional.
- Se disminuya el funcionamiento general de las bases de datos afectando la eficiencia y eficacia de las operaciones de los sistemas Institucionales.
- La Institución no aproveche las nuevas funcionalidades o mejoras respecto de las versiones anteriores del software de base de datos, lo que podría afectar la eficiencia en los sistemas de información institucionales.

De acuerdo con el resultado obtenido se recomienda a la Gerencia:

2. Instruir al Departamento de TI para que en un plazo de dos meses, establezca un procedimiento de mantenimiento periódico de la bases de datos (gestión de parches, estrategias de actualización, riesgos, análisis de vulnerabilidades y requerimientos de seguridad), con la finalidad de minimizar los riesgos por vulnerabilidades a las bases de datos Institucionales.

2.3 ESQUEMA DE CLASIFICACIÓN DE DATOS

No se tiene establecido un esquema para la clasificación de los datos, el cual es necesario para conocer: la criticidad o seguridad, la asignación de la propiedad y custodia y los controles de seguridad apropiados para cada una de las clasificaciones de los datos que requieran protección.

Lo anterior, es contrario con la siguiente normativa:

- La norma 2.1 “Modelo de arquitectura de información” de las NTGCTI indica que la organización debe optimizar la integración, uso y estandarización de sus sistemas de información de manera que se identifique, capture y comunique, en forma completa, exacta y oportuna, sólo la información que sus procesos requieren.

- Al respecto se tiene como buena práctica de referencia la versión 4 de COBIT, que indica en su objetivo de control PO2.3 (p. 34), que se debe establecer un esquema de clasificación que aplique a toda la empresa, basado en que tan crítica y sensible es la información (esto es, pública,

confidencial, secreta) de la empresa. Este esquema incluye detalles acerca de la propiedad de datos, la definición de niveles apropiados de seguridad y de controles de protección, y una breve descripción de los requerimientos de retención y destrucción de datos, además de qué tan críticos y sensibles son. Se usa como base para aplicar control de acceso, archivo o cifrado.

- Por su lado, la versión 5 de COBIT, indica en la práctica de gestión APO01.06 (p. 55), que se debe definir la propiedad de la información (datos) y del sistema, además se deben definir y mantener las responsabilidades de la propiedad de la información (datos) y los sistemas de información y asegurar que los propietarios toman decisiones sobre la clasificación de la información y los sistemas y su protección de acuerdo con esta clasificación.

El motivo por el cual no se ha establecido un esquema para la clasificación de datos, es porque el Departamento de TI no ha considerado establecerlo, ya que tanto el Jefe de TI como el DBA consideran que les corresponde a los dueños de los sistemas o definirse en conjunto con ellos.

El no contar con un esquema de clasificación de datos podría ocasionar que se divulgue o exponga información sensible de la institución.

De acuerdo con lo identificado se recomienda a la Gerencia:

3. Instruir al Departamento de TI para que en el plazo de seis meses, y en conjunto con los dueños de los datos, establezca un esquema de clasificación de datos, el cual según COBIT 4 y 5 debe contener al menos:

    - Información sobre la criticidad o seguridad de la información,
    - Asignación de la propiedad y custodia de los datos;
    - Controles de seguridad apropiados para cada una de las clasificaciones de datos que requieran protección.

2.4 SERVICIO DE ESCUCHA (LISTENER)

El servicio de escucha (listener) de Oracle no está protegido con una contraseña y el puerto asignado es el 1522 el cual no proporciona una seguridad adicional a las bases datos.

Al respecto, como mejor práctica "Oracle Database Security Checklist[14]" recomienda el establecimiento de una contraseña al servicio de escucha (listener) así como el cambio del puerto por defecto.

Además, también como mejor práctica el documento "White paper: Oracle Database Listener Security Guide[15]" (p.20) emitido por Integrigy Corporation, recomienda indica que con el fin de ayudar a detener los ataques automatizados y la detección del listener en las redes, el NTS por defecto debe cambiarse de 1521 a un puerto fuera de los rangos 1521-1550 y 1600-1699, con el fin de proporcionar seguridad adicional.

La causa por la cual el servicio de escucha (listener) no está protegido con una contraseña y no se ha cambiado el puerto, es porque el Departamento de TI no los ha considerado dentro de sus controles de seguridad. Al respecto, el DBA indicó que no tiene contraseña porque solo él tiene acceso al mismo.

Sin embargo, el control indicado por el DBA no garantiza que el servicio de escucha pueda ser utilizado por terceros que impida corromper la base de datos institucionales.

Al no contar el "listener" con una contraseña y un puerto adecuado de seguridad, el ICT podría exponerse a posibles ataques de sus bases de datos por servicios de escucha de terceros, lo que podría afectar la disponibilidad y seguridad de la información institucional.

De acuerdo con el resultado obtenido se recomienda a la Gerencia:

4. Instruir al Departamento de TI para que en un plazo de un mes, implemente las medidas necesarias para la protección del "listener" con el fin de proteger y prevenir ataques a las bases de datos Institucionales y que analice la posibilidad de cambiar el puerto 1522 a otro fuera de los rangos 1521-1550 y 1600-1699.

[14] http://docs.oracle.com/cd/B19306_01/network.102/b14266/checklis.htm#i1009371
[15] https://www.integrigy.com/files/Integrigy_Oracle_Listener_TNS_Security.pdf

2.5 PLAN DE RESPALDO

El Departamento de TI no cuenta con un plan de respaldo (backup) ante la ausencia de colaboradores que realicen funciones críticas, con el objetivo de reducir la dependencia hacia dichos funcionarios.

Al respecto, la versión 5.0 de COBIT en la práctica de gestión APO07.2 (p. 85) indica que se debe identificar el personal clave de TI, con el fin de reducir al mínimo la dependencia de una sola persona en la realización de una función critica de trabajo mediante la captura de conocimiento (documentación), el intercambio de conocimientos, la planificación de la sucesión y el respaldo (backup) del personal.

Según el jefe del Departamento de TI, no ha establecido un plan para reducir la dependencia de personal clave porque no cuenta con los recursos necesarios.

No obstante la justificación externada por el Jefe, es de vital importancia que TI cuente con un plan para disminuir la dependencia del personal clave, pues cada día el Instituto depende más del uso de las TI y de los servicios que presta el Departamento de TI.

Al no contar del Departamento de TI con un plan de respaldo para el personal clave podría ocasionar a la Institución que:

- Se cree dependencia del talento humano con conocimiento técnico y experiencia necesarias para realizar las funciones de críticas en TI.
- No se pueda sustituir al personal clave en caso de una eventualidad que podría afectar la continuidad del negocio.
- No se cuente con personal idóneo para realizar las funciones críticas de TI.

De acuerdo con lo identificado se recomienda a la Gerencia:

5. Instruir al Departamento de TI para que en un plazo de tres meses, proceda a implementar un plan de respaldo del personal que realiza funciones críticas, con la finalidad de minimizar la dependencia de la Institución hacia funcionarios que podrían afectar la continuidad del servicio que debe brindar.

Las anteriores recomendaciones se emiten al amparo del artículo 35 de la Ley Orgánica del Instituto y a la competencia que facultan los artículos 22, 35 y 36 de la Ley General de Control Interno.

3. CONCLUSIÓN

Con el avance tecnológico, se ha incrementado el riesgo de que la integridad y la confidencialidad de la información se vea afectada por intrusiones de terceros, de ahí la necesidad de establecer controles y mecanismos de seguimiento en las bases de datos institucionales.

El estudio determinó algunas situaciones susceptibles de mejora tales como:

- Herramientas de auditoría en las bases de datos
- Gestión de las actualizaciones de las Bases de Datos
- Esquema de clasificación de datos
- Servicio de escucha (listener)
- Personal clave de TI

Si las oportunidades de mejora identificadas en el estudio se subsanan, el Instituto tendrá una garantía razonable de que la administración de las bases de datos institucionales se realiza de acuerdo con la normativa aplicable y las mejoras prácticas de la industria.