UNIVERSIDAD DE COSTA RICA

SISTEMA DE ESTUDIOS DE POSGRADO

# CONTROL SOBRE EL PROCESO DE TI: GARANTIZAR LA SEGURIDAD DE LOS SISTEMAS

Trabajo final de investigación aplicada, sometido a la consideración de la Comisión del Programa de Estudios de Posgrado en Administración y Dirección de Empresas, para optar al grado y título de Maestría Profesional en Auditoría de Tecnologías de la Información.

MAGALY FERNÁNDEZ MARÍN

Ciudad Universitaria Rodrigo Facio, Costa Rica

2013

**Dedicatoria**

*A mis padres, hermanos, y amigos.*

**Agradecimientos**

***A Dios,*** *por permitirme llegar hasta este punto y haberme dado salud para concluir de manera satisfactoria.*

***A mis familiares,*** *por la comprensión, el tiempo y el apoyo que me han dado a lo largo de este proceso.*

***A las lectoras de la práctica profesional,*** *por su retroalimentación, consejos, interés, disponibilidad y en general por su excelente disposición para guiarme en esta etapa final.*

***A los profesores,*** *por todas sus enseñanzas, por todo lo que me aportaron como persona y como profesional.*

***A mis compañeros,*** *por su apoyo, ayuda y buena disposición en compartir sus conocimientos, así como por su amistad y los momentos agradables que compartimos en estos años.*

Este trabajo final de investigación aplicada fue aceptado por la Comisión del Programa de Estudios de Posgrado en Administración y Dirección de Empresas de la Universidad de Costa Rica, como requisito parcial para optar al grado y título de Maestría Profesional en Auditoría de Tecnologías de la Información.

_____

Doctor Aníbal Barquero Chacón

Director Programa de Posgrado en Administración y Dirección de Empresas

_____

Doctor Sergio Espinoza Guido

Profesor Guía

_____

Máster Ana Patricia Porras Solano

Lectora académica

Máster Alina Castro Hernández

Lectora empresarial

Magaly Fernández Marín

Sustentante

# Contenido

## Resumen

El objetivo principal de esta práctica profesional fue evaluar el proceso denominado “Garantizar la Seguridad de los Sistemas”, de acuerdo con la normativa correspondiente a la institución donde fue aplicado, con el fin de emitir un criterio, dirigido a la administración, sobre el nivel de madurez alcanzado en este proceso”. Por motivo de confidencialidad, se ha protegido el nombre real de la institución y se hace referencia a ella como “CDA”.

“CDA” es una institución supervisada por la Superintendencia General de Entidades Financieras (SUGEF), dedicada al negocio de las finanzas, con acceso a información confidencial de alrededor de 100.000 accionistas y de los movimientos económicos que estos realizan en su entidad. Por lo tanto, resulta de vital importancia una gestión apropiada de la seguridad de la información, que considere los elementos de un sistema integral de seguridad, como lo son los procesos, las personas y la tecnología, así como los principios de seguridad y una gestión efectiva de los riesgos, que eventualmente podrían comprometer la confidencialidad, integridad y disponibilidad de la información.

El contenido capitular consta de cuatro capítulos, que abarcan la introducción al tema propuesto, seguido de un diagnóstico de la situación actual; posteriormente se realiza un análisis de los resultados obtenidos, como producto de la evaluación, y finalmente se detallan las conclusiones y recomendaciones a la institución.

## Lista de figuras

## Lista de abreviaturas

| | |
|---|---|
| **TI** | Tecnología de Información. |
| **ISACA** | International Systems Audit and Control Association. |
| **COBIT** | Control Objectives for Information and Related Technologies. |
| **ISO** | International Organization for Standarization / International Electrotechnical Commission. |
| **ITIL** | Information Technology Infrastructure Library. |
| **SUGEF** | Superintendencia General de Entidades Financieras. |
| **CISM** | Certified Information Security Manager. |
| **UCR** | Universidad de Costa Rica. |
| **COEN** | Conocimiento del entorno. |

# CAPÍTULO I

## 1.1 Introducción

### 1.1.1 Delimitación del tema y organización

#### a) Delimitación del tema

El estudio denominado "***Control sobre el proceso de TI: Garantizar la seguridad de los sistemas***" se realizó en las oficinas centrales de una institución financiera, en adelante denominada "CDA", ubicada en San José, avenidas Central y Segunda, calle 13.

#### b) Organización

CDA es una institución privada que administra fondos públicos y fue creada por la Ley N° 12, del 13 de octubre de 1944, con la finalidad de, entre otras cosas, mejorar la calidad de vida de sus accionistas, quienes podrían ser:

- Empleados de la institución.
- Empleados del Ministerio de Educación Pública.
- Jubilados o pensionados de ese Ministerio.

Entre los servicios que ofrece, se encuentran los siguientes:

- Préstamos personales.
- Préstamos de vivienda.
- Préstamos de desarrollo.
- Tarjetas de crédito y de débito.
- Asistencias.

- Planes de ahorro.
- Comercializadora de Seguros.

Actualmente, la institución ofrece estos servicios a sus accionistas desde sus oficinas centrales, o bien desde las oficinas desconcentradas que se ubican en Liberia, Santa Cruz, San Carlos, Limón, Pérez Zeledón, Ciudad Neily, Puntarenas y Cartago.

La institución cumplió 68 años de ser dirigida por educadores: su Junta Directiva está conformada por cinco propietarios y tres suplentes, que se eligen cada cuatro años y representan a diferentes instituciones gremiales del sector de la educación.

Asimismo, es administrada por un Gerente y un Subgerente, quienes son nombrados por la Junta Directiva, cada dos años.

**Misión:**

Somos una institución financiera con sentido social y solidario, que administra eficientemente los recursos y brinda servicios de excelencia, con el fin de contribuir al mejoramiento de la calidad de vida de nuestros accionistas.

**Visión:**

Ser la mejor alternativa en servicios financieros para nuestros accionistas.

**Valores:**

- Solidaridad.
- Confiabilidad.
- Innovación.

- Excelencia.
- Respeto.
- Lealtad.

### 1.1.2 Justificación

CDA es una institución dedicada al negocio de las finanzas, con acceso a información confidencial de alrededor de 100.000 accionistas y de los movimientos económicos que estos realizan en su entidad. Por tal motivo, resulta de vital importancia una gestión apropiada, de la seguridad de la información, que considere los elementos de un sistema integral de seguridad, como lo son los procesos, las personas y la tecnología, así como los principios de seguridad y una gestión efectiva de los riesgos, que eventualmente podrían comprometer la confidencialidad, tanto de la integridad como de la disponibilidad de la información, y al mismo tiempo, resulta relevante que la institución asegure, el cumplimiento de las regulaciones que le aplican.

De acuerdo con todo lo anterior, la Jefatura del Departamento de Informática y la Oficina de Seguridad Informática manifestaron, un interés especial en que la presente práctica profesional, se enfocara en la evaluación del nivel de madurez del proceso COBIT® DS5 “Garantizar la Seguridad de los Sistemas”, el cual debe alcanzar un nivel de madurez 3 “Definido” y formar parte de los primeros 17 procesos, que deben implementar las instituciones supervisadas por la Superintendencia General de Entidades Financieras, según las disposiciones emitidas por medio del acuerdo SUGEF 14-09.

La finalidad de esta práctica profesional es, entonces, entre otras cosas, emitir un criterio dirigido a la administración, sobre el nivel de madurez alcanzado, así como las brechas identificadas, además de las recomendaciones y oportunidades de mejora, para garantizar de manera razonable la confidencialidad, integridad y disponibilidad, de la información de sus accionistas.

### 1.1.3 Ubicación del tema en el contexto

La Superintendencia General de Entidades Financieras (en adelante SUGEF) es un ente supervisor y fiscalizador de las operaciones de las entidades financieras costarricenses, a saber: bancos del Estado, bancos privados, empresas financieras no bancarias, cooperativas de ahorro y préstamo, conglomerados y grupos financieros, grupos financieros inscritos en SUGESE-SUGEVAL, y otras entidades financieras.

Con el fin de cumplir esas labores de fiscalización y supervisión, la SUGEF ha sido facultada para emitir normas que contribuyan con el ejercicio de sanas prácticas bancarias; de esta manera, se asegura el cumplimiento de su misión, la cual es ser "…una organización supervisora que vela por la solidez y estabilidad del sistema financiero costarricense."

En el sector financiero de Costa Rica, las entidades supervisadas por la SUGEF deben acatar las disposiciones del acuerdo denominado "Reglamento sobre la Gestión de la Tecnología de Información" emitido en el año 2009. Entre otros aspectos, dicho reglamento indica que todas las entidades supervisadas deben desarrollar, implementar y mantener un marco para la gestión de TI, que incluya entre otros, el proceso COBIT®

DS5: “Garantizar la Seguridad de los Sistemas” y deberá alcanzar un nivel de madurez 3 “Definido”.

En razón de lo anterior, CDA estableció en el año 2009, un proyecto denominado “Proyecto de implementación del Acuerdo SUGEF 1409” cuyo alcance comprende la implementación de 19 procesos COBIT, en cumplimiento de las disposiciones del ente supervisor. Al inicio de esta evaluación, dicho proyecto se encontraba en su etapa final, con un porcentaje de avance del 98%.

### 1.1.4 Intereses profesionales

- Aplicar los conocimientos adquiridos a lo largo de la maestría en Auditorías de Tecnologías de Información.
- Adquirir experiencia en el ámbito de auditoría de TI.
- Complementar los conocimientos transmitidos, por parte de los diferentes profesores de la maestría, con la guía del profesor del curso, así como de la lectora académica.
- Desarrollar una metodología de trabajo, además de las herramientas necesarias, que puedan aplicarse para futuras evaluaciones.
- Adquirir mayor conocimiento sobre la gestión de seguridad de la información y de las buenas prácticas relacionadas.

### 1.1.5 Aporte

Brindar a la institución, un criterio sobre el nivel de madurez alcanzado, así como las brechas identificadas, las recomendaciones y oportunidades de mejora, para garantizar de manera razonable la confidencialidad, integridad y disponibilidad de la información de sus accionistas.

### 1.1.6 Objetivos

**Objetivo general:**

Evaluar el proceso "Garantizar la Seguridad de los Sistemas", de acuerdo con la normativa aplicable a la institución, con el fin de emitir un criterio, dirigido a la administración, sobre el nivel de madurez alcanzado en este proceso.

**Objetivos específicos:**

1. Indagar con los dueños de proceso correspondientes, sobre las acciones que ha emprendido la institución, como parte de la implementación del proceso "Garantizar la Seguridad de los Sistemas", con el fin de obtener un conocimiento de la situación actual y de los esfuerzos realizados, como parte de la implementación del proceso en estudio.
2. Fundamentar, por medio de criterio de expertos, mejores prácticas y el nivel de madurez para este proceso, de acuerdo con el COBIT®, lo que se espera encontrar por parte de la institución, con el fin de obtener una base, sobre la cual emitir los criterios correspondientes.

3. Determinar el grado de madurez en el que se encuentra el proceso “Garantizar la Seguridad de los Sistemas”, con el fin de que las brechas identificadas se comuniquen a la administración y se asegure, de manera razonable, la confidencialidad, integridad y disponibilidad de la información de sus accionistas.

### 1.1.7 Alcance

Evaluar el nivel de madurez del proceso “Garantizar la Seguridad de los Sistemas”, implementado en la institución, en el periodo comprendido entre setiembre 2012 y abril 2013, con base en el nivel de madurez de este proceso, propuesto en los Objetivos de Control para la Información y Tecnología Relacionada COBIT® 4.0, en cumplimiento del acuerdo SUGEF 1409.

### 1.1.8 Limitaciones

En relación con la confidencialidad de la información, de lo correspondiente a los resultados de análisis de vulnerabilidades, análisis de riesgos y algunos otros documentos considerados como sensibles, por la institución, se indicó expresamente que dicha confidencialidad debe mantenerse; por lo tanto, el acceso a la documentación se limitará a revisiones en el sitio. Asimismo, no es posible la aplicación de herramientas tecnológicas para la elaboración de pruebas de seguridad.

Por otra parte, siempre en relación con el tema de la confidencialidad, para efectos de la elaboración de este documento, se ha protegido el nombre real de la institución, de ahí que se haga referencia a ella únicamente como “CDA”.

## 1.2 Contenido capitulario

El ordenamiento lógico de los capítulos bajo el cual está organizado el presente trabajo se detalla a continuación:

Capítulo I: El capítulo I incluye el tema propuesto, la introducción, la ubicación del tema en el contexto, el objetivo general y los específicos, alcances, limitaciones, los instrumentos, procedimientos y herramientas por utilizar, así como el cronograma de actividades.

Capítulo II: En el capítulo II se detalla el resultado de un diagnóstico, de la situación actual del tema propuesto.

Capítulo III: En el capítulo III se realiza un análisis de los resultados obtenidos, posterior a la evaluación del tema propuesto.

Capítulo IV: En el capítulo IV se detallan las conclusiones y recomendaciones, con base en los resultados que se desprendieron de la evaluación realizada.

Anexos: Se adjuntan los anexos del trabajo.

## 1.3 Operacionalidad de las variables

La operacionalidad de las variables aplica para los estudios con enfoques cuantitativos, por lo que en este caso no aplica la declaración de estas.

Como aspectos teóricos globales, ligados con el tema en estudio, se presenta a continuación la tabla N°1, con el detalle de los niveles de madurez, propuestos en el marco de control COBIT® 4.0:

**Tabla 1: Niveles de madurez Proceso DS5 "Garantizar la Seguridad de los Sistemas"**

| Nivel | Descripción |
|---|---|
| **0**<br>**No existente** | La organización no reconoce la necesidad de la seguridad para TI. Las responsabilidades y la rendición de cuentas no están asignadas para garantizar la seguridad. Las medidas para soportar y administrar la seguridad de TI no están implementadas. No hay reportes de seguridad de TI, ni un proceso de respuesta para resolver brechas de seguridad de TI. Hay una total falta de procesos reconocibles de administración de seguridad de sistemas |
| **1**<br>**Inicial** | La organización reconoce la necesidad de seguridad para TI. La conciencia de la necesidad de seguridad depende principalmente del individuo. La seguridad de TI se lleva a cabo de forma reactiva. No se mide la seguridad de TI. Las brechas de seguridad de TI ocasionan respuestas con acusaciones personales, debido a que las responsabilidades no son claras. Las respuestas a las brechas de seguridad de TI son impredecibles |
| **2**<br>**Repetible** | Las responsabilidades, y la rendición de cuentas sobre la seguridad, están asignadas a un coordinador de seguridad de TI, pero la autoridad gerencial del coordinador es limitada. La conciencia sobre la necesidad de |

| Nivel | Descripción |
|---|---|
| | la seguridad está fraccionada y limitada. Aunque los sistemas producen información relevante respecto a la seguridad, esta no se analiza. Los servicios de terceros pueden no cumplir con los requerimientos específicos de seguridad de la empresa. Las políticas de seguridad se han estado desarrollando, pero las herramientas y las habilidades son inadecuadas. Los reportes de la seguridad de TI son incompletos, engañosos o no aplicables. La capacitación sobre seguridad está disponible, pero depende principalmente de la iniciativa del individuo. La seguridad de TI es vista primordialmente como responsabilidad y disciplina de TI, y el negocio no ve la seguridad de TI como parte de su propia disciplina. |
| **3**<br>**Definido** | Existe conciencia sobre la seguridad y esta es promovida por la gerencia. Los procedimientos de seguridad de TI están definidos y alineados con la política de seguridad de TI. Las responsabilidades de la seguridad de TI están asignadas y entendidas, pero no continuamente implementadas. Existen un plan de seguridad de TI y soluciones de seguridad motivadas por un análisis de riesgo. Los reportes no contienen un enfoque claro de negocio. Se realizan pruebas de seguridad adecuadas (por ejemplo, pruebas contra intrusos). Existe capacitación en seguridad para TI y para el negocio, pero se programa y se comunica de manera informal. |
| **4**<br>**Administrado** | Las responsabilidades sobre la seguridad de TI son asignadas, administradas e implementadas de forma clara. Regularmente se lleva a |

| Nivel | Descripción |
|---|---|
| | cabo un análisis de impacto y de riesgos de seguridad. Las políticas y prácticas de seguridad se complementan con referencias de seguridad específicas. El contacto con métodos para promover la conciencia de la seguridad es obligatorio. La identificación, autenticación y autorización de los usuarios está estandarizada. La certificación en seguridad es buscada por parte del personal, que es responsable de la auditoría y la administración de la seguridad. Las pruebas de seguridad se hacen utilizando procesos estándares y formales, que llevan a mejorar los niveles de seguridad. Los procesos de seguridad de TI están coordinados con la función de seguridad de toda la organización. Los reportes de seguridad están ligados con los objetivos del negocio. La capacitación sobre seguridad se imparte tanto para TI como para el negocio. La capacitación sobre seguridad de TI se planea y se administra, de manera que responda a las necesidades del negocio y a los perfiles de riesgo de seguridad. Los KGI y KPI ya están definidos, pero no se miden aún. |
| **5**<br>**Optimizado** | La seguridad en TI es una responsabilidad conjunta del negocio y de la gerencia de TI y está integrada con los objetivos de seguridad del negocio en la corporación. Los requerimientos de seguridad de TI están definidos de forma clara, optimizados e incluidos en un plan de seguridad aprobado. Los usuarios y los clientes se responsabilizan, cada vez más, de definir requerimientos de seguridad, y las funciones de seguridad están integradas, con las aplicaciones en la fase de diseño. Los incidentes de |

| Nivel | Descripción |
|---|---|
| | seguridad son atendidos de forma inmediata, con procedimientos formales de respuesta, soportados por herramientas automatizadas. Se llevan a cabo valoraciones de seguridad de forma periódica, para evaluar la efectividad de la implementación del plan de seguridad. La información sobre amenazas y vulnerabilidades se recolecta y analiza, de manera sistemática. Se recolectan e implementan, de forma oportuna, controles adecuados para mitigar riesgos. Se llevan a cabo pruebas de seguridad, análisis de causa-efecto e identificación pro-activa de riesgos, para la mejora continua de procesos. Los procesos de seguridad y la tecnología están integrados a lo largo de toda la organización. Los KGI y KPI para administración de seguridad, son recopilados y comunicados. La gerencia utiliza los KGI y KPI para ajustar el plan de seguridad, en un proceso de mejora continua. |

**Fuente: COBIT 4.0**

## 1.4 Metodología

### 1.4.1 Pasos para la aplicación de la planificación y el programa de auditoría

Se aplicó el proceso tradicional de auditoría, que incluye las siguientes etapas:


**Planificación del trabajo**: La planificación consiste en las siguientes actividades:

- Posterior a la aprobación del enfoque de la práctica profesional, se continuó con la documentación de la hoja de asignación del trabajo que incluye el nombre del estudio, objetivo general, objetivos especificados, alcance y criterios por utilizar.
- Obtención de conocimiento de la situación actual del proceso y del entorno, por medio de entrevistas, recopilación y revisión de información relevante.
- Documentación del plan general de estudio, que se basa en el conocimiento del proceso por auditar e incluye (entre otros aspectos) la naturaleza del proceso, la normativa del área, evaluación del control interno, estudios anteriores de auditoría, principales funcionarios del área auditada y herramientas de auditoría por utilizar, para el desarrollo del estudio.
- Elaboración de informe de planificación.
- Confección de programas de trabajo, que indiquen las actividades que se deben realizar en la siguiente etapa.

**Ejecución:** En la etapa de ejecución se aplicaron las pruebas de cumplimiento a las personas entrevistadas, o bien las pruebas sustantivas, y se obtiene la evidencia que respalda los resultados.

**Comunicación:** Posterior al análisis de los resultados obtenidos se elaboró y comunicó el informe a la administración. Dicho informe incluye conclusiones y recomendaciones.

CAPÍTULO II

## 2.1 Situación actual

El propósito de este capítulo es, presentar la situación actual del tema propuesto desde un enfoque global, posteriormente la situación correspondiente a Costa Rica, seguido por la situación en las entidades financieras costarricenses y por último, en la institución en la cual se está desarrollando la práctica profesional, con el fin de que el lector no solo se entere de las tendencias en relación con el tema, sino de la importancia relativa que adquiere, cuando hay que competir sin barreras, en un mundo cada vez más globalizado, principalmente por la influencia de las tecnologías de información.

### 2.1.1 Situación actual en el mundo

Las áreas de tecnología de información en general, requieren de estrategias para responder a los diferentes retos a los cuales se enfrentan, entre ellos:

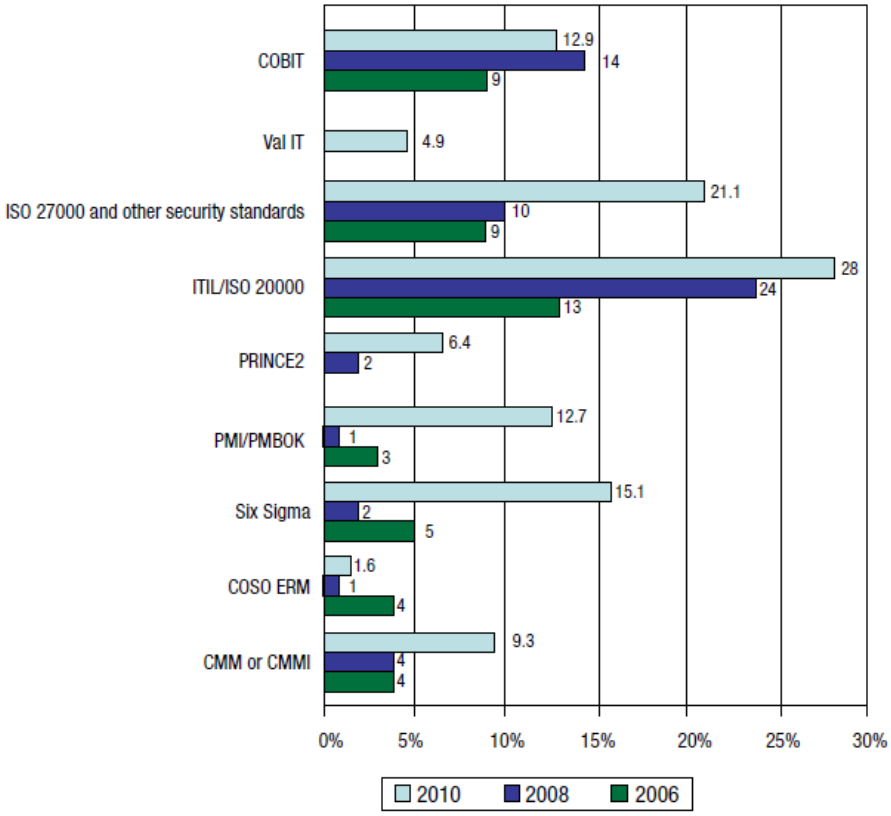
- Mantener TI en marcha.
- Optimizar costos.
- Asegurar el cumplimiento regulatorio.
- Administrar la complejidad.
- Entregar valor.
- Alinear TI con el negocio.
- Proveer de seguridad.

Las empresas necesitan de gobierno de tecnología de información, para responder a los diferentes retos que enfrentan, a través de sus recursos y activos de tecnología, por medio de la alineación con los objetivos de negocio, la administración de los recursos y riesgos, la entrega de valor, las mediciones de desempeño y el cumplimiento de leyes o regulaciones, entre otros.

Acerca de la situación global del gobierno de TI, existen diferentes estudios realizados por entidades como ISACA (Information Systems Audit and Control Association), que buscan establecer las tendencias de la tecnología mundial y de su gestión; por tanto, se citan a continuación algunos de los resultados obtenidos y publicados en el documento denominado "*Global Status Report on the Governance of Enterprise It (Geit)—2011*".

La encuesta revela que en la mayoría de los casos, los marcos de control están aumentando en el nivel de utilización dentro de las instituciones; sin embargo, en el caso del marco de control COBIT, se puede apreciar que del 2008 al 2010, se da una disminución. *(Ver figura Nº1)*

**Figura No.1 Uso de Estándares y Marcos de Control**




**Fuente: Global Status Report on the Governance of Enterprise It (Geit)—2011.**

No obstante lo anterior, se puede visualizar que hay una tendencia de aumento en el uso de marcos de control en general y adicionalmente, se puede apreciar que la serie de normas ISO 27000 (estándares de seguridad de la información) presentó un gran aumento en el 2011, con respecto a los dos años anteriores.

### 2.1.2 Situación actual en Costa Rica

Las empresas, tanto del sector privado como público, han sentido la necesidad de responder a los retos descritos con anterioridad, basándose en las áreas de enfoque del gobierno corporativo, de tecnología de información, como la mejor práctica. Para el caso

particular del ámbito gubernamental, la Contraloría General de la República establece, que todas las instituciones con uso de fondos públicos, tengan como propósito gestionar su marco de control de tecnología de información y procuren una mejor gestión de las tecnologías, mediante la promulgación de las denominadas "Normas técnicas para la gestión y el control de las tecnologías de información" (N-2-2007-CO-DFOE), dentro de las cuales se incluye el apartado "Planificación y Organización" donde se observan los siguientes objetivos:

- La organización debe lograr que las TI apoyen su misión, visión y objetivos estratégicos mediante procesos de planificación, que logren el balance óptimo entre sus requerimientos, su capacidad presupuestaria y las oportunidades que brindan las tecnologías existentes y emergentes. (2.1)
- La organización debe generar los productos y servicios de TI, de conformidad con los requerimientos de sus usuarios, con base en un enfoque de eficiencia y mejoramiento continuo. (1.2)
- La organización debe responder adecuadamente a las amenazas que puedan afectar la gestión de las TI, mediante una gestión continua de riesgos que esté integrada al sistema específico de valoración del riesgo institucional y considere el marco normativo que le resulte aplicable. (1.3)
- La organización debe optimizar el uso de los recursos financieros invertidos en la gestión de TI, procurando el logro de los objetivos de esa inversión, controlando en forma efectiva dichos recursos y observando el marco jurídico que al efecto le resulte aplicable. (2.5)

- La organización debe asegurar el logro de los objetivos propuestos como parte de la gestión de TI, para lo cual debe establecer un marco de referencia y un proceso de seguimiento en los que defina el alcance, la metodología y los mecanismos para vigilar la gestión de TI. Asimismo, debe determinar las responsabilidades del personal a cargo de dicho proceso. (5.1)

No obstante lo anterior, dichas normas no imponen a las entidades fiscalizadas la adopción de un marco de referencia específico; sin embargo, observando su contenido, se nota que guarda una estructura similar a la de los dominios de COBIT, que se pueden comparar de la siguiente manera:

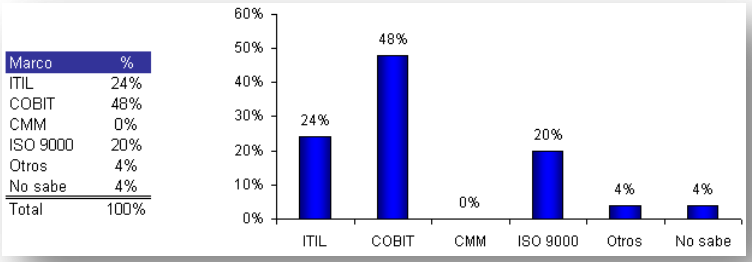
**Figura No.2 Comparación Normas CGR vs COBIT**

| Capítulo Normas Técnicas (N-2-2007-CO-DFOE) | Dominio COBIT homólogo |
|---|---|
| Capítulo II Planificación y organización. | Planear y organizar (PO). |
| Capítulo III Implementación de tecnologías de información. | Adquirir e implementar (AI). |
| Capítulo IV Prestación de servicios y mantenimiento. | Entregar y dar soporte (DS). |
| Capítulo V Seguimiento. | Monitorear y evaluar (ME). |

**Fuente: Normas CGR y COBIT.**

Un estudio realizado en el 2006, aplicado en diferentes entidades financieras costarricenses, ante la pregunta ¿Cuál marco de referencia se está utilizando para estandarizar las operaciones de TI?, reveló los siguientes datos:

**Figura No.3 Uso de marcos de referencia en entidades financieras costarricenses. 2006.**




**Fuente: Tesina Ing. Magaly Fernández Marín.**

Como se puede observar en la figura 3, hace siete años, muchas entidades financieras costarricenses, tanto públicas como privadas, vieron la necesidad de adoptar un marco de referencia que les permitiera gestionar la tecnología de información, con el fin de entregar los servicios de TI de manera eficaz y eficiente; para estos efectos, un poco menos de la mitad (48%) de los encuestados indicó que el marco adoptado era COBIT, seguido por el marco de buenas prácticas para la gestión de servicios de tecnologías de la información: ITIL (Information Technology Infraestructure Library) con el 24%.

Es importante destacar, que muchas empresas acostumbran utilizar un marco conjuntamente con otros estándares y mejores prácticas internacionales, como ITIL e ISO 27000, por lo que se puede inferir, que en Costa Rica, el marco actualmente más utilizado es COBIT. Sin embargo, algunos de sus procesos están siendo implementados a partir de otros marcos de referencia específicos, por ejemplo ITIL para los procesos relacionados con la entrega del servicio e ISO 27000 en lo relacionado con la seguridad de la información.

Lo indicado anteriormente se ha fortalecido en razón de las disposiciones emitidas por la Superintendencia General de Entidades Financieras mediante el acuerdo SUGEF 1409, Artículo 5 y 6 del Capítulo 2, donde se establece que la gestión de tecnología de información debe orientarse al logro de las cinco áreas de enfoque del Gobierno de TI, mediante la implementación de los procesos COBIT en su versión 4.0 como se profundizará en la sección 2.1.3

### 2.1.3 Situación actual en entidades financieras

Como se mencionó en el capítulo I, la SUGEF es un ente supervisor de las operaciones de las entidades financieras costarricenses y con el fin de cumplir esas labores de supervisión, ha sido facultada para emitir normas, que contribuyan con el ejercicio de sanas prácticas bancarias.

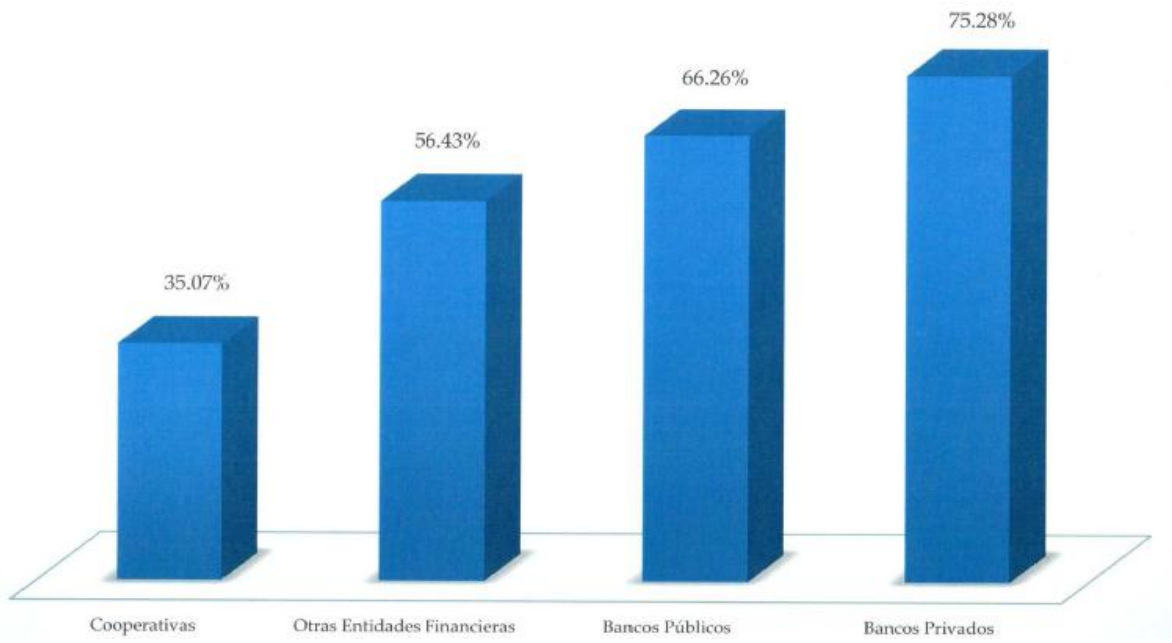
Al respecto, en el año 2009, la SUGEF emitió el "Reglamento sobre la Gestión de la Tecnología de Información" el cual derogó la "Normativa de Tecnología de Información para las entidades fiscalizadas por la Superintendencia General de Entidades Financieras" vigente hasta ese momento desde el año 2002.

El acuerdo SUGEF 1409 establece, que todas las entidades supervisadas deben desarrollar, implementar y mantener un marco para la gestión de tecnología de información, que se oriente al cumplimiento de las cinco áreas de enfoque del Gobierno de TI, a saber: Alineación Estratégica, Administración del Riesgo de TI, Entrega de Valor, Gestión de Recursos y Medición del Desempeño de TI y que incluya inicialmente la

implementación de 17 procesos, entre ellos, el proceso DS5 “Garantizar la Seguridad de los Sistemas” con un nivel de madurez mínimo de 3 “Definido”.

La Cámara de Bancos e Instituciones Financieras de Costa Rica y la Academia Bancaria, en el mes de julio del 2012, presentaron el estudio denominado “Resultados del primer ciclo de auditoría sobre la gestión de TI del Acuerdo SUGEF 1409” del cual se desprenden los siguientes resultados:

**Figura No.4 Resultado de la Auditoría Externa de TI por sector (Diciembre 2011).**




**Fuente: Resultados del primer ciclo de auditoría sobre la gestión de TI del Acuerdo SUGEF 1409 y Acuerdo SUGEF 14-09. Cámara de Bancos e Instituciones Financieras de Costa Rica y la Academia Bancaria**

Como se puede observar, los bancos privados obtuvieron una mejor calificación con respecto a los bancos públicos, cooperativas y otras entidades financieras, ubicándose de manera general, de acuerdo con el Reglamento SUGEF 1409 de la siguiente manera:

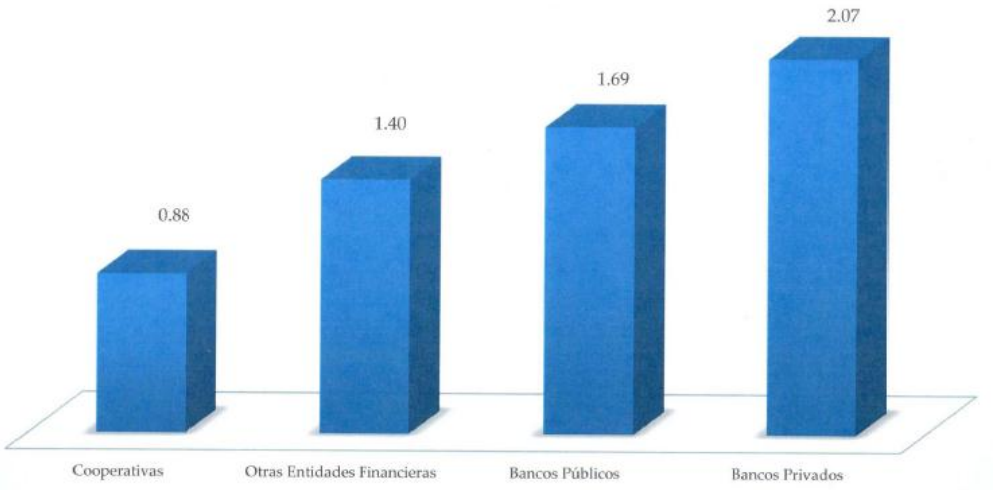
**Tabla 2: Calificación y nivel de acuerdo con calificación obtenida y calificación sobre la gestión de TI**

| Entidad | Calificación | Nivel |
|---|---|---|
| **Bancos Privados.** | Mayor o igual que 70% y menor que 85%. | Irregularidad 1. |
| **Bancos Públicos.** | Mayor o igual que 55% y menor que 70%. | Irregularidad 2. |
| **Otras entidades financieras.** | Mayor o igual que 55% y menor que 70%. | Irregularidad 2. |
| **Cooperativas.** | Menor que 55%. | Irregularidad 3. |

**Fuente: Elaboración propia con base en los resultados del primer ciclo de auditoría sobre la gestión de TI del Acuerdo SUGEF 1409 y Acuerdo SUGEF 14-09**

Los bancos públicos, cooperativas y otras entidades financieras presentan una brecha mayor, con respecto al cumplimiento del Acuerdo SUGEF 1409.

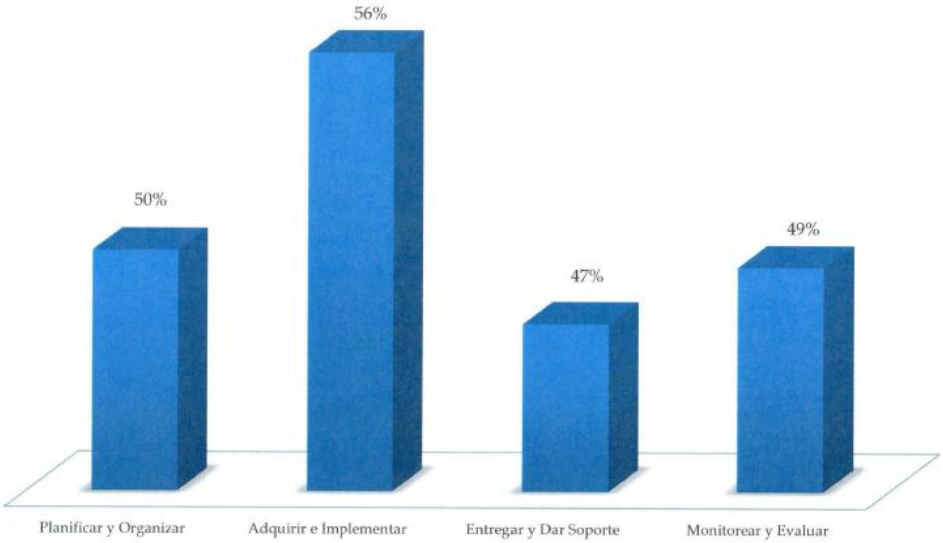
**Figura No.5 Nivel de madurez por sector (Diciembre 2011)**




**Fuente: Resultados del primer ciclo de auditoría sobre la gestión de TI del Acuerdo SUGEF 1409 y Acuerdo SUGEF 14-09. Cámara de Bancos e Instituciones Financieras de Costa Rica y la Academia Bancaria**

El nivel de madurez promedio alcanzado por los bancos privados fue de 2 “Repetible”, de 1 “Inicial” en otras entidades financieras e inexistente en las cooperativas.

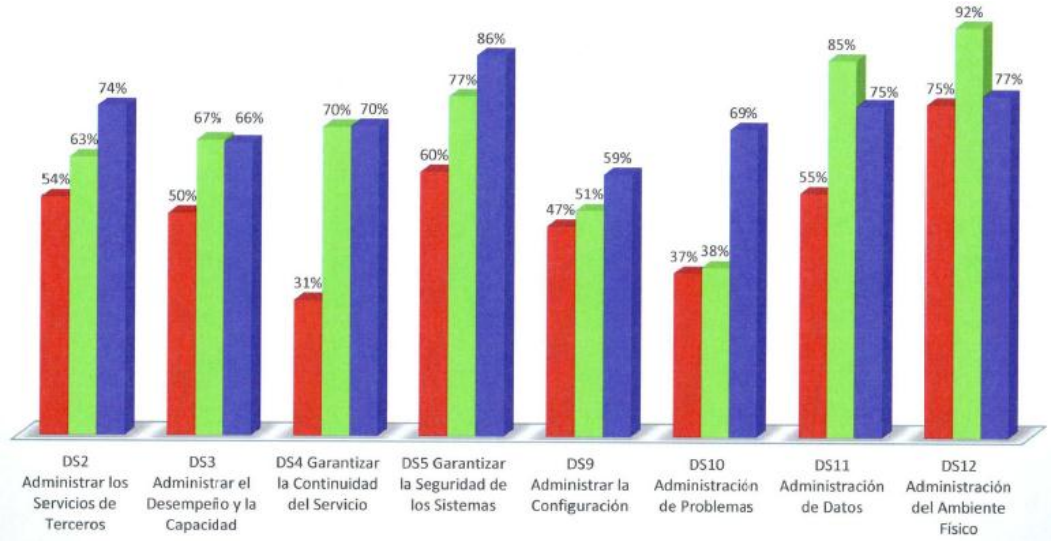
**Figura No.6 Calificación por Dominio COBIT (Diciembre 2011)**




**Fuente: Resultados del primer ciclo de auditoría sobre la gestión de TI del Acuerdo SUGEF 1409 y Acuerdo SUGEF 14-09. Cámara de Bancos e Instituciones Financieras de Costa Rica y la Academia Bancaria**

El dominio COBIT con mayor calificación fue el de "Adquirir e Implementar" y el menor el de "Entregar y dar Soporte", dominio en el que se encuentra el proceso DS5 "Garantizar la Seguridad de los Sistemas."

**Figura No.7 Procesos del dominio "Entregar y Dar Soporte" por sector (Diciembre 2011)**



**Fuente: Resultados del primer ciclo de auditoría sobre la gestión de TI del Acuerdo SUGEF 1409 y Acuerdo SUGEF 14-09. Cámara de Bancos e Instituciones Financieras de Costa Rica y la Academia Bancaria**

Finalmente, en cuanto al proceso DS5 "Garantizar la Seguridad de los Sistemas" se puede observar que la tendencia se mantiene, es decir, los bancos privados obtuvieron mayor calificación (con el 86%), seguido de los bancos públicos (77%) y otras entidades financieras (60%).

### 2.1.4 Situación actual en la institución CDA

#### a) Proyecto de implementación del Acuerdo SUGEF 1409

CDA estableció en el año 2009, un proyecto denominado "Proyecto de implementación del Acuerdo SUGEF 1409" cuyo alcance comprendía la implementación de 19 procesos COBIT; dicho proyecto fue finalizado en octubre del 2012, de manera satisfactoria, de conformidad con el tiempo, los costos y el alcance previamente definido.

#### b) Proceso de Seguridad DS5 "Garantizar la Seguridad de los Sistemas"

El proceso DS5 "Garantizar la Seguridad de los Sistemas" obtuvo una nota de 91.46% y se ubicó en un nivel de madurez 2, de acuerdo con la última autoevaluación realizada por la institución.

La Oficina de Seguridad Informática se ha estado apoyando en la norma ISO 27001 (requisitos del sistema de gestión de seguridad de la información) para la implementación del proceso.

La realización de entrevistas y aplicación de herramientas (basadas en el nivel de madurez 3 según COBIT) para obtener un conocimiento de la situación actual, arrojaron los siguientes resultados:

- Como parte de la implementación del acuerdo SUGEF 1409 y el proceso COBIT DS5 “Garantizar la Seguridad de los Sistemas” la Junta Directiva de CDA, en sesión N° 6469 celebrada el 18 de noviembre del 2010 acordó aprobar la propuesta de implementar la Oficina de Seguridad Informática (ahora denominada Unidad de Seguridad de la Información) la cual rinde cuentas directamente a la Gerencia y está conformada por los siguientes puestos:
    - Jefe.
    - Analista de Seguridad en Redes de Datos y Comunicaciones.
    - Analista Gestor de Riesgos Informáticos.
    - Analista Seguridad de la Infraestructura y Servicios Colaborativos.
    - Analista en Seguridad de Arquitectura de Datos y Sistemas.
- La Oficina de Seguridad Informática realiza esfuerzos para concienciar a los usuarios a lo largo de la institución. No obstante, esto no incluye a los empleados de proveedores.
- Está en proceso de aprobación una normativa, relacionada con empleados de proveedores que están involucrados, de alguna manera, con la seguridad de la información de la organización.
- La gerencia reconoce la necesidad de la seguridad para tecnología de información, y participa en reuniones de comité de seguridad. La Junta Directiva aprueba suficientes recursos para la inversión en seguridad, también aprobó el Programa de

Seguridad, la creación de la Oficina de Seguridad Informática, nuevos puestos, el Comité de Seguridad y las políticas de seguridad, entre otros.

- Se ha establecido una política de seguridad y ha sido comunicada a todos los usuarios. La política se actualiza al menos una vez al año.
- Se ha establecido procedimientos relacionados con la seguridad y han sido comunicados a todos los usuarios. Se actualizan al menos una vez al año.
- Las responsabilidades de la seguridad de tecnología de información están asignadas, fueron comunicadas a los involucrados, están documentadas en las funciones de puesto y las personas a las que le fueron asignadas poseen las competencias necesarias para su desarrollo. En la definición de las responsabilidades se toman en cuenta los siguientes roles:
    - Junta Directiva.
    - Comité de Seguridad.
    - Dueños de la información.
    - Custodios de la información.
    - TI.
    - Oficina de Seguridad Informática.
    - Auditoría interna.
    - Usuarios finales.
- Existe un Plan de Seguridad formalmente aprobado, que se comunica a todos los involucrados y se actualiza al menos una vez por año.

- Se generan diversos tipos de informes, por ejemplo, informes de estudios de vulnerabilidades, informes solicitados por la Gerencia, informes de pruebas, entre otros. Se comunican los informes a los involucrados y se generan y da seguimiento a los planes de acción correspondientes, en caso de que aplique.
- Se cuenta con un cronograma para la ejecución de pruebas de seguridad y estas son comunicadas previamente a los involucrados. Con base en los resultados de las pruebas de seguridad, se establecen análisis de brechas (planes de acción). El cronograma se actualiza anualmente.
- Anualmente, cada área elabora el plan de capacitación para el siguiente año, con base en las necesidades de capacitación.

  Por otra parte, la Oficina de Seguridad Informática elaboró la política sobre capacitación de seguridad, cuyo objetivo es mantener informados a los usuarios y a las personas involucradas sobre las políticas, procedimientos y controles de seguridad, establecidos por TI.
- Como parte del Plan de Trabajo del año 2013, la Unidad de Seguridad Informática ha tomado medidas, para afinar el proceso de gestión de incidentes de seguridad.

Finalmente, se observa que, en los cuatro ambientes evaluados, el conocimiento e interés sobre la utilización de marcos de control, ha venido en aumento los últimos años, situación que llama la atención y evidencia que las instituciones han sentido la necesidad (ya sea por iniciativa propia o por leyes y regulaciones) de orientar la gestión de la tecnología de información, y de los servicios que brindan a las empresas, de acuerdo con las buenas prácticas.

Algunas entidades supervisoras en Costa Rica, como la Contraloría General de la República y la Superintendencia General de Entidades Financieras, han emitido normas con el fin de promover, en el ámbito gubernamental y financiero, la adopción de marcos de control que contribuyan con el ejercicio de sanas prácticas (esto incluye el tema objeto de estudio: seguridad de la información); sin embargo, como se pudo observar en el ámbito financiero, hay brechas importantes con respecto a lo esperado por estas entidades supervisoras, esto se puede asociar a la falta de recursos, en instituciones pequeñas, por ejemplo cooperativas, o bien, a que las entidades supervisadas perciben la adopción de estas mejores prácticas, como un aspecto meramente de cumplimiento regulatorio, y no desde el punto de vista del valor, que se puede entregar al negocio.

Como se indicó inicialmente, la adopción de marcos de control, y por consiguiente mejores prácticas en la gestión de seguridad de la información, adquiere mayor importancia cuando las instituciones tienen que competir sin barreras, en un mundo cada vez más globalizado, principalmente por la influencia de las tecnologías de información; de ahí la importancia de que las disposiciones de los distintos entes, no sean vistas únicamente con el enfoque de cumplimiento, sino de cómo estas pueden facilitar la consecución de los objetivos estratégicos de la empresa, y entregar el valor esperado.

# CAPÍTULO III

El objetivo de este capítulo es detallar los resultados obtenidos a partir del estudio denominado "***Control sobre el proceso de TI: Garantizar la seguridad de los sistemas***" realizado en las oficinas centrales de CDA.

Como parte del estudio, y posterior a una etapa de planificación, durante el mes de febrero del 2013 se coordinaron reuniones con el fin de indagar con los dueños de proceso correspondientes, sobre las acciones que ha emprendido la institución, como parte de la implementación del proceso "Garantizar la seguridad de los sistemas" con el fin de, entre otras cosas, obtener un conocimiento de los esfuerzos realizados, como parte de la implementación del proceso en estudio y determinar el grado de madurez en el que se encuentra el proceso "Garantizar la seguridad de los sistemas".

## 3.1 Sobre las herramientas utilizadas

Se consideró que, como parte de la implementación del acuerdo SUGEF 1409, la institución ha realizado una serie de actividades tendentes a implementar, entre otros, el proceso DS5 "Garantizar la seguridad de los sistemas" de acuerdo con el COBIT 4.0. En razón de lo anterior, se consideró conveniente aplicar herramientas que permitieran:

3.1.1. Evaluar el diseño de los objetivos de control del proceso DS5, con base en la guía de aseguramiento del COBIT. Los objetivos por evaluar son:

- DS5.1 Administración de la seguridad de TI.
- DS5.2 Plan de seguridad de TI.
- DS5.3 Administración de identidad.

- DS5.4 Administración de cuentas del usuario.
- DS5.5 Pruebas, vigilancia y monitoreo de la seguridad-
- DS5.6 Definición de incidente de seguridad-
- DS5.7 Protección de la tecnología de seguridad-
- DS5.8 Administración de llaves criptográficas.
- DS5.9 Prevención, detección y corrección de *software* malicioso.
- DS5.10 Seguridad de la red.
- DS5.11 Intercambio de datos sensitivos.

Se utilizó como referencia la guía de aseguramiento denominada "IT Assurance guide using COBIT" y se obtuvo una calificación para cada objetivo de control, considerando las prácticas de control y el diseño del control, tomado como referencia de la guía en mención.

3.1.2. Calificar el nivel de madurez alcanzado, de acuerdo con:

- Nivel de madurez detallado en COBIT 4.0.
- Los objetivos de control del proceso DS5 listados anteriormente.
- Anexo 2 del acuerdo SUGEF 1409 "Procedimiento para Obtener la Calificación sobre la Gestión de TI" (en este caso considerando únicamente el proceso DS5).

Los siguientes apartados detallan los resultados obtenidos de la siguiente manera:

- Resultados obtenidos a partir de la evaluación de cada uno de los 11 objetivos de control que componen el proceso DS5 "Garantizar la seguridad de los sistemas" con base en el COBIT y la guía de aseguramiento. (Apartado 3.2).

- Calificación obtenida por objetivo de control, de acuerdo con los criterios anteriormente indicados. (Apartado 3.3).
- Determinación del nivel de madurez. (Apartado 3.4).

## 3.2 Resultados obtenidos por objetivo de control

### 3.2.1 DS5. 1 Administración de la Seguridad de TI

c) En noviembre del 2010, la Junta Directiva aprobó la creación de la Oficina de Seguridad Informática y la reportó directamente a la Gerencia. Actualmente, el nombre de la oficina cambió por Unidad de Seguridad de la Información, en adelante USI.

d) Existe un Comité de Seguridad de la Información formalmente aprobado, integrado por:

   a. Gerente.
   b. Auditor de sistemas.
   c. Jefe de la Unidad de Capital Humano.
   d. Jefe del Departamento de Operaciones.
   e. Jefe de la Oficina de Seguridad de la Información.
   f. Jefe de TI.
   g. Asesor legal externo (en caso de que se requiera).

e) Con el fin de regular el funcionamiento del Comité, se elaboró y aprobó el Reglamento del Comité de Seguridad de la Información el cual indica que la periodicidad de convocatoria debe ser al menos trimestral, condición que se pudo constatar, mediante revisión de las actas en sitio.

f) Se ha establecido una política de seguridad de la información, basada en las mejores prácticas del COBIT 4.0 y la norma ISO 27002 y es sustentada por diferentes normativas y procedimientos. La política se encuentra aprobada, actualizada y publicada en la INTRANET tal y como se pudo constatar, mediante una revisión en sitio.

g) Existe un Plan Anual Operativo de Seguridad de la Información donde se pudo constatar que la Unidad ha definido actividades y objetivos de seguridad, con el fin de apoyar los objetivos estratégicos y de contribución, plasmados en el Plan Estratégico institucional.

h) Se ha establecido un plan de seguridad que está actualizado y se publica únicamente para las personas involucradas.

i) En razón de todo lo anterior, se determina que la administración de la seguridad de TI, obedece a acciones de nivel más alto dentro de la organización y se alinea con los requerimientos del negocio, situación que se evidenció anteriormente.

### 3.2.2 DS5.2 Plan de seguridad de TI

a) La institución cuenta con un Plan de Seguridad de TI, el cual fue aprobado por la Junta Directiva en noviembre del 2011 y actualizado por última vez el 01 de noviembre de 2012. Actualmente se encuentra disponible en la INTRANET, y puede ser consultado únicamente por los involucrados, tal y como se pudo constatar en sitio.

b) El Plan de Seguridad considera requerimientos de seguridad de la información del negocio, la clasificación de los datos, políticas de seguridad, gestión de riesgos y requerimientos regulatorios, entre otros.

c) El Plan está implementado en anexos de la siguiente manera:

   i. Requerimientos de cumplimiento-evaluaciones control interno de TI.

   ii. Riesgos de seguridad de la información.

   iii. Roles y estructura de seguridad de la información.

   iv. Configuración de la seguridad de TI.

   v. Políticas, normativas y procedimientos de seguridad informática.

   vi. Inversiones en seguridad de la información.

   vii. Capacitación y entrenamiento de la información.

   viii. Comunicación del Plan de Seguridad de TI.

d) No obstante todo lo anterior, el Plan de Seguridad no considera:

   i. Planes tácticos, no obstante la Unidad sí cuenta con un Plan Anual Operativo y está en proceso la elaboración de una propuesta para el Plan Estratégico de Seguridad de la Información.

   ii. Estándares de tecnología.

   iii. Configuración de la línea base para todas las plataformas, de acuerdo con el Plan de Seguridad, ni se cuenta con un procedimiento para actualizar periódicamente la línea base de configuración, de acuerdo con los cambios en el Plan.

   iv. Inversiones institucionales en recursos de seguridad.

v. Integración con otros procesos, a saber: DS1 Definir y administrar niveles de servicio, DS2 Administrar servicios de terceros, AI1 Identificar soluciones automatizadas, AI2 Adquirir y mantener el *software* aplicativo y AI3 Adquirir y mantener la infraestructura tecnológica.

vi. Aun cuando el Plan de Seguridad se somete a un proceso periódico de actualización (en atención a una política institucional para la administración de la normativa), la Unidad no cuenta con un procedimiento documentado para la actualización de este, que especifique, entre otras cosas, los niveles adecuados de revisión y aprobación, por parte de la dirección y las personas correspondientes.

### 3.2.3 DS5.3 Administración de identidad

a) La USI ha elaborado normativas, con el fin de garantizar que todos los usuarios, y su actividad en sistemas, sean identificados de manera única y que los derechos de acceso estén alineados con las funciones del puesto.

b) No se tiene documentado quiénes son los dueños de los sistemas, lo que supone que la decisión de tramitar un caso relacionado con este tema, queda a criterio de los técnicos; aun cuando se indica que los dueños son fácilmente identificables, podría materializarse en que la administración de accesos no cumpla los requisitos de negocio, y ponga en peligro la seguridad de los sistemas críticos de negocio.

c) Sobre una muestra al azar se constató que:

   i. Se realizan modificaciones en los perfiles, con base en las funciones del puesto.

ii. Los dueños de los sistemas, o bien los Jefes de Departamento, aprueban el acceso a ellos.

d) Se realizan revisiones de perfiles de manera parcial, no es un proceso constante.

e) No existe un repositorio central de las identidades de los usuarios y los derechos de acceso.

### 3.2.4 DS5.4 Administración de cuentas del usuario

a) Existe un procedimiento y normativas, para la solicitud, establecimiento, emisión, suspensión, modificación y cierre de cuentas de usuario y de los privilegios relacionados, el cual se publica en la institución, de manera que puede ser consultado por todas las unidades de negocio.

b) Existe un procedimiento que describe al responsable de los datos o del sistema, como otorgar los privilegios de acceso.

c) La administración debe llevar a cabo, una revisión regular de todas las cuentas y los privilegios asociados, de acuerdo con la normativa NOR-OSI-012 Control de acceso a los sistemas de información. Sin embargo, se identificaron debilidades en el cumplimiento del apartado 4.2.4 “Revisión de Derechos de Acceso de Usuario” establecido en la normativa NOR-OSI-012, ya que las revisiones se realizan de manera parcial, no se obtiene una buena respuesta por parte de los jefes de las unidades de negocio, y adicionalmente, hay confusión con respecto a los responsables de liderar estas revisiones.

### 3.2.5 DS5.5 Pruebas, vigilancia y monitoreo de la seguridad

a) En los últimos dos años, se han realizado estudios de vulnerabilidades y pruebas de penetración; como resultado de lo anterior, se generan planes de acción a los cuales la Unidad de Seguridad de la Información da seguimiento correspondiente en coordinación con TI.

b) No se determina la eficacia de las medidas adoptadas, para resolver una violación de la seguridad.

c) No se valida que la configuración de seguridad, de los parámetros del sistema y de red, esté definida correctamente y en cumplimiento con línea base de seguridad.

d) Inexistencia de un inventario de todos los dispositivos de red, servicios y aplicaciones, con calificación de riesgo de seguridad.

e) No hay vigilancia constante de eventos de seguridad, relacionados con todos los activos de red, críticos para la institución, y de mayor riesgo.

f) La seguridad de la información está integrada de manera parcial, con las iniciativas de gestión de proyectos.

g) En cuanto a la ejecución de procedimientos, para verificar la eficacia de la gestión de cuentas y privilegios, se estableció el procedimiento PROC-OSI-012-004 Monitoreo del Uso de las Cuentas de Usuarios (Logging); sin embargo, mediante las entrevistas y revisiones en sitio no se evidenció cumplimiento de este.

### 3.2.6 DS5.6 Definición de incidente de seguridad

a) Existe el procedimiento denominado “Atención solicitudes servicio e incidentes seguridad-OSI” el cual indica los pasos por seguir para la atención y seguimiento

de incidentes de seguridad. Asimismo, se creó la normativa "NOR-OSI-007 Normativa para la Gestión de Incidentes de Seguridad de la Información" que entre otras cosas, describe las categorías de incidentes de seguridad de la información.

b) Aun cuando se creó la normativa "NOR-OSI-007 Normativa para la Gestión de Incidentes de Seguridad de la Información" y se definieron las categorías de incidentes de seguridad, no se han definido formalmente los niveles de impacto, los números limitados de nivel de impacto para cada incidente, acciones específicas requeridas, las personas que deben ser notificadas, ni medidas de protección de la confidencialidad, de la información relacionada con dichos incidentes.

c) No se ha definido un equipo de respuesta a incidentes de seguridad (ISRT) por ende, no se han considerado las siguientes áreas, como parte de un proceso efectivo de respuesta a incidentes:

    i. Relación con terceros. Roles y responsabilidades de terceros en la prevención y seguimiento de incidentes y corrección de fallas de *software* entre otros.

    ii. Comunicación. Requerimientos, implementación y canales de comunicación en situaciones de emergencia y normales entre los miembros claves del equipo.

    iii. Aspectos legales e investigación criminal. Asuntos impulsados por consideraciones legales y requerimientos de restricción, o limitaciones resultantes de la participación de organismos de investigación, durante el incidente.

iv. Servicios de soporte de centros de apoyo y métodos de interacción con los superiores. Incluyen capacitación, concienciación, gestión de configuración, y autenticación.

v. Investigación. Identificación de actividades de investigación, requerimientos y los fundamentos de la investigación necesaria, en relación con las actividades del centro de respuesta.

d) El proceso de gestión de incidentes de seguridad no incluye los siguientes elementos clave:

i. Detección de eventos.

ii. Correlación de eventos y evaluación de amenazas / incidentes.

iii. Resolución de amenazas o escalamiento en caso de ser necesario.

iv. Criterios para iniciar el proceso de organización del ISRT.

v. Verificación y niveles necesarios de documentación de la Resolución.

vi. Análisis pos-solución.

vii. Cierre del incidente.

### 3.2.7 DS5.7 Protección de la tecnología de seguridad

a) Se han establecido mecanismos de control, para asegurar que el *hardware* o *el software*, relacionados con seguridad de la información, sean a prueba de manipulación, en términos generales por medio de la Política de Seguridad POL-OSI-017 Política de Seguridad de la Información. Además, esta política establece que las violaciones de seguridad serán motivo de sanción, de acuerdo con lo

establecido por la Administración, en el Código de Ética y la normativa de sanciones por acciones disciplinarias.

b) Se han documentado especificaciones de seguridad, para evitar el acceso no autorizado.

c) Se evalúan periódicamente (al menos una vez por año), los mecanismos de protección de la tecnología de seguridad, por medio de estudios de vulnerabilidades y se establecen planes de acción a los cuales la USI da seguimiento.

d) Se han establecido las reglas de contraseña.

e) Se generan informes de seguridad, por medio de herramientas automatizadas para prevenir ataques de penetración; no obstante, llama la atención que las últimas pruebas de penetración fueron efectuadas en el 2008 y no se aporta evidencia de su realización en años posteriores (2009, 2010, 2011, 2012).

f) El ítem correspondiente a robustez de la tecnología de seguridad (por ejemplo algoritmos de encriptación), para resistir la exposición en caso de un acceso no autorizado, resultó negativo.

### 3.2.8 DS5.8 Administración de llaves criptográficas

a) La institución ha establecido políticas para la gestión de las llaves criptográficas, pero estas no consideran:

   i. Lineamientos para determinar cuándo es necesario renovar la llave criptográfica (por ejemplo, cuando se ha visto comprometida o ha caducado).

ii. Mecanismos de seguridad, para asegurar que el almacenamiento y la distribución de las llaves, se realiza de manera segura.

iii. Tamaño mínimo requerido, para la generación de llaves robustas,

iv. Uso de algoritmos de generación de claves requeridos.

v. Identificación de los estándares requeridos para la generación de claves.

vi. Propósitos para los cuales está restringido el uso de las llaves, y para los cuales se debe hacer uso.

vii. Los períodos de uso permitidos. (Solo indica que debe tener una fecha de caducidad).

viii. Copia de seguridad.

ix. Archivo.

x. Destrucción. (Solo indica que deben destruirse utilizando mecanismos seguros).

b) Asimismo, no se evidenció la existencia de procedimientos que consideren:

i. La generación, cambio, revocación, destrucción, distribución, captura y uso de las llaves criptográficas.

ii. Almacenamiento en dispositivos criptográficos seguros.

iii. Exportación desde un módulo criptográfico seguro.

iv. Personas autorizadas para la copia, recuperación y almacenamiento de llaves criptográficas.

### 3.2.9 DS5.9 Prevención, detección y corrección de *software* malicioso

a) Se ha documentado, aprobado, comunicado y publicado políticas y normativas para la prevención, detección y corrección del *malware*.

b) Se han implementado controles automatizados para proporcionar protección contra virus. La Solución Corporativa de Antivirus utilizada es "McAfee EndPointProtectionAdvance".

c) La Solución Corporativa Antivirus es administrada por una Unidad de TI, de modo que la mayoría de las veces las violaciones son comunicadas solo internamente en TI.

d) El *software* de protección está distribuido y configurado de forma centralizada.

e) La Unidad de Seguridad de la Información revisa y evalúa, periódicamente, información sobre nuevas amenazas potenciales.

f) Se han establecido mecanismos para filtrar el correo entrante y evitar correo no deseado.

g) Se ha evaluado la efectividad del proceso de filtrado de correo entrante, por medio de los análisis de vulnerabilidades.

h) Del total de solicitudes de cambio, el 82% son ingresadas por la USI y la mayoría son para el bloqueo de direcciones IP emisoras de Spam o correos fraudulentos. En este sentido, llama la atención el bajo porcentaje de solicitudes de cambio, ingresadas por el Departamento de TI en general, y además, en lo relacionado con cambios en la configuración del *software* de protección.

   Esta situación supone, que los cambios en la configuración del *software* de protección, no están pasando por el proceso de gestión de cambios, aun cuando así

está establecido en la documentación por medio de las normativas, políticas y procedimientos correspondientes.

Es conveniente realizar una evaluación más detallada, del proceso de gestión de cambios; sin embargo, está fuera del alcance de este estudio.

### 3.2.10 DS5.10 Seguridad de la red

a) Los dispositivos de la red se protegen, con mecanismos especiales y se monitorean para identificar patrones, para protegerlos de ataques por medio de herramientas automatizadas.
b) Se planea la arquitectura de seguridad de red, por medio del Plan de Infraestructura.
c) Los dispositivos están sujetos a revisión, en cuanto a implementación o mantenimiento, por parte de expertos independientes. (Auditoría de Sistemas o Unidad de Seguridad de la Información).
d) Para la administración de componentes de red, se cuenta con documentación, actualizada periódicamente por el personal clave y se mantiene un historial de los cambios realizados. No obstante, es conveniente documentar los procedimientos específicos, o bien instrucciones técnicas para la administración de los componentes de la red.

### 3.2.11 DS5.11 Intercambio de datos sensitivos

a) Mensualmente se realiza envío de información sensible a entidades externas por medio de correo electrónico o físico.

b) No se ha definido cómo deben ser protegidos los datos, cuando se intercambian, de acuerdo con la clasificación de la información.

c) No se aplican mecanismos de encriptación previa a ser transmitida fuera de la institución.

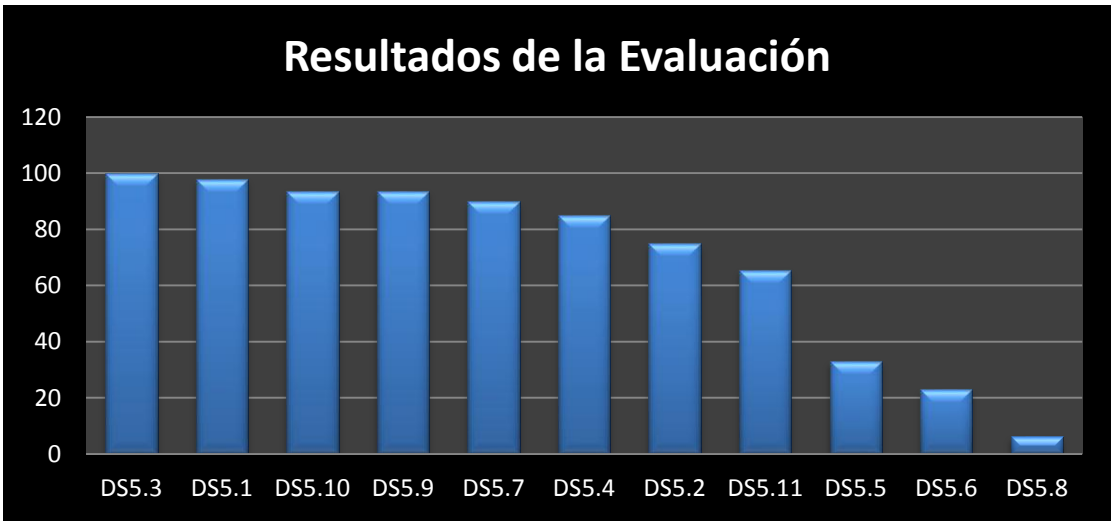
d) Las transacciones de datos sensibles son intercambiadas, con controles que brindan prueba de envío y prueba de recepción, no así autenticidad de contenido, ni rechazo de origen.

### 3.3 Calificación por objetivo de control

Posteriormente a la realización de entrevistas y aplicación de las herramientas diseñadas, para evaluar cada uno de los objetivos de control del proceso COBIT DS5 "Garantizar la Seguridad de los Sistemas", se obtuvo una calificación, tal y como se puede observar en la Figura Nº8.

Es importante mencionar, que estas calificaciones se otorgaron a partir de la definición del diseño del control, de acuerdo con la guía de aseguramiento y los objetivos de control.

**Figura No.8 Calificación por objetivo de control**




**Fuente: De elaboración propia con base en los resultados obtenidos.**

Como se puede observar en el gráfico anterior, los objetivos de control con calificación más baja son: DS5.11 Intercambio de datos sensitivos, DS5.6Gestión de incidentes, DS5.5 Pruebas, vigilancia y monitoreo de la seguridad y DS5.8 Administración de llaves criptográficas, lo que puede acarrear las siguientes consecuencias:

| Objetivo de control | Riesgo. |
|---|---|
| **DS5.8 Administración de llaves criptográficas.** | Pérdidas económicas o de imagen por:<br>• Usurpación de claves con fines malintencionados, por partes no autorizadas.<br>• Acceso no autorizado a las claves criptográficas, lo que puede comprometer la seguridad de la información de los accionistas.<br>• Pérdida de confidencialidad, lo que puede provocar daños de imagen. |

| Objetivo de control | Riesgo. |
|---|---|
| **DS5.6 Gestión de incidentes.** | • Inadecuada respuesta a los incidentes de seguridad, lo que puede provocar un impacto negativo en el servicio al accionista, en los activos de TI y en la seguridad de la información.<br>• Inadecuado proceso de seguimiento de incidentes, lo que puede provocar la materialización de otros eventos negativos e incidentes que no son tratados por medio del proceso de gestión de problemas (análisis de causa raíz).<br>• Brechas de seguridad no identificadas y tratadas de manera oportuna.<br>• Confidencialidad, integridad o disponibilidad de la información comprometida por los incidentes de seguridad |
| **DS5.5 Pruebas, vigilancia y monitoreo de la seguridad.** | • Mal uso de las cuentas de usuario, lo que puede comprometer la seguridad de la información.<br>• Brechas de seguridad no identificadas, ni tratadas de manera oportuna. |
| **DS5.11 Intercambio de datos sensitivos** | • Exposición de información sensible, lo que |

| Objetivo de control | Riesgo. |
|---|---|
| | puede provocar problemas legales, de imagen, o afectar directamente a los accionistas.<br>• Revelación de información a personas inescrupulosas y no autorizadas. |

**Fuente: De elaboración propia**

### 3.4 Calificación del proceso y determinación del nivel de madurez

Aunada a la calificación por objetivo de control se aplicó la matriz denominada "Matriz de Calificación de la Gestión de TI", la cual establece un conjunto de preguntas de respuesta cerrada, asociado a cada objetivo de control, y está referenciada en el cuerpo del "Reglamento Sobre la Gestión de la Tecnología de Información" (Acuerdo SUGEF 1409). Posteriormente, se calcularon la nota y el nivel de madurez, con base en el anexo 2 ("Procedimiento para Obtener la Calificación sobre la Gestión de TI") de dicho acuerdo.

La calificación está compuesta por dos factores, a saber:

#### 3.4.1 Calificación del cumplimiento de los objetivos de control (Factor 1)

Se le asigna un peso de 70 sobre el total de la nota.

La calificación del cumplimiento de los objetivos de control, asociados al proceso en estudio, se puede apreciar en la figura N° 10.

#### 3.4.2 Nivel de madurez alcanzado (Factor 2)

Se le asigna un peso de 30 sobre el total de la nota. En la figura N° 9 se muestran los resultados obtenidos para este factor.

**Figura No.9 Cálculo del nivel de madurez (Factor 2)**

| Nivel | Descripción | Calificación | % |
|---|---|---|---|
| **3** | Definido | 1.00 | 100% |

**Fuente: Obtenido a partir de la aplicación de la matriz denominada "Matriz de Calificación de la Gestión de TI" con base en el anexo 2 "Procedimiento para Obtener la Calificación sobre la Gestión de TI" del Acuerdo SUGEF 1409".**

La calificación obtenida corresponde al Nivel 3 "Definido" (nivel requerido como regulación.)

Según lo que indica COBIT en la sección niveles de madurez:

**"3 Proceso definido**

Existe conciencia sobre la seguridad y esta es promovida por la gerencia. Los procedimientos de seguridad de TI están definidos y alineados con la política de seguridad de TI. Las responsabilidades de la seguridad de TI están asignadas y entendidas, pero no continuamente implementadas. Existe un plan de seguridad de TI y existen soluciones de seguridad motivadas por un análisis de riesgo. Los reportes no contienen un enfoque claro de negocio. Se realizan pruebas de seguridad adecuadas (por ejemplo, pruebas contra intrusos). Existe capacitación en seguridad para TI y para el negocio, pero se programa y se comunica de manera informal." (Pag.122).

Es importante indicar, que como parte del análisis, se identificó que actualmente el proceso DS5 Garantizar la Seguridad de los sistemas, implementado en la institución, cuenta con una brecha del 83% para alcanzar el nivel de madurez 4 "Administrado y medible".

Finalmente, la aplicación de dicha matriz y el "Procedimiento para Obtener la Calificación sobre la Gestión de TI" arrojó los resultados mostrados en la Figura Nº10.

**Figura No.10 Calificación de proceso**

| Descripción | Peso | Calificación | Resultado | % |
|---|---|---|---|---|
| Resultado de la calificación del Objetivos de Control (COC) - Factor 1. | 0.70 | 0.81 | 0.56 | 56% |
| Resultado de la calificación del Nivel de Madurez (CNM) - Factor 2. | 0.30 | 1 | 0.30 | 30% |
| Resultado | | | 0.86 | 86% |

**Fuente: De elaboración propia, obtenido a partir de la aplicación de la matriz denominada "Matriz de Calificación de la Gestión de TI" con base en el anexo 2 "Procedimiento para Obtener la Calificación sobre la Gestión de TI" del Acuerdo SUGEF 1409.**

El resultado obtenido es de **86**, colocando el proceso en un nivel "Normal". Según la tabla de niveles de la gestión de TI, del reglamento sobre la gestión de la tecnología de información para el acuerdo SUGEF 14-09, como se muestra a continuación:

**Figura No.11 Niveles de calificación sobre la gestión de TI.**

| Calificación | Nivel |
|---|---|
| Mayor o igual que 85%. | Normal |
| Mayor o igual que 70% y menor que 85%. | Irregularidad 1. |
| Mayor o igual que 55% y menor que 70%. | Irregularidad 2. |
| Menor que 55%. | Irregularidad 3. |

**Fuente: Reglamento sobre la Gestión de la Tecnología de Información (Acuerdo SUGEF 14-09).**

Aunado a los resultados indicados anteriormente, se elaboró un informe de hallazgos a partir de las debilidades de control, identificadas a lo largo del estudio, con base en criterios de la normativa aplicable a CDA (Normativa interna de la institución y los objetivos de control de COBIT, del proceso COBIT DS5 "Garantizar la Seguridad de los Sistemas"). El informe de hallazgos está disponible en el anexo 2.

En el próximo capítulo se detallan las conclusiones y recomendaciones, con base en los resultados que se desprendieron de la evaluación realizada.

# CAPÍTULO IV

El objetivo de este capítulo es detallar las recomendaciones y conclusiones, con base en los resultados que se desprendieron de la evaluación realizada, y que se van a comunicar a los diferentes responsables en la administración.

## 4.1 Recomendaciones

Al realizar la evaluación y analizar los resultados obtenidos con respecto a lo esperado, se identifica una serie de recomendaciones u oportunidades de mejora, con el fin de que sean comunicadas a la institución.

En primera instancia, es posible especificar cuatro oportunidades de mejora que la institución debe atender con mayor prioridad, las cuales corresponden a los resultados con la calificación más baja, respecto al cumplimiento de los objetivos de control del proceso COBIT® DS5 “Garantizar la Seguridad de los Sistemas” y el nivel de madurez requerido por la institución, en este proceso en particular, según el acuerdo SUGEF 14-09 (apartados 4.1.1, 4.1.2, 4.1.3 y 4.1.4).

Posteriormente, se detallan oportunidades de mejora que se desprenden de la evaluación del diseño de los controles, a partir de la guía de aseguramiento denominada “IT Assurance Guide Using COBIT®”.

### 4.1.1 DS5.4 Gestión de cuentas y derechos de acceso

j) Definir, documentar y comunicar formalmente un proceso para la revisión de derechos de acceso, el cual debe tener claramente establecidos, al menos, los responsables, las funciones y la periodicidad de revisión.

k) Realizar un proceso de sensibilización, que tenga como fin, el conocimiento efectivo del uso e importancia de los derechos de acceso, que al menos considere la participación de los jefes de departamento de las unidades de negocio y de TI.

l) Coordinar con las diferentes áreas involucradas, para la creación del repositorio centralizado, donde se mantengan las identidades del usuario y los derechos de acceso, así como la definición de mecanismos de control, los cuales aseguren que dicho repositorio se mantenga actualizado.

m) Establecer un proceso de evaluación periódica, de forma que se mantengan las condiciones idóneas y los niveles de control adecuados, para lo establecido en las recomendaciones a, b y c, indicadas anteriormente.

### 4.1.2 DS5.6 Gestión de incidentes de seguridad

Se recomienda:

a) Establecer controles de seguimiento y monitoreo a la actividad establecida "fortalecer el proceso de gestión de incidentes" de forma que no se deteriore y se mantenga la calidad y suficiencia de esta, además de involucrar al Departamento de Tecnologías de Información, para que aporten la información necesaria y se ejecute de conformidad con los resultados obtenidos en la consultoría realizada para tal fin.

b) Definir y velar, con el apoyo del Departamento de TI, por la ejecución de mecanismos de control, para garantizar el cumplimiento de lo establecido en consultoría realizada para tal fin, y que las desviaciones en las actividades planeadas se presenten a la Alta Administración, con el fin de que se tomen las medidas necesarias.

### 4.1.3 DS5.8 Administración de llaves criptográficas

a) Documentar, aprobar y comunicar formalmente, los lineamientos relacionados con la administración de llaves criptográficas, que al menos incluyan las siguientes directrices:

   i. Determinación de cuándo es necesario renovar la llave criptográfica.
   ii. Almacenamiento y distribución de las llaves de manera segura.
   iii. Tamaño mínimo requerido para la generación de llaves robustas.
   iv. Algoritmos de generación de claves requeridos.
   v. Identificación de los estándares requeridos para la generación de claves.
   vi. Propósitos para los cuales está restringido el uso de las llaves y para los cuales se debe hacer uso.
   vii. Periodos de uso permitidos.
   viii. Capias de seguridad.
   ix. Políticas y acciones de archivo o almacenamiento
   x. Métodos de desecho.

b) Documentar, aprobar y comunicar un procedimiento (alineado con los lineamientos de llaves criptográficas indicados en la recomendación anterior) que al menos considere:

   i. La generación, cambio, revocación, destrucción, distribución, captura y uso de las llaves criptográficas.
   ii. Lo establecido en las directrices emitidas por la Unidad de Seguridad de la Información.

c) Se establezca y se vele por el cumplimiento de mecanismos de control, para asegurar el cumplimiento del procedimiento.

### 4.1.4 DS5.11 Intercambio de datos sensibles

a) Definir y ejecutar controles, que brinden autenticidad de contenido y no rechazo de origen, durante el proceso de intercambio de datos sensibles y que coordine con las diferentes entidades receptoras, el uso de mecanismos de encriptación, para asegurar la confidencialidad de la información que se intercambia.

### 4.1.5 DS5.1 Administración de la Seguridad de TI

a) Establecer un proceso para priorizar las iniciativas de seguridad, de manera alineada con los objetivos estratégicos de la institución.

### 4.1.6 DS5.2 Plan de Seguridad de TI

a) Documentar, aprobar y comunicar un procedimiento para la actualización del Plan de Seguridad de TI, donde se detalle al menos los responsables, así como la periodicidad para la realización las actualizaciones y además se establezcan mecanismos para evaluar el cumplimiento del procedimiento.
b) Valorar la inclusión de los siguientes elementos (pero no únicamente) en el Plan de Seguridad de TI:
    i. Planes tácticos.
    ii. Estándares de tecnología.

iii. Configuración de la línea base para todas las plataformas, de acuerdo con el Plan de Seguridad, dado que no se cuenta con un procedimiento para actualizar periódicamente la línea base de configuración, de acuerdo con los cambios en el plan.

iv. Inversiones en recursos de seguridad por parte de la institución.

v. Integración con otros procesos, a saber: DS1 Definir y administrar niveles de servicio, DS2 Administrar servicios de terceros, AI1 Identificar soluciones automatizadas, AI2 Adquirir y mantener el *software* aplicativo y AI3 Adquirir y mantener la infraestructura tecnológica.

### 4.1.7 DS5.3 Administración de la identidad

a) Las recomendaciones relacionadas con este objetivo de control, se integraron con las vinculadas con gestión de cuentas, en el apartado 4.1.4 indicado anteriormente.

### 4.1.8 DS5.5Pruebas, vigilancia y monitoreo de la seguridad

a) Determinar la suficiencia de los planteamientos, para atender una violación de la seguridad, de forma que se garantice la prevención y mitigación de este tipo de riesgo.

b) Definir las líneas base de seguridad, de forma que se garantice que la configuración de seguridad de los parámetros, del sistema y de red, estén definidos correctamente.

c) Elaborar un inventario de todos los dispositivos de red, servicios y aplicaciones con calificación de riesgo de seguridad, así como un procedimiento para la actualización de dicho inventario.

d) Establecer vigilancia constante de eventos de seguridad para todos los activos de red críticos para la organización y de mayor riesgo, con el fin de que se tomen las acciones necesarias, de manera oportuna, para evitar la materialización de estos riesgos.

e) Formalizar la integración de la Unidad de Seguridad de la Información, con las iniciativas de gestión de proyectos, a fin de asegurar que su criterio es considerado en el desarrollo, diseño y definición de requerimientos de pruebas, para minimizar el riesgo de materialización de vulnerabilidades, relacionadas con la seguridad de la información.

f) Realizar una revisión general de todos los procedimientos, así como de la ejecución eficaz de estos. Se considera de vital importancia la revisión de los procedimientos denominados: “PROC-OSI-012-004 Monitoreo del Uso de las Cuentas de Usuarios (Logging)” y “PROC-OSI-002-012 Validar cumplimiento procedimientos seguridad información”.

### 4.1.9 DS5.7 Protección de la tecnología de seguridad

a) Definir formalmente y comunicar los algoritmos de encriptación por utilizar, para resistir la exposición en caso de un acceso no autorizado.

### 4.1.10 DS5.9 Prevención, detección y corrección de *software* malicioso

a) Continuar ejecutando los controles, que la institución ha establecido para este objetivo de control. No se identificaron debilidades de control.

### 4.1.11 DS5.10 Seguridad de la red

a) Documentar formalmente el procedimiento, para la administración de componentes de red.

## 4.2 Conclusiones

Al finalizar el desarrollo de este estudio, se alcanzó el objetivo general señalado en este documento el cual consistió en evaluar el proceso "Garantizar la Seguridad de los Sistemas" de acuerdo con la normativa aplicable a la institución, con el fin de emitir un criterio dirigido a la administración, sobre el nivel de madurez alcanzado en este proceso.

La Unidad de Seguridad de la Información, con el apoyo de la Gerencia, ha realizado esfuerzos para el cumplimiento de lo indicado en el marco de referencia COBIT®; sin embargo, se deben tomar en consideración las recomendaciones anteriormente planteadas, para lograr la ejecución óptima del proceso, haciendo énfasis en las debilidades identificadas en la gestión de cuentas y derechos de acceso, gestión de incidentes de seguridad, administración de llaves criptográficas e intercambio de datos sensibles (apartados 4.1.1, 4.1.2, 4.1.3 y 4.1.4).

El no acatamiento de estas recomendaciones podría generar un impacto negativo en la institución por:

- Pérdidas económicas:
    - Reprocesos ocasionados por una inadecuada gestión de incidentes de seguridad, lo que puede provocar la materialización de otros eventos negativos, que no son subsanados por medio del proceso de gestión de problemas (análisis de causa raíz).
- Pérdida de imagen por:
    - Manipulación de información de forma malintencionada, por accesos no autorizados.
    - Inadecuada respuesta a los incidentes de seguridad, lo que puede provocar un impacto negativo en el servicio al accionista, en los activos de TI y en la seguridad de la información.
    - Brechas de seguridad no identificadas y tratadas de manera oportuna.
    - Pérdida de confidencialidad, integridad o disponibilidad de la información, causada por los incidentes de seguridad.
    - Usurpación de llaves criptográficas, con fines malintencionados por partes no autorizadas, lo que puede comprometer la seguridad de la información de los accionistas.
- Procesos legales por:
    - Exposición de información sensible de los accionistas.
    - Revelación de información a personas inescrupulosas y no autorizadas.
- Incumplimiento regulatorio.

Para los otros incumplimientos, a pesar de que no son sustantivos en este momento, la aplicación de las recomendaciones sí contribuiría, a que la institución alcance un mayor grado de madurez, de este proceso en particular.

La sinergia que puedan realizar, la Unidad de Seguridad de la Información y el Departamento de Tecnologías de Información, es vital para el mejoramiento de todas las debilidades que se presentaron.

Destacar la función de la Unidad de Seguridad de la Información que, con el apoyo de la alta dirección, se ha encargado de desarrollar e implementar la seguridad en la Institución, para poder brindar, tanto a los accionistas como a los trabajadores, confidencialidad, integridad y disponibilidad de la información.

Finalmente, lo correspondiente a intereses profesionales y el aporte a la institución, señalado al inicio de esta práctica profesional, de igual manera que los objetivos, fueron alcanzados al finalizar este estudio, con el apoyo y guía de la lectora académica y lectora empresarial, así como el profesor del curso.

## Referencias

IT Governance Institute®. Objetivos de Control para la Información y la Tecnología Relacionada. COBIT 4.0®, 2005.

IT Governance Institute®. Cobit Control Practices. Segunda edición, 2007.

IT Governance Institute®. IT Assurance Guide Using COBIT, 2007.

Contraloría General de la República. Normas técnicas para la gestión y el control de las Tecnologías de Información. (N-2-2007-CO-DFOE)

Tupia, Manuel. Administración de la Seguridad de la Información. Primera Edición. Perú, enero 2010.

Superintendencia General de Entidades Financieras. Acuerdo SUGEF 1409. San José, Costa Rica, 2009.

ISACA. Manual de preparación al examen CISM®. Estados Unidos, 2011.

Escuela de Administración de Negocios. Técnico en Auditorías de Tecnologías de Información. Evaluación de la Seguridad. Editorial UCR. San José, Costa Rica. 2010.

Cámara de Bancos Instituciones Financieras de Costa Rica y la Academia Bancaria. Resultados del primer ciclo de auditoría sobre la gestión de TI del Acuerdo SUGEF 1409, 2012.

IT Governance Institute®. Global Status Report on the Governance of Enterprise It (Geit), 2011.

# Anexos

## 1. Formulario COEN (Conocimiento del entorno) proceso "Garantizar la Seguridad de los Sistemas"

**Objetivo:**

**Instrucciones:**

| N° | Descripción | Acción | SÍ | NO | COMENTARIOS | REF |
|---|---|---|---|---|---|---|
| **1 Conciencia** | | | | | | |
| **1.1** | **Existe conciencia sobre la seguridad** | | | | | |
| 1.1.1 | La organización reconoce la necesidad de la seguridad para TI. | **Conocimiento.** | | | | |
| 1.1.2 | Se realizan campañas de concienciación de seguridad. | **Conocimiento.** | | | | |
| 1.1.3 | Las campañas de concienciación de seguridad son impartidas a todos los colaboradores. | **Conocimiento.** | | | | |
| 1.1.4 | Para las campañas de concienciación de seguridad, se toman en cuenta también los empleados de proveedores que están involucrados de alguna manera con la seguridad de la información de la organización. | **Conocimiento.** | | | | |
| 1.1.5 | Las campañas de concienciación incluyen: | **Conocimiento.** | | | | |
| 1.1.5.1 | Promocionales de mercadeo. | **Conocimiento.** | | | | |
| 1.1.5.2 | Mensajes en las pantallas de inicio de sesión y bloqueo. | **Conocimiento.** | | | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| 1.1.5.3 | Videos. | **Conocimiento.** | | | | |
| 1.1.5.4 | Correos electrónicos. | **Conocimiento.** | | | | |
| 1.1.5.5 | Publicaciones en la intranet. | **Conocimiento.** | | | | |
| 1.1.6 | Los usuarios identifican incidentes de seguridad. | **Comprensión.** | | | | |
| 1.1.7 | Los usuarios identifican ataques de ingeniería social. | **Comprensión.** | | | | |
| 1.1.8 | Los usuarios reportan los incidentes de seguridad. | **Aplicación.** | | | | |
| 1.1.9 | Los usuarios reportan ataques de ingeniería social. | | | | | |
| 1.1.10 | Se realizan comparaciones para determinar si se ha disminuido la cantidad de incidentes de seguridad. | **Evaluación.** | | | | |
| 1.1.11 | Se realizan comparaciones para determinar si la cantidad de usuarios que reconocen ataques de ingeniería social ha aumentado. | **Evaluación.** | | | | |
| 1.1.12 | Las campañas de concienciación de seguridad se realizan al menos una vez al año. | **Mejora continua.** | | | | |
| **1.2** | **La conciencia en seguridad es promovida por la gerencia** | | | | | |
| 1.2.1 | La gerencia reconoce la necesidad de la seguridad para TI. | **Conocimiento.** | | | | |
| 1.2.2 | Existe un procedimiento establecido que indique cuáles de los temas relacionados con la seguridad de la información tienen que recibir la aprobación gerencial. | **Conocimiento.** | | | | |
| 1.2.3 | Se explica adecuadamente a la Gerencia los temas relacionados con seguridad, con el fin de que adquiera un correcto | **Comprensión.** | | | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | entendimiento. | | | | | |
| 1.2.4 | El procedimiento que indique cuáles de los temas relacionados con la seguridad de la Información tienen que recibir la aprobación gerencial se cumple de acuerdo con lo establecido. | **Aplicación.** | | | | |
| 1.2.5 | La gerencia aprueba suficientes recursos para invertir en seguridad de la información. | **Aplicación.** | | | | |
| 1.2.6 | La aprobación de recursos para invertir en seguridad de la información se realiza posteriormente a la evaluación por parte de la Gerencia. | **Evaluación.** | | | | |
| 1.2.7 | | **Mejora.** | | | | |
| **2 Política de Seguridad** | | | | | | |
| **2.1** | **Se ha establecido una política de seguridad** | | | | | |
| 2.1.1 | La política de seguridad ha sido comunicada a todos los usuarios. | **Conocimiento.** | | | | |
| 2.1.2 | Los usuarios conocen sobre la existencia de la política de seguridad. | **Conocimiento.** | | | | |
| 2.1.3 | La política de seguridad se encuentra disponible en un lugar de fácil acceso. | **Conocimiento.** | | | | |
| 2.1.4 | Se informa a los proveedores sobre los requerimientos específicos de seguridad de la empresa, establecidos en la política de seguridad, cuando aplique. | **Conocimiento.** | | | | |
| 2.1.5 | La política de seguridad se somete a un proceso de revisión por parte de las personas involucradas. | **Comprensión.** | | | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| 2.1.6 | La política de seguridad está aprobada. | **Comprensión.** | | | | |
| 2.1.7 | Los usuarios comprenden los lineamientos establecidos en la política de seguridad. | **Comprensión.** | | | | |
| 2.1.8 | Se aplican las sanciones administrativas por incumplimiento de la política (en caso de que aplique). | **Aplicación.** | | | | |
| 2.1.9 | Se incluye en los contratos con proveedores, cláusulas sobre el cumplimento de la política de seguridad de la institución. | **Aplicación.** | | | | |
| 2.1.10 | Se evalúa el cumplimiento de la política de seguridad. | **Evaluación.** | | | | |
| 2.1.11 | Se evalúa el cumplimiento de la política de seguridad, por parte de los proveedores, en caso de que aplique. | **Evaluación.** | | | | |
| 2.1.12 | La política de seguridad se actualiza al menos una vez por año | **Mejora continua.** | | | | |
| **2.2** | **Los procedimientos de seguridad de TI están definidos** | | | | | |
| 2.2.1 | Los procedimientos de seguridad han sido comunicados a las partes involucradas en su ejecución. | **Conocimiento.** | | | | |
| 2.2.2 | Las partes involucradas conocen sobre la existencia de los procedimientos de seguridad. | **Conocimiento.** | | | | |
| 2.2.3 | Los procedimientos de seguridad se encuentran disponibles en un lugar de fácil acceso. | **Conocimiento.** | | | | |
| 2.2.4 | Los procedimientos de seguridad se someten a un proceso de revisión por parte de las personas involucradas. | **Comprensión** | | | | |
| 2.2.5 | Como parte de la revisión de los procedimientos se valida, entre otras cosas, que estén alineados | **Comprensión..** | | | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | con la política de seguridad. | | | | | |
| 2.2.6 | Los procedimientos de seguridad de TI están aprobados. | **Comprensión.** | | | | |
| 2.2.7 | Las partes involucradas comprenden los procedimientos establecidos. | **Comprensión.** | | | | |
| 2.2.8 | Se aplican los procedimientos de seguridad de TI. | **Aplicación.** | | | | |
| 2.2.9 | Se evalúa el cumplimiento de los procedimientos de TI. | **Evaluación.** | | | | |
| 2.2.10 | Los procedimientos de seguridad se actualizan al menos una vez por año. | **Mejora continua.** | | | | |
| **3 Responsabilidades** | | | | | | |
| **3.1** | **Las responsabilidades de la seguridad de TI están asignadas.** | | | | | |
| 3.1.1 | Las responsabilidades de la seguridad de TI fueron formalmente comunicadas a los involucrados. | **Conocimiento.** | | | | |
| 3.1.2 | Las responsabilidades de la seguridad de TI están debidamente documentadas, en las funciones del puesto de las personas involucradas. | **Conocimiento.** | | | | |
| 3.1.3 | Las personas con responsabilidades de la seguridad de TI comprenden las responsabilidades asignadas. | **Comprensión.** | | | | |
| 3.1.4 | Cada área conoce su ámbito de acción. | **Comprensión.** | | | | |
| 3.1.5 | Las personas a las que se les han asignado responsabilidades de seguridad tienen las competencias técnicas necesarias. | **Comprensión.** | | | | |
| 3.1.6 | Las responsabilidades de seguridad se ejecutan de acuerdo con lo establecido. | **Aplicación.** | | | | |
| 3.1.7 | Las responsabilidades asignadas son evaluadas periódicamente, | **Mejora** | | | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | con el fin de que estén acordes con las necesidades, según evolucionan los riesgos tecnológicos del mercado, que pueden impactar la organización. | **continua.** | | | | |
| **Plan de Seguridad** | | | | | | |
| **4.1** | **Existe un plan de seguridad de TI.** | | | | | |
| 4.1.1 | El Plan de seguridad ha sido comunicado a todos los involucrados. | **Conocimiento.** | | | | |
| 4.1.2 | Los involucrados conocen sobre la existencia del Plan de Seguridad. | **Conocimiento.** | | | | |
| 4.1.3 | El Plan de Seguridad se somete a un proceso de revisión o aprobación por parte de las personas involucradas. | **Comprensión.** | | | | |
| 4.1.4 | El Plan de Seguridad ha sido aprobado. | **Comprensión.** | | | | |
| 4.1.5 | El Plan de Seguridad es actualizado al menos una vez por año. | **Mejora.** | | | | |
| **Evaluación de riesgos** | | | | | | |
| **4.2** | **Existen soluciones de seguridad motivadas por un análisis de riesgo.** | | | | | |
| 4.2.1 | Se identifican los riesgos relacionados con seguridad de la información. | **Conocimiento.** | | | | |
| 4.2.2 | Se evalúan los riesgos relacionados con seguridad de la información. | **Comprensión.** | | | | |
| 4.2.3 | La evaluación de riesgos de seguridad de la información se realiza en términos de: | **Comprensión.** | | | | |
| 4.2.3.1 | Confidencialidad. | **Comprensión.** | | | | |
| 4.2.3.2 | Integridad. | **Comprensión.** | | | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| 4.2.3.3 | Disponibilidad. | **Comprensión.** | | | | |
| 4.2.4 | Se generan planes de acción, motivados por el análisis de riesgos. | **Aplicación.** | | | | |
| 4.2.5 | Se realizan, periódicamente, evaluaciones de riesgos. | **Evaluación.** | | | | |
| **5 Reportes de seguridad** | | | | | | |
| **5.1** | **Se generan reportes de seguridad.** | | | | | |
| 5.1.1 | Existe un procedimiento para la generación de los reportes de seguridad. | **Conocimiento.** | | | | |
| 5.1.2 | Se dan a conocer los reportes de seguridad. | **Conocimiento.** | | | | |
| 5.1.3 | Los reportes de seguridad son expuestos, con el fin de que los destinatarios lo comprendan adecuadamente. | **Comprensión.** | | | | |
| 5.1.4 | Se aplica el procedimiento para la generación de los reportes de seguridad. | **Aplicación.** | | | | |
| 5.1.5 | Los reportes de seguridad son analizados por las personas involucradas. | **Evaluación.** | | | | |
| 5.1.6 | Se realizan reportes de medición del desempeño del proceso de seguridad. | **Mejora.** | | | | |
| **6 Pruebas de seguridad** | | | | | | |
| **6.1** | **Se realizan pruebas de seguridad adecuadas (por ejemplo, pruebas contra intrusos).** | | | | | |
| 6.1.1 | Se cuenta con un cronograma de pruebas de seguridad. | **Conocimiento.** | | | | |
| 6.1.2 | Las pruebas de seguridad se comunican a los encargados, con responsabilidades de seguridad, para que las | **Conocimiento.** | | | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | conozcan. | | | | | |
| 6.1.3 | Las pruebas de seguridad son comunicadas a la Gerencia, en caso de que aplique. | **Conocimiento.** | | | | |
| 6.1.4 | Se ejecutan las pruebas de seguridad, de conformidad con el plan. | **Aplicación.** | | | | |
| 6.1.5 | Los resultados de las pruebas de seguridad son evaluados por los responsables. | **Evaluación.** | | | | |
| 6.1.6 | Con base en los resultados de las pruebas de seguridad, se establecen análisis de brechas (planes de acción). | **Evaluación.** | | | | |
| 6.1.7 | Se da seguimiento al cumplimiento de los planes de acción. | **Mejora.** | | | | |
| 6.1.8 | El cronograma de pruebas de seguridad se actualiza anualmente. | **Mejora.** | | | | |
| **7 Capacitación** | | | | | | |
| **7.1** | Se cuenta con un plan de capacitación en seguridad de TI. | | | | | |
| 7.1.1 | El plan incluye: | | | | | |
| 7.1.1.1 | TI. | **Conocimiento.** | | | | |
| 7.1.1.2 | Áreas de negocio. | **Conocimiento.** | | | | |
| 7.1.1.3 | Las capacitaciones son planificadas con base en las necesidades de entrenamiento. | **Conocimiento.** | | | | |
| 7.1.1.4 | Las capacitaciones son recibidas conforme el plan de capacitación previamente definido. | **Aplicación.** | | | | |
| 7.1.1.5 | En caso de capacitaciones externas, se toma en cuenta la opinión de los participantes, sobre el cumplimiento de expectativas del curso. | **Evaluación.** | | | | |
| 7.1.1.6 | El plan de capacitación es actualizado anualmente. | **Mejora.** | | | | |

**Comentarios generales**

| |
|---|
| |

| Datos del auditado | Fecha | Puesto | Firma |
|---|---|---|---|
| | | | _____ |

| Nombre del auditor: | Fecha Inicio: | Fecha Fin: | Firma: |
|---|---|---|---|
| Ing. Magaly Fernández Marín | | | |
| Revisado por: MATI. Ana Patricia Porras S. | | | |

## 2. Cuestionario de control interno

**Objetivo:** Conocer y evaluar el sistema de control interno de la institución, mediante la aplicación del presente cuestionario[1]

| # | Descripción | FACTOR | SÍ | NO | NA | COMENTARIOS |
|---|---|---|---|---|---|---|
| **1) Ambiente interno** | | | | | | |
| 1. | La Alta Dirección aprueba políticas para la gestión del riesgo tecnológico. | Filosofía de gestión de riesgos. | | | | |
| 2. | La institución expresa el riesgo aceptado (apetito de riesgo). | IDEM. | | | | |
| 3. | El Departamento de Informática ha establecido una estrategia para la gestión de riesgos. Justifique. | IDEM. | | | | |
| 4. | Las actividades de gestión de riesgos son apoyadas por la Jefatura del Departamento de Informática. | IDEM. | | | | |
| 5. | Los mandos medios del Departamento de Informática son receptivos a las actividades de gestión de riesgos. | IDEM. | | | | |
| 6. | Existe un código de ética actualizado. | Integridad y valores éticos. | | | | |
| 7. | El código de ética es del conocimiento de los colaboradores. | IDEM. | | | | |
| 8. | El código de ética está en un lugar de fácil acceso para todos los colaboradores. | IDEM. | | | | |
| 9. | Se realizan actividades de sensibilización en aspectos relacionados con el código de ética. | IDEM. | | | | |
| 10. | Se han establecido valores institucionales. | IDEM. | | | | |
| 11. | Se realizan actividades de sensibilización en aspectos relacionados con los valores institucionales. | IDEM. | | | | |

[1] Basado en el Informe COSO ERM

| # | Descripción | FACTOR | SÍ | NO | NA | COMENTARIOS |
|---|---|---|---|---|---|---|
| 12. | Los mandos medios de Informática demuestran un ejemplo positivo de código de ética. Ejemplifique. | IDEM. | | | | |
| 13. | La Jefatura de Informática demuestra, un ejemplo positivo de código de ética. Justifique su respuesta. | IDEM. | | | | |
| 14. | Se elaboran planes de capacitación anualmente. | Competencia. | | | | |
| 15. | Se ejecutan al 100% los planes de capacitación. En caso de que la respuesta sea negativa, indique en qué porcentaje se ejecutan dichos planes. | IDEM. | | | | |
| 16. | Todos los colaboradores del Departamento de Informática son considerados en la elaboración de dichos planes de capacitación. | IDEM. | | | | |
| 17. | Los planes de capacitación se elaboran en función de las necesidades de capacitación de acuerdo con el puesto. | IDEM. | | | | |
| 18. | El Departamento de Informática está formalmente definido en el organigrama de la institución. | Estructura Organizativa | | | | |
| 19. | El organigrama del Departamento se encuentra actualizado. | IDEM. | | | | |
| 20. | Los roles y responsabilidades están formalmente definidos. | Asignación de autoridad y responsabilidad. | | | | |
| 21. | La Alta Dirección ha establecido mecanismos para la rendición de cuentas. | IDEM. | | | | |
| 22. | El Departamento de Informática ha establecido mecanismos para la rendición de cuentas. | IDEM. | | | | |
| **2) Establecimiento de objetivos** | | | | | | |
| 23. | Los objetivos estratégicos institucionales están establecidos. | Objetivos estratégicos | | | | |

| # | Descripción | FACTOR | SÍ | NO | NA | COMENTARIOS |
|---|---|---|---|---|---|---|
| 24. | Los objetivos estratégicos de TI están establecidos. | IDEM. | | | | |
| 25. | Los objetivos estratégicos de TI contribuyen con el logro de los objetivos estratégicos institucionales. | IDEM. | | | | |
| 26. | Se identifican los riesgos asociados a los objetivos estratégicos de TI. | IDEM. | | | | |
| 27. | El Departamento de TI elabora objetivos operativos sobre la base de los objetivos estratégicos. | Objetivos operativos. | | | | |
| 28. | Se han establecido mecanismos para informar sobre el cumplimiento de los objetivos operativos. | IDEM. | | | | |
| 29. | Se establecen los niveles de riesgo de las nuevas iniciativas que la institución está preparada para asumir. | Riesgo aceptado. | | | | |
| 30. | El Departamento de Informática considera los niveles aceptables de desviación relativa a la consecución de objetivos (tolerancia al riesgo) definida por la alta dirección. | Tolerancia al riesgo. | | | | |
| | **3) Identificación de riesgos** | | | | | |
| 31. | Existe alguna metodología para la identificación de riesgos | | | | | |
| 32. | El Departamento de Informática utiliza la metodología de identificación de riesgos relacionados con la tecnología *(los eventos pueden ser positivos: oportunidades o negativos: riesgos)* que puedan afectar el logro de los objetivos | | | | | |
| 33. | La identificación de riesgos se realiza de manera continua | | | | | |
| 34. | El Departamento de Informática ha establecido indicadores de alarma. *(Definir en qué momento debe informarse una situación a los directivos partiendo del tiempo necesario para poner en marcha una acción cuando se* | | | | | |

| # | Descripción | FACTOR | SÍ | NO | NA | COMENTARIOS |
|---|---|---|---|---|---|---|
| | *sobrepasa un umbral establecido)* | | | | | |
| | **4) Evaluación de riesgos** | | | | | |
| 35. | El Departamento de Informática realiza evaluaciones de riesgos. | | | | | |
| 36. | Existe alguna metodología para la evaluación de los riesgos tecnológicos. | | | | | |
| 37. | Los riesgos se evalúan desde una doble perspectiva *(probabilidad e impacto).* | | | | | |
| 38. | Los riegos se evalúan con un doble enfoque *(riesgo inherente: aquel al que enfrenta la institución en ausencia de controles y riesgo residual: riesgo remanente posterior a la aplicación de controles).* | | | | | |
| 39. | La presentación de las evaluaciones de riesgos es clara. | | | | | |
| | **5) Respuesta a los riesgos** | | | | | |
| 40. | Una vez evaluados los riegos tecnológicos, el Departamento de Informática determina cómo responder a ellos *(por ejemplo evitar, reducir, compartir o aceptar el riesgo).* | | | | | |
| 41. | Al considerar la respuesta al riesgo, el Departamento de Informática evalúa su efecto sobre la probabilidad e impacto del riesgo. | | | | | |
| 42. | Al considerar la respuesta al riesgo, se selecciona la opción que sitúe el riesgo residual dentro de la tolerancia al riesgo establecida *(apetito de riesgo)* por la alta dirección. | | | | | |
| 43. | Al considerar la respuesta al riesgo, se realiza un análisis costo/beneficio del control. | | | | | |
| 44. | Posteriormente a la definición de la respuesta al riesgo, del Departamento de Informática identifica los controles necesarios para asegurar que las respuestas al riesgo se llevan a cabo adecuadamente. | | | | | |

| # | Descripción | FACTOR | SÍ | NO | NA | COMENTARIOS |
|---|---|---|---|---|---|---|
| 45. | El Departamento de Informática define políticas que ayuden a asegurar que se llevan a cabo las respuestas a los riesgos tecnológicos. | | | | | |
| 46. | El Departamento de Informática define procedimientos que ayuden a asegurar que se llevan a cabo las respuestas a los riesgos. | | | | | |
| 47. | El Departamento de Informática implementa mecanismos, con el fin de monitorear el cumplimiento de los controles que se establecieron, para asegurar que las respuestas al riesgo se llevan a cabo adecuadamente. | | | | | |
| | **6) Actividades de control** | | | | | |
| 48. | Existe una política de seguridad. | | | | | |
| 49. | Existe un área encargada que vele por la administración de la seguridad de TI. | | | | | |
| 50. | Existen planes de administración de seguridad de TI. | | | | | |
| 51. | Los usuarios y su actividad en sistemas de TI son identificados de manera única. | | | | | |
| 52. | Existe un procedimiento para el otorgamiento de los derechos de acceso. | | | | | |
| 53. | La identidad y los derechos de acceso se encuentran en un repositorio central. | | | | | |
| 54. | Se revisan periódicamente los derechos de acceso de los usuarios. | | | | | |
| 55. | Existe un procedimiento para la gestión de cuentas de usuario | | | | | |
| 56. | Se realizan pruebas de seguridad. | | | | | |
| 57. | Se detectan de manera oportuna las actividades inusuales o anormales. | | | | | |
| 58. | La seguridad de TI es monitoreada de manera | | | | | |

| # | Descripción | FACTOR | SÍ | NO | NA | COMENTARIOS |
|---|---|---|---|---|---|---|
| | proactiva. | | | | | |
| 59. | Se han definido los incidentes de seguridad. | | | | | |
| 60. | Se ha comunicado a las personas involucradas, las características de los incidentes de seguridad (descripción de lo que se considera un incidente de seguridad y su nivel de impacto, acciones específicas requeridas y las personas que necesitan ser notificadas) | | | | | |
| 61. | La gestión de incidentes de seguridad está integrada, con la gestión de incidentes de la institución. | | | | | |
| 62. | La gestión de incidentes de seguridad está integrada, con la gestión de problemas. | | | | | |
| 63. | La gestión de incidentes de seguridad está integrada, con la gestión de cambios. | | | | | |
| 64. | Existen mecanismos, para la protección de la tecnología de seguridad. | | | | | |
| 65. | Existen procedimientos para la administración de llaves criptográficas, que al menos incluyan generación, cambio, revocación, destrucción, distribución, certificación, almacenamiento, captura, uso y archivo. | | | | | |
| 66. | Se aplican medidas para la prevención, detección y corrección de *malware.* | | | | | |
| 67. | Se utilizan mecanismos de seguridad, para autorizar el acceso desde y hacia la red. | | | | | |
| 68. | Existen mecanismos para proteger el flujo de información, a través de la red. | | | | | |
| 69. | Existen políticas de seguridad, para el intercambio de datos sensibles (autenticidad de contenido, prueba de envío, prueba de recepción y no rechazo del origen). | | | | | |
| 70. | Se utilizan métodos de encriptación, para la transmisión de datos sensibles. | | | | | |

| # | Descripción | FACTOR | SÍ | NO | NA | COMENTARIOS |
|---|---|---|---|---|---|---|
| | **7) Información y comunicación** | | | | | |
| 71. | La Jefatura del Departamento de Informática comunica, las expectativas de comportamiento y responsabilidad de los colaboradores. | | | | | |
| 72. | La Jefatura del Departamento de Informática realiza comunicaciones, sobre la filosofía de gestión de riesgos tecnológicos, a todos los colaboradores del Departamento. Ejemplifique. | | | | | |
| 73. | Se realizan comunicaciones periódicas, sobre actualizaciones o creación de políticas. | | | | | |
| 74. | Se realizan actividades para la comunicación de la gestión de riesgos tecnológicos, en los programas de comunicación institucional. | | | | | |
| 75. | Los aspectos relacionados con la gestión de riesgos están disponibles, en un lugar de fácil acceso. | | | | | |
| | **8) Supervisión** | | | | | |
| 76. | Se realiza una supervisión permanente, de la eficacia de los componentes de la gestión de riesgos *(por ejemplo revisión de indicadores clave, revisión del rendimiento comparado contra los índices de riesgo, indicadores de alerta, entre otros).* | | | | | |
| 77. | Se realizan evaluaciones independientes de la gestión de riesgos (pueden ser realizadas por la auditoría interna, especialistas externos o una combinación). | | | | | |

| Nombre del auditor: | Fecha Inicio: | Fecha Fin: | Firma: |
|---|---|---|---|
| Ing. Magaly Fernández Marín | | | |
| Revisado por: MATI. Ana Patricia Porras | | | |

# 3. Informe de planificación preliminar

# 1. INTRODUCCIÓN

## 1.1. Origen del estudio

La evaluación se origina como parte de la práctica profesional para optar por el grado de maestría en Auditorías de Tecnologías de Información de la UCR.

## 1.2. Objetivo general

Evaluar el proceso “Garantizar la Seguridad de los Sistemas”, de acuerdo con la normativa aplicable a la institución, con el fin de emitir un criterio, dirigido a la administración, sobre el nivel de madurez alcanzado en este proceso.

## 1.3. Objetivos específicos

- Indagar con los dueños de proceso correspondientes, sobre las acciones que ha emprendido la institución, como parte de la implementación del proceso “Garantizar la Seguridad de los Sistemas”, con el fin de obtener un conocimiento de la situación actual y de los esfuerzos realizados, como parte de la implementación del proceso en estudio.

- Fundamentar, por medio de criterio de expertos, mejores prácticas, y el nivel de madurez para este proceso de acuerdo con el COBIT®, lo que se espera encontrar por parte de la institución, con el fin de obtener una base sobre la cual emitir los criterios correspondientes.

- Determinar el grado de madurez en el que se encuentra el proceso “Garantizar la Seguridad de los Sistemas”, con el fin de que las brechas identificadas se comuniquen a la administración y se asegure, de manera razonable, la confidencialidad, integridad y disponibilidad de la información de sus accionistas.

## 1.4. Alcance

Evaluar el nivel de madurez del proceso “Garantizar la Seguridad de los Sistemas” implementado en la institución, en el periodo que comprende entre setiembre 2012 y abril 2013; con base en el nivel de madurez de este proceso, propuesto en los Objetivos de Control para la Información y Tecnología Relacionada COBIT® 4.0, en cumplimiento al acuerdo SUGEF 1409.

### 1.5. Limitaciones

En relación con la confidencialidad de la información, de lo correspondiente a los resultados de análisis de vulnerabilidades, análisis de riesgos y algunos otros documentos considerados sensibles por la institución, se indicó expresamente que se debe mantener la confidencialidad de la información; por tanto, sólo se obtendrá acceso a esos documentos mediante revisiones en sitio. Asimismo, no es posible la aplicación de herramientas tecnológicas, para la elaboración de pruebas de seguridad.

En concordancia con el tema de la confidencialidad, para efectos de la elaboración de este documento se ha protegido el nombre real de la institución, de ahí que se haga referencia a ella como “CDA”.

## 2. Resumen del conocimiento del entorno

### 2.1. Sobre la entidad

CDA, es una institución privada que administra fondos públicos con acceso a información confidencial de alrededor de 100.000 accionistas y de los movimientos económicos que estos realizan en su entidad y fue creada por la Ley N° 12 del 13 de octubre de 1944 con la finalidad de, entre otras cosas, mejorar la calidad de vida de sus accionistas, quienes pueden ser:

- Empleados de la institución.
- Empleados del Ministerio de Educación Pública.
- Jubilados o pensionados del Ministerio de Educación Pública.

Entre los servicios que ofrece se encuentran los siguientes:

- Préstamos personales.
- Préstamos de vivienda.
- Préstamos de desarrollo.
- Tarjetas de crédito y débito.
- Asistencias.
- Planes de ahorro.
- Comercialización de Seguros.

Actualmente, la institución ofrece estos servicios a sus accionistas, desde sus oficinas centrales o bien desde las oficinas desconcentradas ubicadas en Liberia, Santa Cruz, San Carlos, Limón, Pérez Zeledón, Ciudad Neily, Puntarenas y Cartago.

La institución tiene 68 años de ser dirigida por educadores, su Junta Directiva está conformada por cinco propietarios y tres suplentes que se eligen cada cuatro años y representan a diferentes instituciones gremiales del sector de la educación.

La administración de la institución está formada por un Gerente y un Subgerente que son nombrados por la Junta Directiva cada dos años.

## 2.2. Sobre las operaciones de TI:

### 2.2.1. Estructura organizativa

La institución cuenta con un Departamento de TI que está formado por las siguientes unidades:

- Desarrollo y mantenimiento de sistemas.
- Infocomunicaciones y servicios colaborativos.
- Soporte técnico.
- Contraloría de servicios informáticos.
- Administración de proyectos.

### 2.2.2. Leyes, regulaciones y marco de control que le aplica al Departamento de TI

El marco de control adoptado para tecnologías de información es COBIT versión 4.0 considerando sus cuatro dominios:

- Planear y Organizar.
- Adquirir e Implementar.
- Entregar y Dar Soporte.
- Monitorear y Evaluar.

### 2.2.3. Disposiciones del ente regulador en cuanto a tecnologías de información

La institución es una entidad supervisada por la Superintendencia General de Entidades Financieras, la cual, mediante el acuerdo SUGEF 1409 “REGLAMENTO SOBRE LA GESTIÓN DE LA TECNOLOGÍA DE INFORMACIÓN” establece que las áreas de TI deben implementar un marco para la gestión de TI que considere lo siguiente:

> *"El marco para la gestión de TI debe ser congruente con el perfil tecnológico de la entidad, la naturaleza y la complejidad de sus operaciones y contar con la aprobación de la Junta Directiva o autoridad equivalente.*
>
> *Sin detrimento de lo anterior, el marco para la gestión de TI debe incluir al menos los procesos identificados como obligatorios en el anexo 1 de este reglamento"*

Siendo los 17 procesos los siguientes:

- PO9 Evaluar y administrar los riesgos de TI.
- PO10 Administrar proyectos.
- AI6 Administración de cambios.
- DS2 Administrar los servicios de terceros.
- DS4 Garantizar la continuidad del servicio.
- DS5 Garantizar la seguridad de los sistemas.
- DS11 Administración de los datos.
- ME2 Monitorear y evaluar el control interno.
- PO1 Definir un plan estratégico de TI.
- PO3 Determinar la dirección tecnológica.
- PO5 Administrar la inversión en TI.
- AI3 Adquirir y mantener infraestructura tecnológica.
- AI5 Adquirir recursos de TI.
- DS3 Administrar el desempeño y la capacidad.
- DS9 Administrar la configuración.
- DS10 Administrar los problemas.
- DS12 Administrar el ambiente físico.

## 2.3. Sobre el proceso de seguridad de la información

### 2.3.1. Sobre la creación de la Oficina de Seguridad de Información

Como parte de la implementación del acuerdo SUGEF 1409 y el proceso COBIT DS5 "Garantizar la Seguridad de los Sistemas" la Junta Directiva de CDA, en sesión N° 6469 celebrada el 18 de noviembre del 2010, acordó aprobar la propuesta de implementar la Oficina de Seguridad Informática la cual rinde cuentas directamente a la Gerencia y está conformada por los siguientes puestos:

- Coordinador.

- Analista de seguridad en redes de datos y comunicaciones.
- Analista gestor de riesgos informáticos.
- Analista en seguridad de la infraestructura y servicios colaborativos.
- Analista en seguridad de arquitectura de datos y sistemas.

### 2.3.2. Marcos de referencia utilizados

Para la implementación del proceso DS5 “Garantizar la Seguridad de los Sistemas”, el área de Seguridad Informática, además del COBIT, se está apoyando con las mejores prácticas de la norma ISO 27002; sin embargo, para efectos de la evaluación, no se evaluará la norma ISO 27002.

| Criterios por evaluar |
|---|
| **1. Conocimientos de COBIT. Proceso DS5** |
| DS5.1 Administración de la seguridad de TI. |
| DS5.2 Plan de seguridad de TI. |
| DS5.3 Administración de identidad. |
| DS5.4 Administración de cuentas del usuario. |
| DS5.5 Pruebas, vigilancia y monitoreo de la seguridad. |
| DS5.6 Definición de incidente de seguridad. |
| DS5.7 Protección de la tecnología de seguridad. |
| DS5.8 Administración de llaves criptográficas. |
| DS5.9 Prevención, detección y corrección de *software* malicioso. |
| DS5.10 Seguridad de la red. |
| DS5.11 Intercambio de datos sensitivos. |
| **2. Guía de aseguramiento “IT Assurance guide using COBIT”** |
| **3. Acuerdo SUGEF 14-09.** |

Adicionalmente, se solicitó a la institución la normativa vigente (políticas, procedimientos) propia del proceso de gestión de la seguridad, existente en la institución.

### 2.3.3. Madurez del proceso de Seguridad

De acuerdo con las entrevistas y aplicación de herramientas (basada en el nivel de madurez 3 según COBIT), para obtener un conocimiento de la situación actual, se obtuvo lo siguiente:

- La Oficina de Seguridad Informática realiza esfuerzos para concienciar a los usuarios de la institución. No obstante, esto no incluye a los empleados de proveedores.

- Está en proceso de aprobación, una normativa relacionada con empleados de proveedores, involucrados de alguna manera con la seguridad de la información de la organización.

- La gerencia reconoce la necesidad de la seguridad para TI, y participa en reuniones de comité de seguridad.

  La Junta Directiva aprueba suficientes recursos para la inversión en seguridad, también aprobó el Programa de Seguridad, la creación de la Oficina de Seguridad Informática, nuevos puestos, el Comité de Seguridad y las políticas de seguridad, entre otros.

- Se ha establecido una política de seguridad y ha sido comunicada a todos los usuarios. La política se actualiza, al menos una vez al año.

- Se ha establecido procedimientos relacionados con la seguridad y han sido comunicados a todos los usuarios. Se actualizan al menos una vez al año.

- Las responsabilidades de la seguridad de TI asignadas, se comunicaron a los involucrados, están documentadas en las funciones de puesto y las personas a las que le fueron asignadas poseen las competencias necesarias para su desarrollo. En la definición de las responsabilidades se toman en cuenta los siguientes roles:

  - Junta Directiva.
  - Comité de Seguridad.
  - Dueños de la información.
  - Custodios de la información.
  - TI.
  - Oficina de Seguridad Informática.
  - Auditoría interna.
  - Usuarios finales.

- Existe un Plan de Seguridad formalmente aprobado que se comunicó a todos los involucrados y se actualiza al menos una vez por año.

- Se generan diversos tipos de informes, por ejemplo de estudios de vulnerabilidades, informes solicitados por la Gerencia, de pruebas y otros. Los informes se comunican a los involucrados y se generan y da seguimiento a los planes de acción correspondientes, en caso de que aplique.

- Se cuenta con un cronograma para la ejecución de pruebas de seguridad y estas son comunicadas previamente a los involucrados. Con base en los resultados de

las pruebas de seguridad, se establecen análisis de brechas (planes de acción). El cronograma se actualiza anualmente.

- Anualmente cada área elabora el plan de capacitación para el siguiente año, con base en las necesidades de capacitación.

  En cuanto a la Oficina de Seguridad Informática, esta elaboró la política sobre capacitación de seguridad, cuyo objetivo es mantener informados a los usuarios y a las personas involucradas sobre las políticas, procedimientos y controles de seguridad establecidos por TI.

No obstante lo anterior, se encontró incumplimiento en los siguientes aspectos:

- Para las campañas de concienciación de seguridad, no se toman en cuenta los empleados de proveedores que están involucrados, de alguna manera, con la seguridad de la información organizacional.

  No se informa a los proveedores sobre los requerimientos específicos de seguridad de la empresa, establecidos en la política de seguridad.

  Al respecto, el entrevistado indicó que fue presentada y se aprobó una propuesta sobre la implementación de mecanismos contractuales, que contempla todo lo anterior. Actualmente está pendiente de implementación.

- Los usuarios no identifican incidentes de seguridad, de modo que tampoco ha sido posible realizar comparaciones, para determinar si se ha disminuido la cantidad de incidentes de seguridad.

- No se evalúa el cumplimiento de los procedimientos relacionados con seguridad.

- No se realizan reportes de desempeño del proceso de seguridad. Sin embargo, mensualmente se expone el PAO a la alta administración.

**2.4. Sobre el sistema de control interno**

En principio se elaboró un cuestionario de control interno, basado en los componentes del Informe COSO ERM, a saber:

1. Ambiente interno.
2. Establecimiento de objetivos.
3. Identificación de eventos.
4. Evaluación de riesgos.

5. Respuesta a los riesgos.
6. Actividades de control.
7. Información y comunicación.
8. Supervisión.
9. Roles y responsabilidades.

Según el análisis efectuado por esta auditoría, a partir del cuestionario contestado por la Administración, se obtuvo los siguientes resultados:

**Tabla 1: Resultados de la evaluación de control interno**

| Componente | Comentarios |
|---|---|
| Ambiente interno. | • La alta dirección aprueba políticas para la gestión del riesgo tecnológico y ha establecido el apetito de riesgo. El Departamento de TI ha establecido una estrategia para la gestión de riesgos y esta es apoyada por la jefatura.<br>• Existe un código de ética actualizado que es del conocimiento de los colaboradores, está publicado en la intranet y anualmente se realizan actividades de sensibilización en aspectos relacionados con él.<br>• Se han definido valores institucionales y frecuentemente, mediante reuniones generales, se insta a los colaboradores a que los sigan ejemplificando. La Jefatura de TI también promueve la aplicación de estos, por medio de reuniones departamentales.<br>• Se elaboran planes de capacitación, en función de las necesidades al respecto, de acuerdo con el puesto; sin embargo, no se ejecutan en un 100%. Según los comentarios de la administración, en años anteriores se logró cumplir solo con el 85%, lo cual, básicamente, se debe a que algunos cursos ofrecidos no contienen el temario requerido o bien son cancelados por las empresas que los imparten.<br>• El Departamento de TI está formalmente definido en el organigrama de la institución y se encuentra actualizado.<br>• La alta dirección ha establecido mecanismos para la rendición de cuentas, mediante la presentación mensual de informes que en principio son dirigidos a la Unidad de Estrategia y Procesos para posteriormente llevarlos a diversos comités y Junta Directiva. |
| Establecimiento de objetivos. | • Los objetivos estratégicos institucionales están establecidos.<br>• En función de los objetivos estratégicos institucionales el Departamento de TI elabora el Plan Estratégico de TI y el Plan Operativo que está formado por objetivos de contribución que apoyan el cumplimiento del objetivo estratégico que les corresponde. Para esos objetivos de contribución se identifican |

| Componente | Comentarios |
|---|---|
| | los riesgos y se definen las acciones contingentes.<br>• Se han establecido mecanismos para informar sobre el cumplimiento de los objetivos operativos.<br>• Se establecen los niveles de riesgo, de las nuevas iniciativas que la institución está preparada para asumir. Estas iniciativas son evaluadas por la Unidad de Administración Integral de Riesgo y el Área de Seguridad de la Información. |
| Identificación de eventos. | • Existe una metodología para la identificación de riesgos utilizada por el Departamento de TI.<br>• No se tienen definidos indicadores de alarma que establezcan en qué momento debe informarse una situación a los directivos, partiendo del tiempo necesario para poner en marcha una acción, cuando se sobrepasa un umbral establecido. |
| Evaluación de riesgos | • La evaluación de riesgos tecnológicos fue iniciada a mediados del 2012 y se realiza desde una perspectiva de probabilidad e impacto, no así con un doble enfoque (de riesgo inherente y riesgo residual).<br>• En lo referente a objetivos estratégicos y de contribución se evalúan los riesgos de manera frecuente. |
| Actividades de control. | • En lo referente a las actividades de control relacionadas con el objeto de estudio:<br>○ Existe una política de seguridad.<br>○ Existe un área encargada de velar por la administración de la seguridad de TI.<br>○ Existen planes de administración de seguridad de TI.<br>○ Los usuarios y su actividad en sistemas de TI son identificados de manera única.<br>○ Existe un procedimiento para el otorgamiento de los derechos de acceso.<br>○ La identidad y los derechos de acceso no se encuentran en un repositorio central.<br>○ Se revisan periódicamente los derechos de acceso de los usuarios; sin embargo, se realiza cuando la jefatura inmediata de los usuarios indica sobre algún cambio y cuando se comunica sobre una renuncia, despido, vacaciones e incapacidad.<br>○ Existe un procedimiento para la gestión de cuentas de usuario.<br>○ Se realizan pruebas de seguridad.<br>○ No se detectan, de manera oportuna, las actividades inusuales o anormales.<br>○ La seguridad de TI es monitoreada de manera proactiva por medio de estudios de vulnerabilidades; sin embargo, esto se realiza de manera anual. |

| Componente | Comentarios |
|---|---|
| | ○ Se han definido los incidentes de seguridad, pero se han registrado pocos, se está en labor de culturización.<br>○ Las características de los incidentes de seguridad (descripción de lo que se considera un incidente de seguridad y su nivel de impacto, acciones específicas requeridas y las personas que necesitan ser notificadas) no han sido definidas ni comunicadas.<br>○ La gestión de incidentes de seguridad está integrada, de manera parcial, a la gestión de incidentes, problemas y cambios de la institución. Se está trabajando en un proceso de mejora de la gestión de incidentes de seguridad.<br>○ Existen mecanismos para la protección de la tecnología de seguridad.<br>○ Existe un procedimiento para la administración de llaves criptográficas, pero no es completo.<br>○ Se aplican medidas para la prevención, detección y corrección de *malware.*<br>○ Existen mecanismos para proteger el flujo de información a través de la red.<br>○ Existen políticas de seguridad para el intercambio de datos sensibles.<br>○ No se utilizan métodos de encriptación para la transmisión de datos sensibles, fuera de la institución. |
| Información y comunicación. | • La Jefatura del Departamento de Informática comunica las expectativas de comportamiento y responsabilidad de los colaboradores; no obstante, no realiza comunicaciones sobre la filosofía de gestión de riesgos tecnológicos a todos los colaboradores del Departamento.<br>• Se realizan comunicaciones periódicas, por medio del correo electrónico, sobre actualizaciones o creación de políticas.<br>• Los aspectos relacionados con la gestión de riesgos están disponibles en un lugar de fácil acceso. |
| Supervisión. | • La Unidad de Administración Integral de Riesgo realiza una supervisión permanente, de la eficacia de los componentes de la gestión de riesgos<br>• Las auditorías, interna y externa, realizan evaluaciones independientes de la gestión de riesgos. |
| Roles y responsabilidades. | • Los roles y responsabilidades están formalmente definidos en el Manual de Puestos. |

**Sobre la evaluación de riesgos del proceso de seguridad**

En principio se solicitó la evaluación de riesgos del proceso de seguridad, a la administración, mediante correo electrónico enviado el día 01/02/2013.

Según el análisis efectuado por esta auditoría, a partir de la información recibida, se obtuvieron los siguientes resultados:

- Se han identificado 18 riesgos del proceso de seguridad de la información de la siguiente manera:

**Tabla 2: Resultados de la evaluación de riesgos**

| Id | Riesgo | Vulnerabilidad | Amenaza |
|---|---|---|---|
| **RTI-001** | Incumplimiento regulatorio. | Ausencia de un plan estratégico, para la seguridad de la información. | No contar con una alineación de la estrategia de la institución, con la estrategia de seguridad de la información |
| **RTI-002** | Pérdida de la información e incumplimiento regulatorio. | No se cuenta con toda la información protegida, según la clasificación de datos. | No brindar las medidas de seguridad necesarias, a la información de la institución. |
| **RTI-003** | Pérdida de la información, continuidad de negocio e incumplimiento regulatorio. | Exposición de amenazas, no incluidas en la estrategia de la institución. | Interrupciones inesperadas en las operaciones, que provoquen pérdidas al negocio. |
| **RTI-004** | Pérdida de la información e incumplimiento regulatorio. | Medidas de seguridad comprometidas por los interesados o usuarios. | Interrupciones inesperadas en las operaciones, que provoquen pérdidas al negocio. |
| **RTI-005** | Incumplimiento regulatorio y continuidad de negocio. | Cambios no autorizados por la Unidad de Seguridad de la Información en *hardware* o *software.* | Incumplimiento de mejores prácticas a nivel de seguridad de la información en los sistemas o aplicaciones de la institución. |
| **RTI-006** | Pérdida de la información, continuidad de negocio e incumplimiento | Debilidades en la gestión de acceso, de acuerdo con los requisitos de negocio, comprometiendo la seguridad de los sistemas críticos de negocio. | Incumplimiento de mejores prácticas en cuanto a seguridad de la información, en los sistemas o |

| Id | Riesgo | Vulnerabilidad | Amenaza |
|---|---|---|---|
| | regulatorio. | | aplicaciones de la institución. |
| **RTI-007** | Pérdida de la información, reprocesos e incumplimiento regulatorio. | Existencia de algunos sistemas sin requerimientos de seguridad (por ejemplo autenticación con el directorio activo). | Incumplimiento de mejores prácticas en cuanto a seguridad de la información, en los sistemas o aplicaciones de la institución. |
| **RTI-008** | Pérdida de la información, pérdidas por fraude e incumplimiento regulatorio. | Fallas en la segregación de funciones, en relación con los sistemas. | Incumplimiento de mejores prácticas respecto a seguridad de la información, en los sistemas o aplicaciones de la institución. |
| **RTI-009** | Pérdida de la información, pérdidas por fraude e incumplimiento regulatorio. | Ausencia de un proceso formal y documentado para la administración de la identidad. | Incumplimiento de mejores prácticas de seguridad de la información, en los sistemas o aplicaciones de la institución. |
| **RTI-010** | Pérdida de la información, pérdidas por fraude e incumplimiento regulatorio. | Ausencia de un proceso formal y documentado, para la administración de cuentas de usuario. | Incumplimiento de mejores prácticas de seguridad de la información, en los sistemas o aplicaciones de la institución. |
| **RTI-011** | Pérdida de la información e incumplimiento regulatorio. | Incumplimiento de la política de seguridad, por parte de los usuarios. | Incumplimiento de mejores prácticas de seguridad de la información, en los sistemas o aplicaciones de la institución. |
| **RTI-012** | Pérdida de la información, pérdidas por fraude e incumplimiento regulatorio. | Eliminación o bloqueo de cuentas de usuario de manera no oportuna. | Incumplimiento de mejores prácticas de seguridad de la información, en los sistemas o aplicaciones de la |

| Id | Riesgo | Vulnerabilidad | Amenaza |
|---|---|---|---|
| | | | institución. |
| **RTI-013** | Pérdida de la información e incumplimiento regulatorio. | Mal uso de las cuentas por parte de los usuarios. | Incumplimiento de mejores prácticas de seguridad de la información, en los sistemas o aplicaciones de la institución. |
| **RTI-014** | Pérdida de la información, pérdida por fraudes, continuidad de negocio e incumplimiento regulatorio. | Ausencia de un procedimiento formal y documentado, para la administración de incidentes de seguridad. | Incidentes de seguridad a los que no se brinda un debido tratamiento. |
| **RTI-015** | Pérdida de la información e incumplimiento regulatorio. | No contar con una cultura organizacional, para la clasificación de la información. | Exposición de la información. |
| **RTI-016** | Pérdida de la información e incumplimiento regulatorio. | Ausencia de un procedimiento formal y documentado, para la administración de llaves criptográficas. | Incumplimiento de mejores prácticas de seguridad de la información, en los sistemas o aplicaciones de la institución. |
| **RTI-017** | Pérdida de la información, pérdidas por fraude, continuidad del negocio e incumplimiento regulatorio. | Sistemas y datos propensos a ataques de virus. | Contaminación de *software* malicioso (virus, troyanos y otros), en las estaciones de trabajo. |
| **RTI-018** | Pérdida de la información, continuidad del negocio e incumplimiento regulatorio. | Arquitectura de red comprometida respecto a seguridad. | *Spam* o propagación de virus informáticos. |

Los riesgos han sido evaluados por la administración, de la siguiente manera:

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| Probabilidad | 5 | Muy probable | | | | | |
| | 4 | Bastante probable | | | | | |
| | 3 | Probable | | RTI-001<br>RTI-002<br>RTI-004<br>RTI-005<br>RTI-006<br>RTI-007<br>RTI-008<br>RTI-009<br>RTI-010<br>RTI-011<br>RTI-012<br>RTI-013<br>RTI-015<br>RTI-016<br>RTI-017 | RTI-003<br>RTI-014<br>RTI-018 | | |
| | 2 | Poco probable | | | | | |
| | 1 | Improbable | | | | | |
| | | | Muy bajo | Bajo | Moderado | Alto | Muy alto |
| | | | 1 | 2 | 3 | 4 | 5 |
| | | | Impacto | | | | |

## 3. Conclusiones

Se identifican debilidades en los siguientes componentes del control interno:

- ***Identificación de eventos***: No se dispone de indicadores de alarma definidos, que establezcan en qué momento debe informarse una situación a los directivos, partiendo del tiempo necesario, para poner en marcha una acción, cuando se sobrepasa un umbral establecido. Sin embargo, una vez efectuada la evaluación del riesgos y analizada en el Comité de Riesgos, se presentan los informes ante Junta Directiva y es en esa instancia, donde se decide asumir el riesgo que puede afectar a la institución o no.

- ***Evaluación de riesgos***: La evaluación de riesgos tecnológicos fue iniciada a mediados del 2012 y no ha sido finalizada, se realiza desde una perspectiva de

probabilidad e impacto, no así con un doble enfoque (de riesgo inherente y riesgo residual).

- ***Información y comunicación***: La Jefatura del Departamento de TI no brinda comunicaciones, sobre la filosofía de gestión de riesgos tecnológicos, a todos los colaboradores del Departamento.

- ***Actividades de control:*** Se identificaron debilidades en los siguientes procesos:

  ***Identidad***

  - La identidad y los derechos de acceso no se encuentran en un repositorio central.

  ***Gestión de cuentas***

  - Se revisan periódicamente los derechos de acceso de los usuarios; sin embargo, es una actividad que se realiza cuando la jefatura inmediata de los usuarios indica sobre algún cambio y cuando se comunica sobre una renuncia, despido, vacaciones e incapacidad.

  ***Pruebas, vigilancia y monitoreo de la seguridad***

  - No se detectan, de manera oportuna, las actividades inusuales o anormales.
  - La seguridad de TI es monitoreada de manera proactiva por medio de estudios de vulnerabilidades; pero se realiza anualmente.

  ***Incidentes de seguridad***

  - Se han definido los incidentes de seguridad; sin embargo, se han registrado pocos, se está en labor de culturización.
  - Las características de los incidentes de seguridad (descripción de lo que se considera un incidente de seguridad y su nivel de impacto, acciones específicas requeridas y las personas que necesitan ser notificadas) no han sido definidas ni comunicadas.
  - La gestión de incidentes de seguridad está integrada de manera parcial con la gestión de incidentes, problemas y cambios de la institución. Se está trabajando en un proceso de mejora de la gestión de incidentes de seguridad.

  ***Administración de llaves criptográficas***

  - Existe un procedimiento para la administración de llaves criptográficas, peros no es completo.

  ***Intercambio de datos sensitivos***

- No se utilizan métodos de encriptación para la transmisión de datos sensibles fuera de la institución

Al realizar una comparación de los riesgos identificados por la Administración, y las debilidades en el componente de actividades de control, se observa lo siguiente:

**Tabla 3: Comparación riesgos y actividades de control**

| Riesgo | Actividad de control de acuerdo con cuestionario de control interno |
|---|---|
| • RTI-014 Ausencia de un procedimiento formal y documentado para la administración de incidentes de seguridad. | Las características de los incidentes de seguridad no han sido definidas ni comunicadas.<br>La gestión de incidentes de seguridad está integrada de manera parcial, con la gestión de incidentes, problemas y cambios de la institución. |
| • RTI-006 Debilidades en la gestión de acceso de acuerdo con los requisitos de negocio, comprometiendo la seguridad de los sistemas críticos de negocio.<br>• RTI-010 Ausencia de un proceso formal y documentado para la administración de cuentas de usuario. | La identidad y los derechos de acceso no se encuentran en un repositorio central.<br>Se revisan periódicamente los derechos de acceso de los usuarios; sin embargo, es una actividad que se realiza cuando la jefatura inmediata de los usuarios indica sobre algún cambio y cuando se comunica sobre una renuncia, despido, vacaciones e incapacidad |
| • RTI-016 Ausencia de un procedimiento formal y documentado para la administración de llaves criptográficas. | Existe un procedimiento para la administración de llaves criptográficas, pero no es completo. |
| • RTI-019 Exposición de información sensible. | No se utilizan métodos de encriptación, para la transmisión de datos sensibles fuera de la institución. |
| • RTI-013 Mal uso de las cuentas por parte de los usuarios. | No se detectan, de manera oportuna, las actividades inusuales o anormales. |

- Las debilidades identificadas en los componentes: identificación de eventos, evaluación de riesgos, información y comunicación serán comunicadas a la Administración; no obstante, están fuera del alcance de este estudio, por lo que no serán objeto de evaluación en la etapa de ejecución.

- Los esfuerzos de esta evaluación se dirigirán a los objetivos de control del proceso DS5 en general, dando mayor énfasis en:
  - DS5.3 Administración de identidad.

- DS5.4 Administración de cuentas de usuario.
- DS5.5 Pruebas, vigilancia y monitoreo de la seguridad.
- DS5.6 Definición de incidente de seguridad.
- DS5.8 Administración de llaves criptográficas.
- DS5.11 Intercambio de datos sensitivos.

# 4. PLANIFICACIÓN DETALLADA

Se elabora guía de las actividades por realizar, en dicha etapa, de la siguiente manera:

| Planificación Detallada | Referencia |
|---|---|
| Desarrolle las herramientas para comprobar y verificar los controles con base en lo concluido en la etapa de planificación preliminar. | PD1 |
| Elabore programa de ejecución. | PD2 |
| Elabore informe de planificación detallada. | PD3 |

# 5. anexos

## 5.1. Programa de ejecución

| # | Procedimiento | Criterio utilizado | Ref. |
|---|---|---|---|
| 1 | Solicite el organigrama actualizado de la institución y el plan estratégico institucional. Consulte si existen planes de seguridad donde se evidencie la alineación con los requerimientos de negocio, evalúe mediante el formulario de cumplimiento "***FORM-DS5.1 Administración de la seguridad de TI"***, y la matriz "***SUGEF-DS5***". Documente sus resultados. | DS5.1 Administración de la Seguridad de TI Administrar la seguridad de TI al nivel más alto apropiado dentro de la organización, de manera que las acciones de administración de la seguridad estén en el nivel de los requerimientos del negocio.<br><br>Guía de aseguramiento usando COBIT, extracto DS5.1.<br><br>Prácticas de control, extracto DS5.1 | **PE1** |
| 2 | Consulte si se ha elaborado un plan de seguridad de TI, de ser así, solicítelo y evalúe mediante el formulario de cumplimiento "***FORM-DS5.2 Plan de Seguridad de TI"*** y la matriz "***SUGEF-DS5***". Documente sus resultados. | DS5.2 Plan de seguridad de TI: Trasladar los requerimientos de información del negocio, la configuración de TI, los planes de acción del riesgo de la información y la cultura sobre la seguridad en la información a un plan global de seguridad de TI. El plan se implementa en políticas y procedimientos de seguridad, en conjunto con inversiones apropiadas en servicios, personal, *software* y *hardware*. Las políticas y procedimientos de seguridad se comunican a los interesados y a los usuarios. | **PE2** |

| # | Procedimiento | Criterio utilizado | Ref. |
|---|---|---|---|
| | | Guía de aseguramiento usando COBIT, extracto DS5.2<br>Prácticas de control, extracto DS5.2 | |
| **3** | Consulte al Jefe de la Unidad de seguridad de la información sobre cómo se está gestionando el proceso de identidad en la institución. Aplique el cuestionario de cumplimiento "***FORM-DS5.3 Administración de Identidad"*** y la matriz "***SUGEF-DS5***". Documente sus resultados. | DS5.3 Administración de identidad Todos los usuarios (internos, externos y temporales) y su actividad en sistemas de TI (aplicación de negocio, operación del sistema, desarrollo y mantenimiento) deben ser identificables de manera única. Los derechos de acceso del usuario a sistemas y datos deben estar alineados con necesidades de negocio definidas y documentadas y con requerimientos de trabajo. Los derechos de acceso del usuario son solicitados por la gerencia del usuario, aprobados por el responsable del sistema, e implementado por la persona responsable de la seguridad. Las identidades del usuario y los derechos de acceso se mantienen en un repositorio central. Se implementan y se mantienen actualizadas medidas técnicas y procedimientos rentables, para establecer la identificación del usuario, realizar la autenticación y habilitar los derechos de acceso.<br><br>Guía de aseguramiento usando COBIT, extracto DS5.3<br>Prácticas de control, extracto DS5.3 | PE3 |
| **4** | Solicite los procedimientos formales sobre la administración de cuentas y evalúe mediante el formulario "***FORM-DS5.4 Administración de Cuentas de Usuario"*** y la matriz "***SUGEF-DS5***". Documente sus resultados. | DS5.4 Administración de cuentas del usuario Garantizar que la solicitud, establecimiento, emisión, suspensión, modificación y cierre de cuentas de usuario y de los privilegios relacionados, sean tomados en cuenta por la gerencia de cuentas de usuario. Debe incluirse un procedimiento que describa al responsable de los datos o del sistema, cómo otorgar los privilegios de acceso. Estos procedimientos deben aplicar para todos los usuarios, incluyendo administradores (usuarios privilegiados), usuarios externos e internos, para casos normales y de emergencia. Los derechos y obligaciones relacionados con el acceso a los sistemas e información de la empresa son acordados contractualmente para todos los tipos de usuarios. La gerencia debe llevar a cabo una revisión regular de todas las cuentas y los privilegios asociados.<br><br>Guía de aseguramiento usando COBIT, extracto DS5.4<br>Prácticas de control, extracto DS5.4 | PE4 |
| **5** | Solicite el plan que detalla la realización de pruebas, vigilancia y monitoreo de actividades inusuales, que atenten a la seguridad de TI; indague sobre los | DS5.5 Pruebas, vigilancia y monitoreo de la seguridad: Garantizar que la implementación de la seguridad en TI sea probada y monitoreada de forma pro-activa. La seguridad en TI debe ser reacreditada periódicamente | PE5 |

| # | Procedimiento | Criterio utilizado | Ref. |
|---|---|---|---|
| | resultados de dichas pruebas aplicadas el último año y verifique si los resultados han sido contemplados en planes de acción y si se ejecutan según lo establecido. Aplique cuestionario de cumplimiento "***FORM-DS5.5 Pruebas, Vigilancia y Monitoreo de la Seguridad"*** y la matriz "***SUGEF-DS5***". Documente sus resultados. | para garantizar que se mantiene el nivel seguridad aprobado. Una función de ingreso al sistema (*logging*) y de monitoreo permite la detección oportuna de actividades inusuales o anormales que pueden requerir atención. El acceso a la información de ingreso al sistema está alineado con los requerimientos del negocio en términos de requerimientos de retención y de derechos de acceso.<br><br>Guía de aseguramiento usando COBIT, extracto DS5.5<br><br>Prácticas de control, extracto DS5.5 | |
| **6** | Consulte al Jefe de la Unidad de seguridad de la información, sobre cómo se está gestionando la gestión de incidentes; indague acerca de la existencia de documentación formal sobre la clasificación y tratamiento de incidentes y problemas de seguridad, evalúe mediante el formulario de cumplimiento "***FORM-DS5.6 Definición de Incidentes de Seguridad"*** y la matriz "***SUGEF-DS5***". Documente sus resultados. | DS5.6 Definición de incidente de seguridad: Garantizar que las características de los posibles incidentes de seguridad sean definidas y comunicadas de forma clara, de manera que los problemas de seguridad sean atendidos apropiadamente por medio del proceso de administración de problemas o incidentes. Las características incluyen una descripción de lo que se considera un incidente de seguridad y su nivel de impacto. Un número limitado de niveles de impacto se definen para cada incidente, se identifican las acciones específicas requeridas y las personas que necesitan ser notificadas.<br><br>Guía de aseguramiento usando COBIT, extracto DS5.6.<br><br>Prácticas de control, extracto DS5.6. | PE6 |
| **7** | Consulte con el encargado de seguridad sobre los mecanismos para la protección de la Tecnología de Seguridad, aplique cuestionario de cumplimiento "***FORM-DS5.7 Protección de la tecnología de seguridad"*** y la matriz "***SUGEF-DS5***". Documente sus resultados. | DS5.7 Protección de la tecnología de seguridad: Garantizar que la tecnología importante relacionada con la seguridad no sea susceptible de sabotaje y que la documentación de seguridad no se divulgue de forma innecesaria, es decir, que mantenga un perfil bajo. Sin embargo, no permitir que la seguridad de los sistemas dependa, de la confidencialidad de las especificaciones de seguridad.<br><br>Guía de aseguramiento usando COBIT, extracto DS5.7.<br><br>Prácticas de control, extracto DS5.7. | PE7 |
| **8** | Solicite las políticas y procedimientos relacionados con la administración de llaves criptográficas y aplique cuestionario de cumplimiento "***FORM-DS5.8 Administración de llaves criptográficas"*** y la matriz "***SUGEF-*** | DS5.8 Administración de llaves criptográficas: Determinar qué las políticas y procedimientos para organizar la generación, cambio, revocación, destrucción, distribución, certificación, almacenamiento, captura, uso y archivo de llaves criptográficas están implantadas, para garantizar la protección de las llaves | PE8 |

| # | Procedimiento | Criterio utilizado | Ref. |
|---|---|---|---|
| | ***DS5***". Documente sus resultados. | contra modificaciones y divulgación no autorizadas.<br><br>Guía de aseguramiento usando COBIT, extracto DS5.8.<br>Prácticas de control, extracto DS5.8. | |
| **9** | Consulte a los involucrados sobre las medidas para la prevención, detección y corrección de *malware*, aplique cuestionario de cumplimiento "***FORM-DS5.9 Protección, Detección y Corrección de Software Malicioso"*** y la matriz "***SUGEF-DS5***". Documente sus resultados. | DS5.9 Prevención, detección y corrección de *software* malicioso: Garantizar que se cuente con medidas de prevención, detección y corrección (en especial contar con parches de seguridad y control de virus actualizados) a lo largo de toda la organización, para proteger los sistemas de información y la tecnología contra *software* malicioso (virus, gusanos, *spyware*, correo basura, *software* fraudulento desarrollado internamente, etc.).<br><br>Guía de aseguramiento usando COBIT, extracto DS5.9.<br>Prácticas de control, extracto DS5.9. | PE9 |
| **10** | Consulte a los involucrados sobre los mecanismos de control para garantizar la seguridad de la red. Aplique cuestionario de cumplimiento "***FORM-DS5.10 Seguridad en la red"*** y la matriz "***SUGEF-DS5***". Documente sus resultados. | DS5.10 Seguridad de la red: Garantizar que se utilizan técnicas de seguridad y procedimientos de administración asociados (por ejemplo, *firewalls,* dispositivos de seguridad, segmentación de redes, y detección de intrusos) para autorizar acceso y controlar los flujos de información desde y hacia las redes.<br><br>Guía de aseguramiento usando COBIT, extracto DS5.10.<br>Prácticas de control, extracto DS5.10. | PE10 |
| **11** | Consulte acerca de la existencia de procesos que contemplen intercambio de datos sensitivos; de existir, aplique el formulario de cumplimiento "***FORM-DS5.11 Intercambio de datos sensitivos"*** y la matriz "***SUGEF-DS5***". Documente sus resultados. | DS5.11 Intercambio de datos sensitivos: Garantizar que las transacciones de datos sensibles sean intercambiadas solamente a través de una ruta o medio confiable, con controles para brindar autenticidad de contenido, prueba de envío, prueba de recepción y no rechazo del origen.<br><br>Guía de aseguramiento usando COBIT, extracto DS5.11.<br>Prácticas de control, extracto DS5.11. | PE11 |
| **12** | Analice los resultados obtenidos, redacte los hallazgos correspondientes. | | PE12 |
| **13** | Elabore el borrador de informe, con base en el conocimiento obtenido de la | NA | PE13 |

| # | Procedimiento | Criterio utilizado | Ref. |
|---|---|---|---|
| | institución y la aplicación de los procedimientos de ejecución. En caso de ser necesario, unifique los hallazgos documentados en el procedimiento 12, envíe el borrador de informes y discuta los comentarios efectuados por la entidad, en caso de ser necesario. | | |
| **14** | Realice las correcciones correspondientes en el informe, de acuerdo con los comentarios de la administración, en caso de que aplique. | NA | PE14 |
| **15** | Aplique formulario de control de calidad, con el fin de verificar el cumplimiento de los estándares mínimos de calidad, con base en la "***Guía de verificación para revisión de procedimientos***". | NA | PE15 |
| **16** | Realice la presentación del estudio, elabore y aplique el acta de presentación, tomando en cuenta a todos los presentes, indique nombre y puesto, solicite firma, copie el documento y entregue uno a la administración. | NA | PE16 |

## 4. Programa de ejecución

# Control sobre el proceso "Garantizar la Seguridad de los Sistemas"

| Referencia | Normativa | Código |
|---|---|---|
| **Ver** | Objetivos de Control para Tecnologías de información y relacionadas (COBIT) 4.0 | N1 |
| **Ver** | Guía de aseguramiento de TI usando COBIT | N2 |
| **Ver** | Prácticas de control | N3 |
| **Ver** | Acuerdo SUGEF 1409 (Versión actualizada) | N4 |

| # | Procedimiento | Criterio utilizado | Ref. |
|---|---|---|---|
| **1** | Solicite el organigrama actualizado de la institución y el plan estratégico institucional, consulte si existen planes de seguridad donde se evidencie la alineación con los requerimientos de negocio, evalúe mediante el formulario de cumplimiento "***FORM-DS5.1 Administración de la seguridad de TI"***, y la matriz "***SUGEF-DS5***". Documente sus resultados. | DS5.1 Administración de la Seguridad de TI Administrar la seguridad de TI al nivel más alto apropiado dentro de la organización, de manera que las acciones de administración de la seguridad estén en línea con los requerimientos del negocio.<br><br>Guía de aseguramiento usando COBIT, extracto DS5.1<br><br>Prácticas de control, extracto DS5.1 | PE1 |
| **2** | Consulte si se ha elaborado un plan de seguridad de TI, de ser así solicítelo y evalúe mediante el formulario de cumplimiento "***FORM-DS5.2 Plan de Seguridad de TI"*** y la matriz "***SUGEF-DS5***". Documente sus resultados. | DS5.2 Plan de seguridad de TI Trasladar los requerimientos de información del negocio, la configuración de TI, los planes de acción del riesgo de la información y la cultura sobre la seguridad en la información a un plan global de seguridad de TI. El plan se implementa en políticas y procedimientos de seguridad en conjunto con inversiones apropiadas en servicios, personal, software y hardware. Las políticas y procedimientos de seguridad se comunican a los interesados y a los usuarios.<br><br>Guía de aseguramiento usando COBIT, extracto DS5.2<br><br>Prácticas de control, extracto DS5.2 | PE2 |
| **3** | Consulte al Jefe de la Unidad de seguridad de la información sobre cómo se está gestionando el proceso de identidad en la institución. Aplique el cuestionario de cumplimiento "***FORM-DS5.3 Administración de*** | DS5.3 Administración de identidad Todos los usuarios (internos, externos y temporales) y su actividad en sistemas de TI (aplicación de negocio, operación del sistema, desarrollo y mantenimiento) deben ser identificables de manera única. Los derechos de acceso del usuario a sistemas y datos | PE3 |

| # | Procedimiento | Criterio utilizado | Ref. |
|---|---|---|---|
| | ***Identidad"*** y la matriz "***SUGEF-DS5***". Extienda las pruebas en caso de ser necesario. Documente sus resultados. | deben estar alineados con necesidades de negocio definidas y documentadas y con requerimientos de trabajo. Los derechos de acceso del usuario son solicitados por la gerencia del usuario, aprobados por el responsable del sistema e implementado por la persona responsable de la seguridad. Las identidades del usuario y los derechos de acceso se mantienen en un repositorio central. Se implementan y se mantienen actualizadas medidas técnicas y procedimientos rentables, para establecer la identificación del usuario, realizar la autenticación y habilitar los derechos de acceso.<br><br>Guía de aseguramiento usando COBIT, extracto DS5.3<br>Prácticas de control, extracto DS5.3 | |
| **4** | Solicite los procedimientos formales sobre la administración de cuentas y evalúe mediante el formulario "***FORM-DS5.4 Administración de Cuentas de Usuario"*** y la matriz "***SUGEF-DS5***". Extienda las pruebas en caso de ser necesario. Documente sus resultados. | DS5.4 Administración de cuentas del usuario Garantizar que la solicitud, establecimiento, emisión, suspensión, modificación y cierre de cuentas de usuario y de los privilegios relacionados, sean tomados en cuenta por la gerencia de cuentas de usuario. Debe incluirse un procedimiento que describa al responsable de los datos o del sistema como otorgar los privilegios de acceso. Estos procedimientos deben aplicar para todos los usuarios, incluyendo administradores (usuarios privilegiados), usuarios externos e internos, para casos normales y de emergencia. Los derechos y obligaciones relacionados al acceso a los sistemas e información de la empresa son acordados contractualmente para todos los tipos de usuarios. La gerencia debe llevar a cabo una revisión regular de todas las cuentas y los privilegios asociados.<br><br>Guía de aseguramiento usando COBIT, extracto DS5.4<br>Prácticas de control, extracto DS5.4 | PE4 |
| **5** | Solicite el plan que detalla la realización de pruebas, vigilancia y monitoreo de actividades inusuales que atenten a la seguridad de TI, indague sobre los resultados de | DS5.5 Pruebas, vigilancia y monitoreo de la seguridad Garantizar que la implementación de la seguridad en TI sea probada y monitoreada de forma pro-activa. La seguridad en TI debe ser reacreditada periódicamente para garantizar que | PE5 |

| # | Procedimiento | Criterio utilizado | Ref. |
|---|---|---|---|
| | dichas pruebas aplicadas el último año y verifique si los resultados han sido contemplados en planes de acción y que los mismos se ejecutan según lo establecido. Aplique cuestionario de cumplimiento "***FORM-DS5.5 Pruebas, Vigilancia y Monitoreo de la Seguridad"*** y la matriz "***SUGEF-DS5***". Documente sus resultados. | se mantiene el nivel seguridad aprobado. Una función de ingreso al sistema (logging) y de monitoreo permite la detección oportuna de actividades inusuales o anormales que pueden requerir atención. El acceso a la información de ingreso al sistema está alineado con los requerimientos del negocio en términos de requerimientos de retención y de derechos de acceso.<br><br>Guía de aseguramiento usando COBIT, extracto DS5.5<br>Prácticas de control, extracto DS5.5 | |
| **6** | Consulte al Jefe de la Unidad de seguridad de la información sobre cómo se está gestionando la gestión de incidentes, indague acerca de la existencia de documentación formal sobre la clasificación y tratamiento de incidentes y problemas de seguridad, evalúe mediante el formulario de cumplimiento "***FORM-DS5.6 Definición de Incidentes de Seguridad"*** y la matriz "***SUGEF-DS5***". Documente sus resultados. | DS5.6 Definición de incidente de seguridad Garantizar que las características de los posibles incidentes de seguridad sean definidas y comunicadas de forma clara, de manera que los problemas de seguridad sean atendidos de forma apropiada por medio del proceso de administración de problemas o incidentes. Las características incluyen una descripción de lo que se considera un incidente de seguridad y su nivel de impacto. Un número limitado de niveles de impacto se definen para cada incidente, se identifican las acciones específicas requeridas y las personas que necesitan ser notificadas.<br><br>Guía de aseguramiento usando COBIT, extracto DS5.6<br>Prácticas de control, extracto DS5.6 | PE6 |
| **7** | Consulte con el encargado de seguridad sobre los mecanismos para la protección de la Tecnología de Seguridad, aplique cuestionario de cumplimiento "***FORM-DS5.7 Protección de la tecnología de seguridad"*** y la matriz "***SUGEF-DS5***". Documente sus resultados. | DS5.7 Protección de la tecnología de seguridad Garantizar que la tecnología importante relacionada con la seguridad no sea susceptible de sabotaje y que la documentación de seguridad no se divulgue de forma innecesaria, es decir, que mantenga un perfil bajo. Sin embargo no hay que hacer que la seguridad de los sistemas dependa de la confidencialidad de las especificaciones de seguridad.<br><br>Guía de aseguramiento usando COBIT, extracto DS5.7 | PE7 |

| # | Procedimiento | Criterio utilizado | Ref. |
|---|---|---|---|
| | | Prácticas de control, extracto DS5.7 | |
| **8** | Solicite las políticas y procedimientos relacionados con la administración de llaves criptográficas y aplique cuestionario de cumplimiento "***FORM-DS5.8 Administración de llaves criptográficas"*** y la matriz "***SUGEF-DS5***". Documente sus resultados. | DS5.8 Administración de llaves criptográficas Determinar que las políticas y procedimientos para organizar la generación, cambio, revocación, destrucción, distribución, certificación, almacenamiento, captura, uso y archivo de llaves criptográficas estén implantadas, para garantizar la protección de las llaves contra modificaciones y divulgación no autorizadas.<br><br>Guía de aseguramiento usando COBIT, extracto DS5.8<br>Prácticas de control, extracto DS5.8 | PE8 |
| **9** | Consulte a los involucraos sobre las medidas para la prevención, detección y corrección de malware, aplique cuestionario de cumplimiento "***FORM-DS5.9 Protección, Detección y Corrección de Software Malicioso"*** y la matriz "***SUGEF-DS5***". Documente sus resultados. | DS5.9 Prevención, detección y corrección de software malicioso Garantizar que se cuente con medidas de prevención, detección y corrección (en especial contar con parches de seguridad y control de virus actualizados) a lo largo de toda la organización para proteger a los sistemas de información y a la tecnología contra software malicioso (virus, gusanos, spyware, correo basura, software fraudulento desarrollado internamente, etc.).<br><br>Guía de aseguramiento usando COBIT, extracto DS5.9<br>Prácticas de control, extracto DS5.9 | PE9 |
| **10** | Consulte a los involucrados sobre los mecanismos de control para garantizar la seguridad de la red. Aplique cuestionario de cumplimiento "***FORM-DS5.10 Seguridad en la red"*** y la matriz "***SUGEF-DS5***". Documente sus resultados. | DS5.10 Seguridad de la red Garantizar que se utilizan técnicas de seguridad y procedimientos de administración asociados (por ejemplo, firewalls, dispositivos de seguridad, segmentación de redes, y detección de intrusos) para autorizar acceso y controlar los flujos de información desde y hacia las redes.<br><br>Guía de aseguramiento usando COBIT, extracto DS5.10<br>Prácticas de control, extracto DS5.10 | PE10 |
| **11** | Consulte acerca de la existencia de procesos que contemplen intercambio | DS5.11 Intercambio de datos sensitivos Garantizar que las transacciones de datos sensibles sean | PE11 |

| # | Procedimiento | Criterio utilizado | Ref. |
|---|---|---|---|
| | de datos sensitivos, de existir aplique el formulario de cumplimiento "***FORM-DS5.11 Intercambio de datos sensitivos"*** y la matriz "***SUGEF-DS5***". Documente sus resultados. | intercambiadas solamente a través de una ruta o medio confiable con controles para brindar autenticidad de contenido, prueba de envío, prueba de recepción y no rechazo del origen.<br><br>Guía de aseguramiento usando COBIT, extracto DS5.11<br><br>Prácticas de control, extracto DS5.11 | |
| **12** | Analice los resultados obtenidos, redacte los hallazgos correspondientes. | | PE12 |
| **13** | Elabore el borrador de informe con base en el conocimiento obtenido de la institución y la aplicación de los procedimientos de ejecución. En caso de ser necesario unifique los hallazgos documentados en el procedimiento 12, envíe el borrador de informes y discuta los comentarios efectuados por la entidad en caso de ser necesario. | NA | PE13 |
| **14** | Realice las correcciones correspondientes en el informe, de acuerdo con los comentarios de la administración en caso de que aplique. | NA | PE14 |
| **15** | Aplique formulario de control de calidad con el fin de verificar el cumplimiento de los estándares mínimos de calidad con base en la "***Guía de verificación para revisión de procedimientos***". | NA | PE15 |
| **16** | Realice la presentación del estudio, elabore y aplique el acta de presentación, tomando en cuenta a todos los presentes, indique nombre y puesto, solicite firma, copie el documento y entregué uno a la administración. | NA | PE16 |

# 4. Informe final

**INFORME IF-001-2013**
**05 de Marzo, 2013**

# AUDITORIA DE TECNOLOGÍAS DE INFORMACIÓN

## INFORME

## CONTROL SOBRE EL PROCESO DE TI “GARANTIZAR LA SEGURIDAD DE LOS SISTEMAS”

**2013**

# 1. INTRODUCCIÓN

## 1.1. Origen del estudio

La evaluación se origina como parte de la práctica profesional para optar por el grado de maestría en Auditorías de Tecnologías de Información de la UCR.

## 1.2. Objetivo general

Evaluar el proceso "Garantizar la Seguridad de los Sistemas" de acuerdo con la normativa aplicable a la institución, con el fin de emitir un criterio a la administración sobre el nivel de madurez alcanzado en este proceso.

## 1.3. Objetivos específicos

- Indagar con los dueños de proceso correspondientes, sobre las acciones que ha emprendido la institución como parte de la implementación del proceso "Garantizar la Seguridad de los Sistemas" con el fin de obtener un conocimiento de la situación actual y de los esfuerzos realizados como parte de la implementación del proceso en estudio.

- Fundamentar, por medio de criterio de expertos, mejores prácticas, y el nivel de madurez para este proceso de acuerdo con el COBIT®, lo que se espera encontrar por parte de la institución, con el fin de obtener una base sobre la cual emitir los criterios correspondientes.

- Determinar el grado de madurez en el que se encuentra el proceso "Garantizar la Seguridad de los Sistemas" con el fin de que las brechas identificadas sean comunicadas a la administración y se asegure, de manera razonable, la confidencialidad, integridad y disponibilidad de la información de sus accionistas.

## 1.4. Alcance

Evaluar el nivel de madurez del proceso "Garantizar la Seguridad de los Sistemas" implementado en la institución en el periodo comprendido entre setiembre 2012 y abril 2013; con base en el nivel de madurez de este proceso propuesto en los Objetivos de Control para la Información y Tecnología Relacionada COBIT® 4.0, en cumplimiento al acuerdo SUGEF 1409.

## 1.5. Limitaciones

En relación con la confidencialidad de la información de lo correspondiente a los resultados de análisis de vulnerabilidades, análisis de riesgos y algunas otros documentos considerados por la institución como sensibles, se indicó expresamente que se debe mantener la confidencialidad de la información, por tanto sólo se obtendrá acceso a esos documentos mediante revisiones en sitio, así mismo no es posible la aplicación de herramientas tecnológicas para la elaboración de pruebas de seguridad.

En línea con el tema de la confidencialidad, para efectos de la elaboración de este documento se ha protegido el nombre real de la institución, de ahí que se haga referencia a ella como “CDA”.

## 2. SOBRE LA RECOPILACIÓN DE LOS DATOS

Durante el mes de Febrero del 2013 se coordinaron reuniones con el personal de la Unidad de Seguridad de la Información para realizar la evaluación de los objetivos de control de Cobit del proceso DS5 Garantizar la Seguridad de los Sistemas mediante los diferentes cuestionarios de cumplimiento - elaborados con base en la Guía de Aseguramiento del COBIT - y la Matriz de Calificación de la Gestión de TI de la SUGEF según el acuerdo 14-09. A continuación se detalla el cronograma de las reuniones realizadas para la evaluación con los involucrados, tal y como se puede observar en la Tabla No. 1:

**Tabla No. 1: Detalle de entrevistas**

| Objetivo de Control a evaluar | Fecha reunión | Participantes | Puesto |
|---|---|---|---|
| **DS5.1 Administración de la seguridad de TI** | 19-feb-13 | Lic. Abarca | Jefe de la Unidad de Seguridad de la Información |
| **DS5.2 Plan de Seguridad de TI** | 20-feb-13 | Lic. Abarca | Jefe de la Unidad de Seguridad de la Información |
| | | MBA. Obando | Analista de Seguridad |
| **DS5.3 Administración de Identidad** | 13-feb-13 | Lic. Abarca | Jefe de la Unidad |

| Objetivo de Control a evaluar | Fecha reunión | Participantes | Puesto |
|---|---|---|---|
| | | | de Seguridad de la Información |
| **DS5.4 Administración de Cuentas de Usuario** | 13-feb-13 | Lic. Abarca | Jefe de la Unidad de Seguridad de la Información |
| **DS5.5 Pruebas, Vigilancia y Monitoreo de la Seguridad** | 19-feb-13 | MGTI. Hernández | Analista de Seguridad |
| **DS5.6 Definición de Incidentes de Seguridad** | 20-feb-13 | Lic. Abarca | Jefe de la Unidad de Seguridad de la Información |
| | | Ing. Madrigal | Analista de Seguridad |
| **DS5.7 Protección de la Tecnología de la Seguridad** | 21-feb-13 | MGTI. Hernández | Analista de Seguridad |
| **DS5.8 Administración de llaves criptográficas** | 21-feb-13 | Lic. Abarca | Jefe de la Unidad de Seguridad de la Información |
| **DS5.9 Protección, Detección y Corrección de Software Malicioso** | 21-feb-13 | Lic. Abarca | Jefe de la Unidad de Seguridad de la Información |
| **DS5.10 Seguridad en la red** | 20-feb-13 | Lic. Abarca | Jefe de la Unidad de Seguridad de la Información |
| | | Ing. Madrigal | Analista de |

| Objetivo de Control a evaluar | Fecha reunión | Participantes | Puesto |
|---|---|---|---|
| | | | Seguridad |
| **DS5.11 Intercambio de datos sensitivos** | 20-feb-13 | Lic. Abarca | Jefe de la Unidad de Seguridad de la Información |
| | | MBA. Obando | Analista de Seguridad |

## 3. RESULTADOS

Al realizar la evaluación y analizar los resultados obtenidos con respecto a lo esperado se identifican una serie de recomendaciones u oportunidades de mejora, con el fin de que sean comunicadas a los diferentes responsables en la administración.

Se identifican cuatro oportunidades de mejora que la institución debe atender con mayor prioridad, que corresponden a los resultados con la calificación más baja respecto al cumplimiento de los objetivos de control del proceso COBIT® DS5 “Garantizar la Seguridad de los Sistemas” y el nivel de madurez requerido por la institución en este proceso en particular según el acuerdo SUGEF 14-09; (apartados 3.1.1, 3.1.2, 3.1.3 y 3.1.4).

Posteriormente se detallan otras oportunidades de mejora que se desprenden de la evaluación del diseño de los controles a partir de la guía de aseguramiento denominada “IT Assurance Guide Using COBIT®”. Estas recomendaciones se pueden consultar en el apartado 4.5.

### 3.1. Hallazgos

#### 3.1.1. H1 Debilidades en la revisión de cuentas y derechos de acceso.

La necesidad de proteger la información de accesos no autorizados a los datos de una empresa requiere de un proceso que garantice, entre otras cosas, la administración de la identidad y la revisión periódica de los derechos de acceso otorgados a los usuarios con

base en los principios de seguridad de la información “Mínimo Privilegio” y “Necesidad de saber”.

De acuerdo con las buenas prácticas establecidas en el COBIT, el objetivo de control “DS5.4 Administración de cuentas del usuario” y DS5.3 “Administración de la identidad”, indican respectivamente:

> **DS5.4 Administración de cuentas del usuario**
>
> “Garantizar que la solicitud, establecimiento, emisión, suspensión, modificación y cierre de cuentas de usuario y de los privilegios relacionados, sean tomados en cuenta por la gerencia de cuentas de usuario. Debe incluirse un procedimiento que describa al responsable de los datos o del sistema como otorgar los privilegios de acceso. Estos procedimientos deben aplicar para todos los usuarios, incluyendo administradores (usuarios privilegiados), usuarios externos e internos, para casos normales y de emergencia. Los derechos y obligaciones relacionados al acceso a los sistemas e información de la empresa son acordados contractualmente para todos los tipos de usuarios. La gerencia debe llevar a cabo una revisión regular de todas las cuentas y los privilegios asociados.”
>
> **DS5.3 Administración de identidad**
>
> Todos los usuarios (internos, externos y temporales) y su actividad en sistemas de TI (aplicación de negocio, operación del sistema, desarrollo y mantenimiento) deben ser identificables de manera única. Los derechos de acceso del usuario a sistemas y datos deben estar alineados con necesidades de negocio definidas y documentadas y con requerimientos de trabajo. Los derechos de acceso del usuario son solicitados por la gerencia del usuario, aprobados por el responsable del sistema e implementado por la persona responsable de la seguridad. Las identidades del usuario y los derechos de acceso se mantienen en un repositorio central. Se implementan y se mantienen actualizadas medidas técnicas y procedimientos rentables, para establecer la identificación del usuario, realizar la autenticación y habilitar los derechos de acceso.

Por otro lado la institución ha establecido a nivel interno las siguientes normativas:

> **NOR-OSI-012 Control de acceso a los Sistemas de Información**
>
> 4.2.4 Revisión de derechos de acceso de usuario
>
> “4.2.4.1 Las jefaturas y coordinadores de área de negocio deberán revisar los accesos otorgados a sus trabajadores al menos una vez al año o luego de cualquier cambio significativo, tales como un ascenso, un traslado o la finalización del contrato laboral.”
>
> **POL-OSI-007 Política de identificación de Usuarios del Sistema**
>
> “5.3 […] La identidad de los usuarios y los derechos de acceso deben encontrarse en un repositorio central […]”

En línea con lo anterior, el análisis realizado por esta Auditoria evidenció que la Unidad de Seguridad de la Información ha establecido procedimientos y normativas sobre la

administración de cuentas y privilegios de usuario, no obstante actualmente no se realizan revisiones regulares de todas las cuentas y privilegios asociados. Si bien es cierto que lo anterior se ha realizado en otras ocasiones, esto ha obedecido a ciertas eventualidades o bien a iniciativas aisladas de los técnicos, iniciativas que tienen una respuesta parcial por los jefes de las unidades de negocio.

Adicionalmente no se mantiene un registro formal (Repositorio Central) que incluya los niveles de acceso de todas las personas registradas y de acuerdo con las necesidades del puesto.

Lo anterior obedece a que no se ha definido formalmente un área que se encargue de dirigir los esfuerzos tendientes a realizar las revisiones de derechos de acceso ni la creación y el mantenimiento del repositorio central que contenga la identidad y los derechos de acceso de los usuarios, situación puede acarrear riesgos de pérdida de imagen o económica como consecuencia de:

- Manipulación de información de forma malintencionada por accesos no autorizados.
- Incumplimientos regulatorios por violaciones a las directrices establecidas tanto a nivel interno como externo.

La condición observada incumple con los criterios establecidos en el objetivo de control DS5.4 “Administración de cuentas del usuario”, DS5.3 “Administración de la Identidad”, así como la Normativa “NOR-OSI-012 Control de acceso a los Sistemas de Información” y la política “POL-OSI-007 Política de identificación de Usuarios del Sistema”.

### 3.1.2. H2 Debilidades en la gestión de incidentes de seguridad.

Un incidente de seguridad es cualquier evento negativo que comprometa la confidencialidad, disponibilidad o integridad de la información. Los incidentes y las crisis son dinámicas por naturaleza, puesto que evolucionan y según las circunstancias pueden ser rápidos e imprevistos, por tanto su gestión debe ser igualmente dinámica, proactiva y bien documentada.

El proceso de gestión de incidentes de seguridad busca analizar y responder con eficacia a estos eventos inesperados, minimizando su impacto y alcanzando la recuperación dentro del objetivo de tiempo aceptados por la institución.

De acuerdo con las buenas prácticas establecidas en el COBIT, el objetivo de control “DS56 Definición de incidente de seguridad” indica:

> **DS5.6 Definición de incidente de seguridad**
>
> Garantizar que las características de los posibles incidentes de seguridad sean definidas y comunicadas de forma clara, de manera que los problemas de seguridad sean atendidos de

> forma apropiada por medio del proceso de administración de problemas o incidentes. Las características incluyen una descripción de lo que se considera un incidente de seguridad y su nivel de impacto. Un número limitado de niveles de impacto se definen para cada incidente, se identifican las acciones específicas requeridas y las personas que necesitan ser notificadas.

El análisis realizado evidenció que aun cuando se creó la normativa NOR-OSI-007 Normativa para la Gestión de Incidentes de Seguridad de la Información y se definieron las categorías de incidentes de seguridad, no se ha definido y comunicado de forma clara los niveles de impacto, los números limitados de nivel de impacto para cada incidente, acciones específicas requeridas, las personas que deben ser notificadas ni medidas de protección de la confidencialidad de la información relacionada con dichos incidentes.

Con el objetivo de definir, documentar y comunicar las áreas de atención, niveles de escalamiento, áreas de atención según niveles de impacto y tiempos de atención, en el año 2012 la Unidad de Seguridad de la Información, creó un documento denominado “Catálogo de Servicios Incidentes de Seguridad de la Información”; sin embargo alguna de la información de dicho documento debe ser proporcionada por el Departamento de TI, no obstante, de acuerdo con lo manifestado en la entrevista, a la fecha de la evaluación no se ha tenido respuesta, razón por la cual no se encuentra debidamente aprobado ni comunicado a los involucrados.

En términos generales el CISO indicó que como parte de la operativa diaria del 2013 se estableció la actividad denominada “Actividad OC 8.3 -1. Fortalecer el proceso de gestión de incidentes de seguridad de la información” con la asesoría de un consultor externo con el fin de afinar el proceso y a partir de esos resultados coordinar con el Departamento de TI las actividades requeridas, incluyendo el llenado del documento “Catálogo de Servicios Incidentes de Seguridad de la Información” o algún otro similar.

Esta situación puede acarrear riesgos de pérdidas económicas o de imagen como consecuencia de:

- Inadecuada respuesta a los incidentes de seguridad.
- Inadecuado proceso de seguimiento de Incidentes.
- Brechas de seguridad no identificadas.
- Confidencialidad, integridad o disponibilidad de la información comprometida por los incidentes de seguridad

La condición observada incumple con los criterios establecidos en el objetivo de control DS5.6 “Definición de incidente de seguridad” y la normativa interna “NOR-OSI-007 Normativa para la Gestión de Incidentes de Seguridad de la Información”.

### 3.1.3. H3 Debilidades en la administración de llaves criptográficas.

Una llave criptográfica consiste en una pieza de información que se usa dentro de un algoritmo de encriptación con el fin de poder reconvertir un mensaje cifrado a texto plano, de modo que el receptor del mensaje debe usar la llave correcta para tener acceso o descifrar el mensaje. Es importante establecer mecanismos de control para garantizar la protección de las llaves criptográficas contra modificaciones o divulgaciones no autorizadas.

De acuerdo con las buenas prácticas establecidas en el COBIT, el objetivo de control "DS5.8 Administración de llaves criptográficas" indica:

> **DS5.8 Administración de llaves criptográficas**
>
> Determinar que las políticas y procedimientos para organizar la generación, cambio, revocación, destrucción, distribución, certificación, almacenamiento, captura, uso y archivo de llaves criptográficas estén implantadas, para garantizar la protección de las llaves contra modificaciones y divulgación no autorizadas.

Por otro lado la institución ha establecido la siguiente política:

> **POL-OSI-008 Política mantener y salvaguardar las llaves criptográficas.**
>
> "5.1 Se deben establecer procedimientos que organicen la generación, cambio, revocación, destrucción, distribución, certificación, almacenamiento, captura, uso y archivo de las llaves criptográficas, para garantizar la protección de las llaves contra modificaciones y divulgación no autorizada."

El análisis realizado evidenció que la institución ha establecido políticas para la gestión de las llaves criptográficas sin embargo las mismas no consideran:

- Lineamientos para determinar cuándo es necesario renovar la llave criptográfica (por ejemplo cuando se ha visto comprometida o ha caducado)
- Mecanismos de seguridad para asegurar que el almacenamiento y la distribución de las llaves se realiza de manera segura.
- Tamaño mínimo requerido para la generación de llaves robustas
- Uso de algoritmos de generación de claves requeridos.
- Identificación de los estándares requeridos para la generación de claves.
- Propósitos para los cuales está restringido el uso de las llaves y para los cuales se debe hacer uso.
- Los períodos de uso permitidos. (sólo indica que debe tener una fecha de caducidad)
- Copia de seguridad.
- Archivo

- Destrucción. (sólo indica que deben destruirse utilizando mecanismos seguros)

Así mismo no se evidenció la existencia de procedimientos que consideren:

- La generación, cambio, revocación, destrucción, distribución, captura y uso de las llaves criptográficas.
- Almacenamiento en dispositivos criptográficos seguros.
- Exportación desde un módulo criptográfico seguro.
- Personas autorizadas para la copia, recuperación y almacenamiento de llaves criptográficas.

Lo anterior obedece a que las áreas responsables no han atendido lo indicado en la política para mantener y salvaguardar las llaves criptográficas. Por otro lado los lineamientos relacionados con llaves criptográficas - mencionados anteriormente - no han sido considerados por la institución.

Esta situación puede acarrear riesgos de pérdidas económicas o de imagen como consecuencia de:

- Usurpación de claves por partes no autorizadas.
- Acceso no autorizado a las claves criptográficas.
- Perdida de confidencialidad

En línea con todo lo anterior, la condición observada incumple con los criterios establecidos en el objetivo de control “DS5. DS5.8 Administración de llaves criptográficas” y la política interna “POL-OSI-008 Política mantener y salvaguardar las llaves criptográficas”.

### 3.1.4. H4 Debilidades en el Intercambio de datos sensitivos.

CDA es una institución financiera que administra fondos públicos, con acceso a información confidencial de alrededor de 100.000 accionistas, por tanto resulta de vital importancia que la información que intercambia con otras instituciones, como parte de la operativa diaria y la naturaleza de sus operaciones sea protegida con mecanismos de control que garanticen que esa transmisión se realice por medios seguros y que asegure autenticidad, pruebas de envío y recepción y no rechazo de origen.

De acuerdo con las buenas prácticas establecidas en el COBIT, el objetivo de control “DS5.11 Intercambio de datos sensitivos” indica:

> **DS5.11 Intercambio de datos sensitivos**
>
> "Garantizar que las transacciones de datos sensibles sean intercambiadas solamente a través de una ruta o medio confiable con controles para brindar autenticidad de contenido, prueba de envío, prueba de recepción y no rechazo del origen."

Por otro lado la institución ha establecido la siguiente política:

> **POL-OSI-010 Política de transacciones de intercambio de información sensitiva**
>
> "5.1 El Departamento de Informática y demás áreas de la institución que requieran intercambiar información sensitiva deberán seguir los lineamientos de seguridad para la protección de la misma, por medio de la definición y aplicación de procedimientos que permitan lo siguiente:
>
> > 5.1 Establecer los controles que el intercambio de transacciones de información sensitiva utilizan rutas seguras; controles que proveen autenticidad, prueba de envío, prueba de recepción y no rechazo de origen"

El análisis realizado evidenció que mensualmente se intercambia información con otras entidades fuera de la institución presentándose las siguientes debilidades:

- No se ha definido cómo los datos deben ser protegidos cuando se intercambian de acuerdo con la clasificación de la información.
- No se aplican mecanismos de encriptación de previo a la transmisión fuera de la institución, excepto para el caso del Poder Judicial que facilitó una herramienta para el intercambio de información con ese entidad.
- Las transacciones de datos sensibles no se intercambian con controles que brinden autenticidad de contenido y no rechazo de origen.

Mediante entrevista con los encargados de realizar el intercambio de datos se indicó que no se aplican mecanismos de encriptación de previo a la transmisión fuera de la institución, ya que ha sido difícil coordinar con las diferentes instituciones receptoras de la información.

Esta situación puede acarrear riesgos de pérdidas económicas, legales o de imagen como consecuencia de:

- Exposición de información sensible.
- Revelación de información a personas inescrupulosas y no autorizadas.

La condición observada incumple con los criterios establecidos en el objetivo de control DS5. Intercambio de datos sensitivos y la política POL-OSI-010 Política de transacciones de intercambio de información sensitiva.

### 3.1.5. Sobre el nivel de madurez:

Como parte de la evaluación realizada al proceso “DS5 Garantizar la Seguridad de los Sistemas” se utilizó, entre otros instrumentos, la “Matriz de Calificación de la Gestión de TI” del acuerdo SUGEF 14-09.

La “Matriz de Calificación de la Gestión de TI” establece un conjunto de preguntas de respuesta cerrada, asociado a cada objetivo de control.

El resultado obtenido es de 81, colocando el proceso en Irregularidad 1, según la tabla de niveles de la gestión de TI del reglamento sobre la gestión de la tecnología de información para el acuerdo SUGEF 14-09, como se muestra a continuación en la Tabla No. 2:

**Tabla No. 2: Calificación sobre la gestión de TI**

| Calificación | Nivel |
|---|---|
| Mayor o igual que 85% | Normal |
| Mayor o igual que 70% y menor que 85% | Irregularidad 1 |
| Mayor o igual que 55% y menor que 70% | Irregularidad 2 |
| Menor que 55% | Irregularidad 3 |

Los cálculos realizados para obtener la calificación se realizaron con base en las fórmulas estipulas en el reglamento sobre la gestión de la tecnología de información para el acuerdo SUGEF 14-09.

La calificación del nivel de madurez como parte de la evaluación fue un nivel 3 definido.

Según lo que indica COBIT en la sección niveles de madurez:

> **“3 Proceso definido**
>
> Existe conciencia sobre la seguridad y ésta es promovida por la gerencia. Los procedimientos de seguridad de TI están definidos y alineados con la política de seguridad de TI. Las responsabilidades de la seguridad de TI están asignadas y entendidas, pero no continuamente implementadas. Existe un plan de seguridad de TI y existen soluciones de seguridad motivadas por un análisis de riesgo. Los reportes no contienen un enfoque claro de negocio. Se realizan pruebas de seguridad adecuadas (por ejemplo, pruebas contra intrusos). Existe capacitación en seguridad para TI y para el negocio, pero se programa y se comunica de manera informal.” (Pag.122).

Es importante indicar que se identificó como parte del análisis que actualmente el proceso DS5 Garantizar la Seguridad de los sistemas cuenta con una brecha de un 83% para alcanzar el nivel de madurez 4 administrado y medible. El resultado de la evaluación se puede apreciar en la Tabla No. 3:

**Tabla No. 3 Resultado de la evaluación**

| Descripción | Peso | Calificación | Resultado | % |
|---|---|---|---|---|
| **Resultado de la calificación del Objetivos de Control (COC)** | **0.70** | **0.81** | **0.56** | **56%** |
| **Resultado de la calificación del Nivel de Madurez (CNM)** | **0.30** | **0.83** | **0.25** | **25%** |
| **Resultado** | | | **0.81** | **81%** |

# 4. Recomendaciones

## 4.1. HH1 Debilidades en la revisión de cuentas y derechos de acceso.

- Definir, documentar y comunicar formalmente un proceso para la revisión de derechos de acceso el cual debe tener claramente establecido, al menos, los responsables, las funciones y la periodicidad de revisión.

- Realizar un proceso de sensibilización que tenga como fin el conocimiento efectivo del uso e importancia de los derechos de acceso que al menos considere la participación de los Jefes de Departamento de las unidades de negocio y de TI.

- Coordinar con las diferentes áreas involucradas para la creación del repositorio centralizado donde se mantengan las identidades del usuario y los derechos de acceso; así como la definición de mecanismos de control que aseguren que dicho repositorio se mantenga actualizado.

- Establecer un proceso de evaluación periódica de forma que se mantengan las condiciones idóneas y los niveles de controles adecuados para lo establecido en las recomendaciones a, b y c indicadas anteriormente.

## 4.2. HH2 Debilidades en la gestión de incidentes de seguridad.

- Establecer controles de seguimiento y monitoreo a la actividad establecida “fortalecer el proceso de gestión de incidentes” de forma que no se deteriore y se mantenga la calidad y suficiencia de la misma, además de involucrar al Departamento de Tecnologías de Información para que aporten la información necesaria y se ejecute de conformidad con los resultados obtenidos en la consultoría realizada para tal fin.

- Definir y velar, con el apoyo del departamento de TI, por la ejecución de mecanismos de control para garantizar el cumplimiento de lo establecido en consultoría realizada para tal fin y que las desviaciones en las actividades planeadas sean presentadas a la Alta Administración con el fin de que se tomen las medidas necesarias.

## 4.3. HH3 Debilidades en la administración de llaves criptográficas.

- Documentar, aprobar y comunicar formalmente los lineamientos relacionados con la administración de llaves criptográficas que al menos incluyan las siguientes directrices:
    - Determinación de cuándo es necesario renovar la llave criptográfica.
    - Almacenamiento y distribución de las llaves de manera segura.
    - Tamaño mínimo requerido para la generación de llaves robustas
    - Algoritmos de generación de claves requeridos.
    - Identificación de los estándares requeridos para la generación de claves.
    - Propósitos para los cuales está restringido el uso de las llaves y para los cuales se debe hacer uso.
    - Periodos de uso permitidos.
    - Capias de seguridad.
    - Políticas y acciones de Archivo o almacenamiento
    - Métodos de Desecho.

- Documentar, aprobar y comunicar un procedimiento (alineado con los lineamientos de llaves criptográficas indicados en la recomendación anterior) que al menos considere:

    - La generación, cambio, revocación, destrucción, distribución, captura y uso de las llaves criptográficas.

    - Así mismo que considere lo establecido en las directrices emitidas por la Unidad de Seguridad de la Información.

- Se establezca y se vele por el cumplimiento de mecanismos de control para asegurar el cumplimiento del procedimiento.

## 4.4. HH4 Debilidades en el Intercambio de datos sensitivos.

- Definir y ejecutar controles que brinden autenticidad de contenido y no rechazo de origen durante el proceso de intercambio de datos sensibles y que coordine con las diferentes entidades receptoras el uso de mecanismos de encriptación para asegurar la confidencialidad de la información que se intercambia.

## 4.5. Otras oportunidades de mejora.

**DS5.1 Administración de la Seguridad de TI**

- Establecer un proceso para priorizar las iniciativas de seguridad de manera alineada con los objetivos estratégicos de la institución.

**DS5.2 Plan de Seguridad de TI**

- Documentar, aprobar y comunicar un procedimiento para la actualización del Plan de Seguridad de TI, donde se detalle, al menos, los responsables y periodicidad para realización las actualizaciones. Así mismo que se establezcan mecanismos para evaluar el cumplimiento del procedimiento.

- Valorar la inclusión de los siguientes elementos (pero no únicamente) en el Plan de Seguridad de TI:
    - Planes tácticos.
    - Estándares de tecnología.
    - Configuración de la línea base para todas las plataformas de acuerdo con el Plan de Seguridad, así mismo no se cuenta con un procedimiento para actualizar periódicamente la línea base de configuración de acuerdo con los cambios en el plan.
    - Inversiones en recursos de seguridad a nivel institucional.
    - Integración con otros procesos, a saber: DS1 Definir y administrar niveles de servicio, DS2 Administrar servicios de terceros, AI1 Identificar soluciones automatizadas, AI2 Adquirir y mantener el software aplicativo y AI3 Adquirir y mantener la infraestructura tecnológica.

**DS5.3 Administración de la identidad**

- Las recomendaciones relacionadas con este objetivo de control se integraron con las recomendaciones relacionadas con gestión de cuentas en el apartado 4.1.4 indicado anteriormente.

**DS5.5 Pruebas, vigilancia y monitoreo de la seguridad**

- Determinar la suficiencia de los planteamientos para atender una violación de la seguridad, de forma que se garantice la prevención y mitigación de este tipo de riesgo.

- Definir las líneas base de seguridad, de forma que se garantice que la configuración de seguridad de los parámetros del sistema y de red estén definidos correctamente.

- Elaborar un inventario de todos los dispositivos de red, servicios y aplicaciones con calificación de riesgo de seguridad, así como un procedimiento para la actualización de dicho inventario.

- Establecer vigilancia constante de eventos de seguridad para todos los activos de red críticos para la organización y de mayor riesgo con el fin de que se tomen las acciones necesarias de manera oportuna para evitar la materialización de estos riesgos.

- Formalizar la integración de la Unidad de Seguridad de la Información con las iniciativas de gestión de proyectos con el fin de asegurar que su criterio es considerado en el desarrollo, diseño y definición de requerimientos de pruebas, para minimizar el riesgo de materialización de vulnerabilidades relacionadas con la seguridad de la información.

- Realizar una revisión general de todos los procedimientos así como de la ejecución eficaz de estos. Se considera de vital importancia la revisión de los procedimientos denominados: "PROC-OSI-012-004 Monitoreo del Uso de las Cuentas de Usuarios (Logging)" y "PROC-OSI-002-012 Validar cumplimiento procedimientos seguridad información"

**DS5.7 Protección de la tecnología de seguridad**

- Definir formalmente y comunicar los algoritmos de encriptación a utilizar para resistir la exposición en caso de un acceso no autorizado.

**DS5.9 Prevención, detección y corrección de software malicioso**

- Continuar ejecutando los controles que la institución ha establecido para este objetivo de control. No se identificaron debilidades de control.

**DS5.10 Seguridad de la red**

- Documentar formalmente el procedimiento para la administración de componentes de red.

## 5. conclusiones

Al finalizar el desarrollo de este estudio se alcanzó el objetivo general señalado en este documento el cual consistió en evaluar el proceso "Garantizar la Seguridad de los Sistemas" de acuerdo con la normativa aplicable a la institución, con el fin de emitir un criterio a la administración sobre el nivel de madurez alcanzado en este proceso.

La Unidad de Seguridad de la Información, con el apoyo de la Gerencia, ha realizado esfuerzos para el cumplimiento de lo indicado en el marco de referencia COBIT®, sin embargo se debe tomar en consideración las recomendaciones anteriormente planteadas para lograr la ejecución óptima del proceso, haciendo énfasis en las debilidades identificadas en la gestión de cuentas y derechos de acceso, gestión de incidentes de

seguridad, administración de llaves criptográficas e intercambio de datos sensibles; apartados 3.1.1, 3.1.2, 3.1.3 y 3.1.4.

El no acatamiento de estas recomendaciones podría generar un impacto negativo en la institución por:

- Perdidas económicas:
    - Reprocesos ocasionados por una inadecuada gestión de incidentes de seguridad lo que puede provocar la materialización de otros eventos negativos que no son subsanados por medio del proceso de gestión de problemas (análisis de causa raíz).
- Pérdida de imagen por:
    - Manipulación de información de forma malintencionada por accesos no autorizados.
    - Inadecuada respuesta a los incidentes de seguridad lo que puede provocar un impacto negativo en el servicio al accionista, en los activos de TI y en la seguridad de la información.
    - Brechas de seguridad no identificadas y tratadas de manera oportuna.
    - Pérdida de Confidencialidad, integridad o disponibilidad de la información causada por los incidentes de seguridad
    - Usurpación de llaves criptográficas con fines malintencionados por partes no autorizadas lo que puede comprometer la seguridad de la información de los accionistas.
- Procesos legales por:
    - Exposición de información sensible de los accionistas.
    - Revelación de información a personas inescrupulosas y no autorizadas.
- Incumplimiento regulatorio.

Para los otros incumplimientos, a pesar de que no son sustantivos en este momento, la aplicación de las recomendaciones sí contribuiría a que la institución alcance un mayor grado de madurez de este proceso en particular.

La sinergia que puedan realizar la Unidad de Seguridad de la Información y el Departamento de Tecnologías de Información es vital para el mejoramiento de todas las debilidades que se presentaron.

Destacar la función de la Unidad de Seguridad de la Información que, con el apoyo de la alta dirección, se ha encargado de desarrollar e implementar la seguridad en la Institución

para poder brindar tanto a los accionistas como a los trabajadores confidencialidad, integridad y disponibilidad de la información.

## 5. Formularios para la evaluación del proceso COBIT DS5 "Garantizar la seguridad de los Sistemas"

Para el diseño de las herramientas a utilizar se consideró que, como parte de la implementación del acuerdo SUGEF 1409, la institución ha realizado una serie de actividades tendientes a implementar, entre otros, el proceso DS5 "Garantizar la seguridad de los sistemas" de acuerdo con el COBIT 4.0, en razón de lo anterior, se considera conveniente aplicar herramientas que permitan:

1. **Evaluar el diseño de los objetivos de control del proceso DS5, a saber:**
    - DS5.1 Administración de la seguridad de TI
    - DS5.2 Plan de seguridad de TI
    - DS5.3 Administración de identidad
    - DS5.4 Administración de cuentas del usuario
    - DS5.5 Pruebas, vigilancia y monitoreo de la seguridad
    - DS5.6 Definición de incidente de seguridad
    - DS5.7 Protección de la tecnología de seguridad
    - DS5.8 Administración de llaves criptográficas
    - DS5.9 Prevención, detección y corrección de software malicioso
    - DS5.10 Seguridad de la red
    - DS5.11 Intercambio de datos sensitivos

Para el diseño de estas herramientas se utilizó como referencia el detalle del objetivo de control descrito en COBIT y la Guía de aseguramiento "IT Assurance guide using COBIT"

y se obtiene una calificación para cada objetivo de control, considerando las prácticas de control y el diseño del control tomado como referencia las guías en mención.

2. **Calificar el nivel de madurez alcanzado, de acuerdo con:**
    - Nivel de madurez detallado en COBIT 4.0
    - Los objetivos de control del proceso DS5 listados anteriormente
    - Anexo 2 del acuerdo SUGEF 1409 "Procedimiento para Obtener la Calificación sobre la Gestión de TI" (en este caso considerando únicamente el proceso DS5).

Se elaboraron las siguientes herramientas:

- FORM-DS5.1 Administración de la seguridad de TI
- FORM-DS5.2 Plan de Seguridad de TI
- FORM-DS5.3 Administración de Identidad
- FORM-DS5.4 Administración de Cuentas de Usuario
- FORM-DS5.5 Pruebas, Vigilancia y Monitoreo de la Seguridad
- FORM-DS5.6 Definición de Incidentes de Seguridad
- FORM-DS5.7 Protección de la tecnología de seguridad
- FORM-DS5.8 Administración de llaves criptográficas
- FORM-DS5.9 Protección, Detección y Corrección de Software Malicioso
- FORM-DS5.10 Seguridad en la red
- FORM-DS5.11 Intercambio de datos sensitivos
- SUGEF-DS5