AUDITORIA INTERNA

Tel: 2527 2276

Telefax: 2224 9684

Apdo. 474-2050

San Pedro de Montes de Oca

UNIVERSIDAD ESTATAL A DISTANCIA

AUDITORIA INTERNA

ESTUDIO SOBRE LA SEGURIDAD FISICA Y LÓGICA DEL "DATA CENTER" DE LA UNED

INFORME FINAL X-24-2011-02

2012

Tel: 2527 2276
Telefax: 2224 9684
Apdo. 474-2050
San Pedro de Montes de Oca

1. INTRODUCCIÓN:

1.1 Origen del Estudio

El presente Estudio se originó en atención al Plan Anual de Trabajo de la Auditoría Interna de la UNED para el año 2011, en el área de Auditoría en Tecnología de la Información.

1.2 Objetivo General

Evaluar la seguridad física y lógica del "DATA CENTER" de las Oficinas Centrales de la UNED.

1.3 Alcance

El estudio abarcó la evaluación de Seguridad Física del área asignada al "Data Center", ubicado en oficinas de la Dirección de Tecnología, Información y Comunicaciones (DTIC), sitio donde residen los servidores institucionales; además se evaluó la seguridad lógica de estos equipos.

El período objeto de estudio está comprendido del 01 de febrero del 2010 al 01 de febrero del 2011. Se abarcaron los acuerdos tomados por el Consejo de Rectoría en ese período.

1.4 Limitaciones

En este estudio se presentaron las siguientes limitaciones:

- La DTIC no cuenta con la lista de todos los usuarios que utilizan los sistemas de información automatizados en la institución; tampoco se tiene identificado por sistemas, el acceso concedido a cada funcionario, según el perfil informático respectivo.

- El documento denominado *"inventario activos tecnológicos"* aportado por la DTIC y el listado de *"inventario"* suministrado por la Oficina de Contabilidad General, presentan diferencias entre sí, aspecto que dificulta conciliar los datos relacionados con el equipo existente y el software del Data Center.

1.5 Deberes en el trámite de informes y plazos que se deben observar

Con el fin de prevenir sobre los deberes del titular subordinado, en el trámite de informes y de los plazos que se deben observar, a continuación se citan los artículos Nos. 36 y 38 de la Ley General de Control Interno; así como el artículo Nº 39 sobre las causales de responsabilidad administrativa.

> *Artículo 36.—**Informes dirigidos a los titulares subordinados**. Cuando los informes de auditoría contengan recomendaciones dirigidas a los titulares subordinados, se procederá de la siguiente manera:*
>
> *a) El titular subordinado, en un plazo improrrogable de diez días hábiles contados a partir de la fecha de recibido el informe, ordenará la implantación de las recomendaciones. Si discrepa de ellas, en el transcurso de dicho plazo elevará el informe de auditoría al jerarca, con copia a la auditoría interna, expondrá por escrito las razones por las cuales objeta las recomendaciones del informe y propondrá soluciones alternas para los hallazgos detectados.*
>
> *b) Con vista de lo anterior, el jerarca deberá resolver, en el plazo de veinte días hábiles contados a partir de la fecha de recibo de la documentación remitida por el titular subordinado; además, deberá ordenar la implantación de recomendaciones de la auditoría interna, las soluciones alternas propuestas por el titular subordinado o las de su propia iniciativa, debidamente fundamentadas. Dentro de los primeros diez días de ese lapso, el auditor interno podrá apersonarse, de oficio, ante el jerarca, para pronunciarse sobre las objeciones o soluciones alternas propuestas. Las soluciones que el jerarca ordene implantar y que sean distintas de las propuestas por la auditoría interna, estarán sujetas, en lo conducente, a lo dispuesto en los artículos siguientes.*
>
> *c) El acto en firme será dado a conocer a la auditoría interna y al titular subordinado correspondiente, para el trámite que proceda.*

.....

"Artículo 38. —Planteamiento de conflictos ante la Contraloría General de la República. *Firme la resolución del jerarca que ordene soluciones distintas de las recomendadas por la auditoría interna, esta tendrá un plazo de quince días hábiles, contados a partir de su comunicación, para exponerle por escrito los motivos de su inconformidad con lo resuelto y para indicarle que el asunto en conflicto debe remitirse a la Contraloría General de la República, dentro de los ocho días hábiles siguientes, salvo que el jerarca se allane a las razones de inconformidad indicadas.*

Una vez completado el expediente que se formará al efecto. El hecho de no ejecutar injustificadamente lo resuelto en firme por el órgano contralor, dará lugar a la aplicación de las sanciones previstas en el capítulo V de la Ley Orgánica de la Contraloría General de la República, N° 7428, de 7 de setiembre de 1994".

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

2. RESULTADOS DEL ESTUDIO:

2. 1 DE LOS CONTROLES DE SEGURIDAD FISICA.

2.1.1 Área donde se ubican los servidores institucionales.

La UNED concentra la mayoría de los equipos (servidores, "switch", enrutadores, etc.) que manejan los programas e información sensible de la institución en la Dirección de Tecnología, Información y Comunicaciones (en adelante DTIC)**;** en un área ubicada en el tercer piso del edificio B, denominado "Granja de Servidores" que mide 27,09 metros cuadrados, según informe IE-9640 sobre el *"Rediseño electrónico y mejoras para cuarto de servidores"*, del 10 de octubre del 2010, realizado por el Ing. Andrés Morales Jiménez.

En el área se encuentran instalados más de 40 equipos (SERVER), y se observaron las debilidades **(Ver anexo 1)** que a continuación se enuncian:

1. Espacio:

No se evidencia la planificación del espacio de distribución entre racks, observándose poca separación, y por ende, ausencia de puntos de flexibilidad para brindar mantenimiento, además de obstaculizar la distribución del aire proporcionado por el dispositivo del control ambiental.

2. Temperatura:

El equipo de aire acondicionado instalado en esta área es de "confort", aunque cumple hasta la fecha con el objetivo de bajar la temperatura, incrementa los riesgos en los equipos de alto valor que se ubican en el Data Center, al no ser una unidad de aire acondicionado de precisión, equipo que es el indicado para realizar una climatización controlada para este tipo de Centros de Procesamiento de la Información.

Seguidamente se indican las siguientes debilidades asociadas:

a. Es un equipo de confort y no cuenta con un sistema de medición del estado ambiental o monitoreo de indicadores, que sirvan para accionar controles compensatorios, de detección o tomar acciones correctivas.
b. No cuenta con sistemas de alarmas en caso de fallo, o de autorregulación y ajuste del clima, con tecnología que permita comunicar al personal variaciones importantes como desconexión o fallas en el equipo de aire acondicionado, no cuenta con control de humedad.
c. Carece de dispositivos de detección de filtraciones de agua, entre otros, por lo que de materializarse un riesgo inherente al control ambiental, no se podría atender la contingencia con la oportunidad requerida.
d. Por el comportamiento de equipos similares se conoce que pueden expulsar agua o congelarse, afectando el control del clima o siendo una fuente de riesgo de un cortocircuito eléctrico.
e. No se evidenció que se cuenta con una instalación que permita implementar una estrategia de corriente de aire continua, que asegure mitigar los problemas causados por exceso de calor de todos los equipos por igual.
f. El piso del "Data Center" no fue construido con piso elevado, situación que afecta entre otros aspectos, las corrientes de aire que podrían obtenerse de contar con este.
g. No se observa que la distribución de los pasillos se haya planeado en función de favorecer la circulación de aire, o se haya distribuido el espacio

según el procedimiento conocido como "hot aisle/cold aisle" ("pasillo caliente/pasillo frío").

3. Infraestructura y Ambiente

Las paredes y cielorrasos del "Data Center" no distan del material del resto del área con que se construyó la DTIC:

a. No se observa que sean construidos con material aislante al calor. (Elementos ignífugos).
b. No se evidencia que sean paredes donde se haya considerado la estabilidad térmica.
c. La estancia donde se colocan los servidores no cuenta con suelos técnicos flotantes registrables.
d. No se observa que se cuente con paredes y techos sellados con un material que reduzca al máximo la aparición de polvo o estática.
e. No se encontró evidencia de un dictamen técnico o similar, que determine y asegure que esta área cuenta con la capacidad y resistencia suficiente para soportar tanto la carga o peso concentrado como distribuido, de los cuantiosos equipos instalados.

Sobre este particular, existe un acuerdo del CONRE, tomado en Sesión 1670-2011, Art. 1 inciso 1), celebrada el 14 de marzo del 2011, que le asigna al Ing. Carlos Morgan Marín, Asesor de la Rectoría, el análisis de esta situación con el fin de determinar:

> *"la solución más apropiada para un centro de datos de la UNED con un criterio de calidad que pueda certificarse internacionalmente".*

En el documento *"Análisis y Valoración de propuestas de soluciones para el centro de datos (DATA CENTER) de la UNED"* del 15 de junio del 2011, elaborado por el Ing. Morgan Marín, se indicó en la página No. 5 lo siguiente:

> *"La evaluación realizada al centro de datos actual de la UNED, evidencia que este no responde a los criterios de calidad sobre la instalación y la gestión normalmente aceptados. En conclusión, cualquier solución futura para el centro de datos de la UNED, exige la aplicación de un criterio de calidad que pueda certificarse internacionalmente y que le permita simultáneamente a la universidad valorar y financiar progresivamente la calidad que se desea para un momento dado." (**El subrayado es nuestro).***

Este documento fue enviado al Consejo de Rectoría mediante oficio R-238-2011 de 20 de junio del 2011, y el señor Morgan Marín le realiza una serie de recomendaciones al señor Rector, entre ellas:

> *"Una vez realizado el diseño del centro de datos, considerando las observaciones y recomendaciones de los Ingenieros Federico Arce Miranda y Andrés Morales Jiménez, y en consecuencia, determinada la lógica de inversión según las posibilidades financieras de la UNED, dicha lógica de inversión deberá realizarse inmediatamente, sobre todo en lo que se refiere a la redistribución espacial de los racks, UPS y transformadores secos, todo el costo podrá ascender a unos 70 millones de colones, de acuerdo a las estimaciones iniciales".*

La situación descrita, evidencia que esta debilidad es de conocimiento de la Administración e involucra la toma de acciones inmediatas por parte de la Rectoría, en este proceso gradual para establecer una solución a la seguridad física del lugar.

4. Sistema de Extinción de incendios.

a. El personal entrevistado desconoce si el equipo de detección de humo instalado se prueba periódicamente.
b. No se cuenta con un sistema de ductos y alimentación de algún producto que pueda contrarrestar los efectos de un cortocircuito eléctrico o un incendio en esta área.
c. No se evidencia que la puerta principal cuente con protección anti incendio.
d. En el momento de la inspección realizada por la Auditora responsable del estudio, los equipos para extinción de incendios se encontraban ubicados en el suelo y no en una altura adecuada para fácil acceso y uso.

5. Seguridad

a. No se cuenta con puertas con sistema de acceso automatizado con tarjeta electrónica o biométrica.
b. No se observan sistemas de circuito cerrado de televisión.

c. El área no cuenta con salidas de emergencia, que permitan al personal salir en caso de un siniestro, o que le permita al personal de bomberos acceder al sitio en una contingencia, como es el caso de incendios.

En línea con lo anterior, la norma 1.4.3 "Seguridad Física y ambiental" incisos a, b, g y h del Manual de normas técnicas para la gestión y el control de las tecnologías de información, emitido por la Contraloría General de la República y publicado en la Gaceta N° 119 del 21 de junio de 2007, señalan:

> *"La organización debe proteger los recursos de TI estableciendo un ambiente físico seguro y controlado, con medidas de protección suficientemente fundamentadas en políticas vigentes y análisis de riesgos.*
> *Como parte de esta protección debe considerar:*
>
> *a. Los controles de acceso a las instalaciones: seguridad perimetral, mecanismos de control de acceso a recintos o áreas de trabajo, protección de oficinas, separación adecuada de áreas.*
>
> *b. La ubicación física segura de los recursos TI*
> *….*
> *g. El acceso de terceros.*
> *h. Los riesgos asociados con el ambiente".*

Lo regulado por la normativa vinculante emitida por la Contraloría General de la República en adelante CGR, es coincidente con lo que al respecto establecen sobre el tema, estándares internacionales o guías de mejores prácticas en materia de Tecnologías de Información, tales como Cobit e ISO, al indicar:

> *DS12.4 "Protección Contra Factores Ambientales" de Cobit 4.1,* [1] *indica que la Administración debe:*
> *"Diseñar e implementar medidas de protección contra factores ambientales. Deben instalarse dispositivos y equipo especializado para monitorear y controlar el ambiente."*

[1] *Cobit* se fundamenta en los Objetivos de Control existentes de la "*Information Systems Audit and Control Foundation"* (ISACF), mejorados a partir de estándares internacionales técnicos, profesionales, regulatorios y específicos para la industria, ha sido desarrollado como un estándar generalmente aplicable y aceptado para las buenas prácticas de seguridad y control en Tecnología de Información (TI)

Adicionalmente la Norma ISO-27001[2] en el Objetivo de Control y controles de su anexo A, apartado A.9 "Seguridad física y ambiental" indica:

> *"A.9.1.1* ***Perímetro de Control seguridad física.***
> *Control.*
> *Se deben utilizar perímetros de seguridad (barreras tales como paredes y puertas de ingreso controlado o recepcionistas) para proteger áreas que contienen información y medios de procesamiento de información.*
>
> *A.9.1.2* ***Controles de entrada físicos***
> *Control*
> *Se deben proteger las áreas seguras mediante controles de entrada apropiados para asegurar que sólo se permita acceso al personal autorizado.*
>
> *….*
>
> *A.9.1.4* ***Protección contra Control amenazas externas y ambientales.***
> *Control*
> *Se debe diseñar y aplicar protección física contra daño por fuego, inundación, terremoto, explosión, disturbios civiles y otras formas de desastre natural o creado por el hombre.*
>
> *….*
>
> *A.9.2* ***Seguridad del equipo Objetivo***
> *Objetivo: Evitar la pérdida, daño, robo o compromiso de los activos y la interrupción de las actividades de la organización.*
>
> *A.9.2.1* ***Ubicación y protección del equipo.***
> *Control*
> *El equipo debe estar ubicado o protegido para reducir los riesgos de las amenazas y peligros ambientales, y las oportunidades para el acceso no autorizado.*
>
> *A.9.2.2* ***Servicios públicos.***
> *Control*
> *El equipo debe ser protegido de fallas de energía y otras interrupciones causadas por fallas en los servicios públicos."*

[2] ISO/IEC 27001 fue preparado por el Comité Técnico Conjunto ISO/IEC JTC 1, Tecnología de la información, Subcomité SC 27, Técnicas de seguridad TI.

Sobre esta realidad, el objetivo de control DS12.3 Acceso Físico, de Cobit 4.1 indica que la Administración debe:

> *"Definir e implementar procedimientos para otorgar, limitar y revocar el acceso a locales, edificios y áreas de acuerdo con las necesidades del negocio, incluyendo las emergencias. El acceso a locales, edificios y áreas debe justificarse, autorizarse, registrarse y monitorearse. Esto aplica para todas las personas que accedan a las instalaciones, incluyendo personal, clientes, proveedores, visitantes o cualquier tercera persona."*

Sobre las debilidades detectadas, tanto el Encargado de Seguridad Digital como el Director de la DTIC fueron consultados, rescatando las siguientes observaciones:

El Ing. Johnny Saborío Alvarez, Analista de Sistemas, con las funciones de Encargado de Seguridad Digital en entrevista del 23 de junio del 2011, dijo con respecto al control de acceso:

> *"se usaba en la DTIC un sistema electrónico de tarjeta pero con la remodelación efectuada al sitio, no se volvió a utilizar."*

El Director de la DTIC, Mag. Francisco Durán Montoya, manifestó en el oficio DTIC-2011-161 del 26 de julio de 2011, sobre la carencia de un control para el acceso que:

> *"Desde el año 2008 se han realizado diferentes reportes y solicitudes para la atención al tema del Control de Acceso, sin embargo no se ha realizado ninguna gestión hasta el momento."*

Todas las debilidades señaladas, podrían exponer a la Administración a pérdidas sensibles de información y comprometer el cumplimiento de los objetivos institucionales, con efectos financieros negativos de llegar a materializarse pérdidas de activos.

2.1.2 Sobre el libro de anotaciones para acceso a la DTIC

En el periodo de estudio se observó el uso de un libro de anotaciones para registrar el acceso a la DTIC, en este se anota la entrada y salida de personas ajenas a esta Dirección. Se solicita al visitante que anote el nombre, dependencia, hora de entrada y salida; sin embargo, en algunas ocasiones los datos requeridos no son registrados en su totalidad.

Refiriéndose a esta situación, el Director de la DTIC informó que: "esta bitácora no es monitoreada"; revelando que aunque exista ese control, no es supervisado por ningún funcionario de la DTIC, tampoco han sido asignadas formalmente tales funciones a algún funcionario.

Al respecto, el Manual de normas de Control Interno para el sector público publicado en la Gaceta N°26 de 6 febrero de 2009, en sus normas 4.4.1 "Documentación y registro de la gestión institucional" y 4.5.1 "Supervisión constante" indican que:

> *"4.4.1 El jerarca y los titulares subordinados, según sus competencias, deben establecer las medidas pertinentes para que los actos de la gestión institucional, sus resultados y otros eventos relevantes, se registren y documenten en el lapso adecuado y conveniente, y se garanticen razonablemente la confidencialidad y el acceso a la información pública, según corresponda.*
>
> *4.5.1 El jerarca y los titulares subordinados, según sus competencias, deben ejercer una supervisión constante sobre el desarrollo de la gestión institucional y la observancia de las regulaciones atinentes al SCI, así como emprender las acciones necesarias para la consecución de los objetivos".*

Como complemento a este criterio, en la Normativa ISO-27001, en su apartado "4.3.3 Control de registros", se aborda el tema señalado, normando:

> *"Se deben establecer y mantener registros para proporcionar evidencia de conformidad con los requerimientos y la operación efectiva del SGSI. Deben ser protegidos y controlados. El SGSI[1] debe tomar en cuenta cualquier requerimiento legal o regulador relevante. Los registros deben mantenerse legibles, fácilmente identificables y recuperables. Se deben documentar e implementar los controles necesarios para la identificación, almacenaje, protección, recuperación tiempo de retención y disposición de los registros. Se deben mantener registros del desempeño del proceso tal como se delinea en 4.2 y de todas las ocurrencias de incidentes de seguridad significativos relacionados con el SGSI[3].*
>
> *EJEMPLO. Son ejemplos de registros los libros de visitantes, los registros de auditoría y las solicitudes de autorización de acceso".*

[3] Sistema de Gestión de Seguridad de la Información (SGSI)

Esta situación podría eventualmente dejar al descubierto accesos no autorizados a la DTIC, inclusive al "DATA CENTER", con el riesgo de no contar con evidencia o registros de personal interno, e incluso externo a la UNED que visita el área para realizar diferentes tareas, entre ellas, la de mantenimiento a los servidores institucionales u otros trabajos contratados.

2.1.3 Del registro de algunos Server del "Data Center" en el sistema de inventario.

Los equipos principales denominados "Server" (servidores), suman un valor aproximado de $ 642.200.00, según datos cuantificados en el oficio DTIC-2010-230 del 13 de diciembre de 2010, enviado por el MSc. Vigny Alvarado Castillo, en ese entonces Director de la DTIC, al Lic. Alverto Cordero Fernández, Director Financiero, en respuesta al oficio DF 421-2010.

Dicha suma no se pudo corroborar en el listado de activos aportado por la Oficina de Contabilidad General, al determinarse que existen errores en el registro y clasificación de los mismos, ya que en la información suministrada por esa Unidad se evidenció que se registraron contablemente dispositivos que son "Servidores" con clase 676 y 677 como clase 624, que corresponde a "switch" o equipo de comunicación.

Sobre esta situación la normativa vinculante sobre esta materia Manual de Normas de Control Interno para el Sector Público, aprobado por la CGR, y publicado en la Gaceta N° 26 de 6 de febrero de 2009 en su apartado 4.4.5 "Verificaciones y conciliaciones periódicas" señala:

> La exactitud de los registros sobre activos y pasivos de la institución debe ser comprobada periódicamente mediante las conciliaciones, comprobaciones y otras verificaciones que se definan, incluyendo el cotejo contra documentos fuentes y el recuento físico de activos tales como el mobiliario y equipo, los vehículos, los suministros en bodega u otros, para determinar cualquier diferencia y adoptar las medidas procedentes.

Esta situación podría exponer a la administración a una inadecuada planificación de contrataciones futuras, de bienes o de mantenimiento, además no obtendría información confiable y oportuna sobre la cantidad y estado de los bienes, para el

análisis y toma de decisiones administrativas frente a su estado y uso eficiente, así como la priorización de recursos para inversión.

2.1.4 Del Control de salida de activos en el "DATA CENTER".

Para el registro de salida de activos de la DTIC, se utiliza un documento en formato Microsoft Word, que se imprime una vez que se completa la información requerida ante la salida de activos de esta Dirección; sin embargo, se observaron algunas debilidades de control **(ver anexo2)**, porque aunque indica el nombre de la persona que despacha el activo, no se solicita, y por ende no consta en ese registro la firma del funcionario que autoriza la salida del activo, ni se estampa el sello de la DTIC.

Sobre esta situación, se consultó al Director de la DTIC, Mag. Francisco Durán Montoya en entrevista del 1 de julio de 2011: ¿Los equipos, la información o software son solicitados al encargado del "Data Center" por medio de un proceso formal utilizando formulario u oficio? indicando que:

> *"existe un procedimiento no escrito, pero cualquier funcionario de la DTIC puede entregar un activo".*

Sobre este particular el señor Durán Montoya, durante la misma entrevista, aseveró que:

> *"Los activos son cedidos a funcionarios de la institución que diariamente ven y que tienen la autoridad para retiro de estos fuera del "DATA CENTER"; los contratistas y terceras personas que pertenecen ya sea a empresas que dan mantenimiento no están claramente identificadas, no siempre es la misma persona que llega a retirar un activo; no se les solicita identificación."*

En este aspecto, las normas 4.3.3 "Regulaciones y dispositivos de seguridad"; y 4.4.2 "Formularios Uniformes" del Manual de Normas de Control Interno para el Sector Público N-2-2009-CO-DFOE emitido por la CGR, publicado en la Gaceta N° 26 de 6 de febrero de 2009, indican que:

> *"4.3.3 El jerarca y los titulares subordinados, según sus competencias, deben disponer y vigilar la aplicación de las regulaciones y los dispositivos de seguridad que se estimen pertinentes según la naturaleza de los activos y la relevancia de los riesgos asociados, para garantizar su rendimiento óptimo y su protección contra pérdida, deterioro o uso irregular, así como para prevenir cualquier daño a la integridad física de los funcionarios que deban utilizarlos".*

> *"4.4.2 El jerarca y los titulares subordinados, según sus competencias, deben disponer lo pertinente para la emisión, la administración, el uso y la custodia, por los medios atinentes, de formularios uniformes para la documentación, el procesamiento y el registro de las transacciones que se efectúen en la institución. Asimismo, deben prever las seguridades para garantizar razonablemente el uso correcto de tales formularios. (El subrayado es nuestro)."*

La falta de puntos de control en los documentos utilizados en el trámite de transacciones institucionales como la de referencia, podría generar incumplimiento en la normativa vinculante, situación que expone eventualmente a la Administración Activa a pérdidas de equipo e información, y al personal involucrado ante una entrega indebida de equipo, a posibles causales de responsabilidad en sus diferentes tipos.

2.1.5 Sobre el Inventario de activos en el "DATA CENTER" realizado por la Auditoría Interna.

La DTIC carece de un listado de activos actualizado, esto fue evidenciado en el inventario de equipos que realizó esta Auditoría Interna, en el "DATA CENTER" versus la información suministrada mediante documento sin número de oficio enviado por el Director de la DTIC, en ese entonces el Msc. Vigny Alvarado Castillo, de fecha 16 de febrero del 2011. Durante la verificación se evidenció que:

1) Cinco (5) de los equipos no coincidían con número de patrimonio que indicaba el listado suministrado.
2) Diez (10) activos no estaban en el sitio; no obstante, posterior a la revisión de los oficios de traslado de equipo emitidos por la DTIC, se determinó que esos activos fueron enviados a otros departamentos o dados de baja.

Mantener un inventario actualizado de equipos ubicados en la Granja de Servidores de la DTIC, permite, entre otras cosas, planear adecuadamente su mantenimiento, actualización e incluso su remplazo, lo cual favorece la continuidad de las operaciones de la Organización.

Toda esta situación incumple lo establecido en las normas "4.4.5 Verificaciones y conciliaciones periódicas" y "5.6.3 Utilidad", del Manual de normas de control interno para el sector público N-2-2009-CO-DFOE, emitido por la CGR publicado en la Gaceta N° 26 del 6 de febrero de 2009, que indican:

> *4.4.5 "Verificaciones y conciliaciones periódicas*
> *La exactitud de los registros sobre activos y pasivos de la institución deber ser comprobada periódicamente mediante las conciliaciones, comprobaciones y otras verificaciones que se definan, incluyendo el cotejo contra documentos fuentes y el recuento físico de activos tales como mobiliario y equipo,…., para determinar cualquier diferencia y adoptar las medidas procedentes".*
> *…*
>
> *5.6.3 "Utilidad La información debe poseer características que la hagan útil para los distintos usuarios, en términos de pertenencia, relevancia, suficiencia y presentación adecuada, de conformidad con las necesidades específicas de cada destinatario".*

Según entrevista aplicada el 01 de julio del 2011, el Director de la DTIC, sobre el tema expresó:

> *"no existe un encargado de manejar esta información razón por la que se den diferencias en los datos suministrados en lo que corresponde a inventario del "DATA CENTER".*

Esta situación podría exponer negativamente a la Institución en caso de materializarse un evento indeseado como robo y hurto, o ante una eventual catástrofe natural o producto de un delito, con las correspondientes pérdidas no solo económicas por el valor del activo, sino a la privación de información sensible. Además debilita el control interno al no existir una asignación de responsabilidades para la ejecución de la tarea de registro y control de activos. También podría limitar a las Autoridades Universitarias en la toma de decisiones relacionada con el aseguramiento, mantenimiento y futuras inversiones tecnológicas.

2.2 De la Identificación de activos del "DATA CENTER" en el contrato de seguro.

La UNED paga el contrato de seguro, N° 01 01 EQE-4652-05 el cual mantiene una vigencia anual al 01 de setiembre de cada año; a saber "¢548.664.844,00. Equipo Fijo Sabanilla y ¢5.647.289,00 en Discos Duros Sabanilla" entre otros. A la fecha no están identificados por número de placa, número de serie y marca, los activos que están cubiertos por la póliza respectiva, de acuerdo con el oficio OCG-052-2011 del 31 de mayo del 2011, enviado por el Mag. Carlos Chaves Quesada, Contador General.

Al respecto el Artículo 12. —"**Deberes del jerarca y de los titulares subordinados en el sistema de control interno"** de la Ley General de Control Interno publicada en la Gaceta N°169 de 04 de setiembre de 2002. Indica que:

> *"En materia de control interno, al jerarca y los titulares subordinados les corresponderá cumplir, entre otros, los siguientes deberes:*
>
> *a) Velar por el adecuado desarrollo de la actividad del ente o del órgano a su cargo.*
> *b) Tomar de inmediato las medidas correctivas, ante cualquier evidencia de desviaciones o irregularidades".*

Además, la norma 4.3 "Protección y conservación del patrimonio", del Manual de normas técnicas para la gestión y el control de las tecnologías de Información N-2-2007-CO-DFOE, emitida por la CGR y publicada en la Gaceta N°119 del 21 de junio de 2007, indica que:

> *4.3 "El jerarca y los titulares subordinados, según sus competencias, deben establecer, evaluar y perfeccionar las actividades de control pertinentes a fin de asegurar razonablemente la protección, custodia, inventario, correcto uso y control de los activos pertenecientes a la institución, incluyendo los derechos de propiedad intelectual".*

Sobre este particular se consultó a la Licda. Lorena Aguilar Solano, Coordinadora de seguros de la UNED, en entrevista efectuada el 21 de julio del 2011 indicando que:

> *"Estoy en este puesto aproximadamente hace un año y tengo a cargo todo el proceso para determinar los activos que se encuentran cubiertos por la póliza está llevándose a cabo pues anteriormente no se manejaba este control, todo esto se pudo realizar luego de consultoría efectuada por el CICAP (Centro de Investigación y Capacitación en Administración Pública) de la Universidad de Costa Rica en el mes de marzo de 2011 y en donde "se efectuó un análisis al contrato de Equipo Electrónico vigente con el fin de determinar las condiciones de aseguramiento, políticas de control y manejo del riesgo y reportes al instituto para establecer la cobertura según indica este informe.(pág. 3 resumen ejecutivo)."*
>
> *Se efectuó una solicitud ante el INS para modificación a la póliza y en el mes de Agosto (día 11) se tienen prevista la visita del agente del INS para verificar la infraestructura en lo que respecta a*

> *instalaciones eléctricas, sistemas de detección y protección contra incendios, brigada o grupos de emergencia, entre otros".*

Igualmente indicó posteriormente en mensaje de correo electrónico de 14 de Marzo de 2012, que: *"La propuesta ya la envió el INS pero está por aprobar en la Vicerrectoría Ejecutiva"*

Esta condición genera que la institución pague periódicamente importantes sumas de dinero al Instituto Nacional de Seguros, por la adquisición de seguros, con la finalidad de proteger sus equipos, no obstante, al no estar identificados tales activos por placa de inventario, marca y serie en la póliza respectiva, ante cualquier pérdida o evento adverso, resultará realmente difícil hacer efectivo algún reclamo a la institución aseguradora, perdiéndose la finalidad u objetivo de adquisición del seguro y por ende el posible resarcimiento.

2. 3 Sobre seguridad lógica del "Data Center"

2.3.1 De la creación e inhabilitación de usuarios en el correo electrónico y los sistemas de información institucional.

El activo más importante que posee la institución luego de sus funcionarios, es la información, por lo tanto, deben existir técnicas más allá de la seguridad física que la aseguren, tales como las que brinda la "Seguridad Lógica" (aplicación de barreras y procedimientos que resguarden el acceso a los datos y sólo se permita su acceso a las personas autorizadas para hacerlo).

Los controles de acceso son establecidos con el objetivo de resguardar la información confidencial de accesos no autorizados. A continuación de detallan las debilidades detectadas:

1. Administración de cuentas y claves de usuarios

No se encontró evidencia de un procedimiento escrito, debidamente aprobado, divulgado y actualizado, que regule entre otras, las actividades relacionadas con la creación e inhabilitación de usuarios, el control, mantenimiento, inactividad de usuarios; entrega, reasignación de contraseñas de la institución. Según el Director de la DTIC Mag. Francisco Durán Montoya en entrevista sobre el tema, efectuada el 01 de julio del 2011, explicó:

> *"se cuenta con un procedimiento por escrito a nivel de Recursos Humanos para que las jefaturas reporten los movimientos de personal para que se realicen los cambios respectivos".*

A pesar de la carencia de procedimientos escritos que regulen la creación de los diferentes tipos de usuarios, ya sea para solicitud de usuario de correo electrónico, uso de equipos en la red de datos y acceso a los sistemas de información, según el Mag. Durán Montoya en entrevista efectuada el 26 de agosto de 2011; "la DTIC cuenta con varios procesos no documentados, por ejemplo, para acceso a los sistemas de información, el jefe o encargado de cada oficina es quien envía la solicitud al Director de la DTIC, indicando en el oficio los sistemas que requieren ser utilizados por cada funcionario"; además hizo referencia a la página web de la UNED en donde se encuentra un formulario de solicitud para acceso a equipos de la red institucional.

Según el Mag. Johnny Saborío Álvarez quien ejerce las funciones de Encargado de Seguridad Digital, en la entrevista efectuada el 23 de Junio de 2011, ante la consulta formulada por parte de esta unidad Fiscalizadora, sobre la existencia de un proceso para realizar la administración de las cuentas de usuarios en caso de cese por pensión, traslado de funciones o muerte, indicó:

> *"Se envía nota indicando el movimiento, pero se han encontrado casos de personas que hasta se han pensionado y siguen activas en algún sistema; o la persona puede que esté en la UNED pero en otra área, con acceso a un sistema que ya no debe manejar, esto porque no se comunica a la DTIC sobre el movimiento y no tenemos a nivel de seguridad digital de la DTIC documentación que indique cual es el procedimiento a seguir. Para el caso de los funcionarios de DTIC que se trasladan, se les cambia la cuenta de correo electrónico, esto se efectúa mediante oficio en donde se les explica los motivos del cambio de código de usuario".*

En relación con lo anterior, esta Auditoría Interna ubicó la existencia del documento denominado "*Uso de correo electrónico*", aprobado por el Consejo de Rectoría en Sesión N°1605 Artículo IV, inciso 2), celebrada el 26 de agosto de 2009, que hace referencia a la "*Gestión y control del servicio de correo electrónico*" y en su punto No. 1, establece:

> *"N°1. Indicar a la Oficina de Recursos Humanos la responsabilidad de informar a la Dirección de Tecnología, Información y Comunicaciones (DTIC) cuando un funcionario deja de laborar para la institución, con el fin de eliminar la correspondiente cuenta de correo electrónico.(El subrayado es nuestro)"*

Con esta regulación se normaliza únicamente lo que corresponde a exclusión de cuentas de correo electrónico; no obstante, queda desprotegido lo que concierne a inhabilitación de cuentas y usuarios de los restantes sistemas de información (Red), no encontrándose evidencia escrita de normativa emitida por parte del CONRE o por el Consejo Universitario que establezca la acción a ejecutar cuando un funcionario se traslada a otra dependencia, e incluso cuando cambia de puesto en la misma dependencia, y en virtud de sus nuevas funciones podría requerir un nuevo perfil informático. Esta situación se agudiza cuando el funcionario deja de laborar para la UNED y a falta de regulación administrativa, eventualmente podría conservar su acceso a los sistemas institucionales y correo electrónico.

2. Inhabilitación de usuarios

Con el oficio AI-135-2011 del 26 de agosto del 2011, se le solicitó a la Mag. Rosa María Vindas Chávez, Jefe de la Oficina de Recursos Humanos en adelante ORH, un listado de funcionarios de la UNED que estén en la condición de "cese de labores", ya sea por jubilación, renuncia o muerte y en condición de "traslado" a otras oficinas, con el fin de verificar si las cuentas de usuario (a), aún están activas en la plataforma AS/400 y correo electrónico.

Según el listado suministrado por la ORH, se reporta que 127 personas se han desvinculado por renuncia, jubilación o muerte desde el 31 de julio de 2009 hasta el 31 de julio de 2011. De acuerdo con el punto N°1 del documento llamado "*Uso de correo electrónico*" aprobado por el Consejo de Rectoría, la Oficina de Recursos Humanos debe comunicar a la DTIC cuando un funcionario deja de laborar para la institución para que se efectúe el procedimiento correspondiente.

Sin embargo, se identificaron debilidades en la gestión de inhabilitación de usuarios, al comparar el listado suministrado por la ORH versus la información contenida en el Active Directory (Herramienta utilizada para control de acceso a nivel de software en la DTIC), evidenciándose las siguientes condiciones:

1) Diecisiete (17) personas continúan con el correo electrónico habilitado.

2) Dieciocho (18) personas continúan activas en el sistema AS/400. (no todos los funcionarios cuentan con acceso a sistemas de información).

3) Setenta (70) funcionarios fueron comunicados mediante oficios a la DTIC para inhabilitación.

De las consultas relacionadas con la existencia de normativa interna, en lo que respecta a "Seguridad Lógica", el Mag. Johnny Saborío Alvarez facilitó a esta Auditoría Interna el documento llamado "Seguridad Digital", acuerdo tomado por el Consejo de Rectoría en sesión No. 1160-2000, Art XVIII, que a letra dice:

> *"La seguridad Digital es una política que debe establecerse de tal manera que no disminuya la capacidad de la organización y que le permita a todos los usuarios de la red realizar y cumplir con sus funciones y tareas de forma adecuada y eficiente pero igualmente segura y eficaz en la protección de los siguientes recursos:*
>
> - *Información y/o datos ubicados en archivos o bases de datos de cualquier equipo propiedad de la UNED.*
> - *Computadoras, servidores de acceso o remotos ubicados en la granja de servidores o Sala de Operaciones de la Oficina de Sistemas, equipos interconectados a la red institucional.*
> - *Equipo telemático, enrutadores, conmutadores (switch), concentradores (hub), instalados en los gabinetes ubicados en algunas oficinas.*
> - *Estaciones de trabajo, microcomputadoras o pc's propiedades de la UNED ubicadas en todas las oficinas o dependencias de la UNED.*
> - *Cableado Estructurado, cables de red o eléctricos para equipo computarizado.*
> - *Software, programas o sistemas de información propiedad de la UNED o en convenio". (el subrayado es nuestro).*

En el documento supra, se considera el resguardo de la información institucional, sin embargo no se detalla cuales mecanismos o acciones deberá implantar la administración para realizar la inhabilitación de usuarios de los sistemas de información, una vez que exista una desvinculación del usuario con la UNED.

Existe un apartado dentro del texto que hace referencia a las medidas que deben establecerse para resguardo de información, sin embargo no abarca lo referente a mantenimiento de cuentas por parte de la Administración:

> - "Enlistar a los usuarios (funcionarios y funcionarios) que tendrán acceso a los recursos.
> - Informar por medio de los Consejos de Vicerrectoría cuál es el uso adecuado de la red y los recursos, así como las responsabilidades de su manejo.

- La Oficina de Sistemas es la única instancia que puede instalar e interconectar equipos a la red institucional, conceder accesos y aprobar el uso de la red y sus recursos.
- La oficina de sistemas es la única instancia que puede asignar privilegios de administrador de red, así como sus responsabilidades y deberes.
- Los propietarios de los sistemas de información son los responsables por los datos que se incluyan y por la información que se emite, por lo que la Oficina de Sistemas sólo con la autorización y a solicitud de los propietarios de los sistemas de información podrán emitir o extraer algún tipo de datos o información".

Las condiciones anteriormente comentadas, van en contra de lo establecido en el artículo N°15 "Actividades de Control" de la Ley General de Control Interno N° 8292, publicada en la Gaceta N°169 del 4 de Setiembre de 2002, que exterioriza:

> *Artículo N°15 "Respecto de las actividades de control, serán deberes del jerarca y de los titulares subordinados, entre otros, los siguientes:*
> *a) Documentar, mantener actualizados y divulgar internamente, las políticas, las normas y los procedimientos de control que garanticen el cumplimiento del sistema de control interno institucional y la prevención de todo aspecto que conlleve a desviar los objetivos y las metas trazados por la institución en el desempeño de sus funciones.*
> *b) Documentar, mantener actualizados y divulgar internamente tanto las políticas como los procedimientos que definan claramente, entre otros asuntos, los siguientes:*
> *i. La autoridad y responsabilidad de los funcionarios encargados de autorizar y aprobar las operaciones de la Institución.*
> *ii. La protección y conservación de todos los activos institucionales.*
> *iii. El diseño y uso de documentos y registros que coadyuven en la anotación adecuada de las transacciones y los hechos significativos que se realicen en la Institución. Los documentos y registros deberán ser administrados y mantenidos apropiadamente".*

Además en la norma: 1.4" Gestión de la seguridad de la Información"; del Manual de normas técnicas para la gestión y control de las tecnologías de información de la CGR se indica:

> *"1.4 La organización debe garantizar, de manera razonable, la confidencialidad, integridad y disponibilidad de la información, lo que implica protegerla contra uso, divulgación o modificación no autorizados, daño o pérdida u otros factores disfuncionales:*

-La implementación de un marco de seguridad de la información.
…
-El control de acceso.
- La seguridad en la implementación y mantenimiento de software e infraestructura tecnológica".

La carencia de un procedimientos que norme o regule el proceso de solicitud, asignación y administración de cuentas de usuarios en armonía con los controles para asegurar razonablemente su manejo a nivel administrativo y tecnológico, podría ser, entre otros, uno de los factores que genera las deficiencias encontradas, además del incumplimiento a los acuerdos del Consejo de Rectoría, siendo un elemento que debilita el control interno.

Esta situación eventualmente podría exponer a la Administración activa a que ex funcionarios que ya no tienen ninguna relación laboral con la UNED o personas ajenas a la entidad utilizando cuentas activas de ex funcionarios, tengan acceso a los sistemas de información y al uso de recursos institucionales como correo electrónico, generando escenarios que podrían atentar contra los atributos de confidencialidad e integridad de la información, al materializarse un acceso no autorizado.

2.3.2 Sobre controles de acceso lógico a las de Bases de Datos.

Según los datos suministrados por la DTIC, a la fecha del estudio de campo, la UNED cuenta con setenta (70) Sistemas de Información en producción, de ellos siete (7) inactivos; se administran cuatro plataformas de bases de datos: DB2(AS/400), SQL Server, ORACLE y MySQL; en ellas se crean los diferentes objetos de Bases de Datos para los sistemas Institucionales, tanto para los que se desarrollan con recursos internos como para los que son adquiridos. En el ambiente Oracle, la base de datos se denomina "PUNED", en el ambiente SQL Server "BD Produccion" y en el ambiente IBM-AS/400 opera la Base de Datos "DB2 s1030557". Lo anterior fue expresado en entrevista efectuada el 16 de agosto de 2011, por el administrador de bases de datos, Mag. Gonzalo Rodríguez Benavides, por lo que es sumamente importante determinar la existencia, confiabilidad y cumplimiento de los controles de acceso lógico establecidos a los funcionarios de la UNED para el acceso a sistemas de información sensible como lo son Contabilidad, Planillas, Presupuesto, y Administración de Estudiantes, entre otros. Consecuentes con ello, se efectuaron indagaciones y se determinó que:

1. La DTIC no cuenta con información disponible o un listado de todos los usuarios que tienen acceso a cada uno de los diferentes sistemas institucionales. En la solicitud realizada con el oficio AI-118-2011 del 20 de julio del 2011 al Director de la DTIC Mag. Durán Montoya, a fin de que suministre un listado de

los usuarios de la institución con acceso a los sistemas de información y sus respectivos roles, indicó en oficio DTIC-2011-161 de 26 de julio 2011, lo siguiente:

> *"Le solicito por favor un plazo no menor a tres meses para la entrega de la información solicitada, esto debido a que se requiere realizar la recopilación de la misma". (El subrayado es nuestro).*

Esta debilidad de control, a su vez constituyó un impedimento para realizar las pruebas respectivas que tenía planeado efectuar esta Auditoría Interna, sobre el ambiente del AS/400 donde se encuentran sistemas sensibles.

2. Con oficio AI-118-2011 del 20 de julio del 2011, se solicitó información al Director de la DTIC, referente al detalle de los Sistemas de Información en producción a los que los funcionarios de la DTIC tienen acceso, y sus roles asignados en cada sistema. Al respecto, una vez analizada su respuesta, se determinó que no concordaba con la misma información que le fue solicitada posteriormente al Mag. Gonzalo Rodríguez Benavides, DBA de la DTIC, y que nos facilitó mediante entrevista del 16 de agosto de 2011.

Según el Mag. Rodríguez Benavides, para otorgar permisos de acceso y roles a las Bases de Datos, en el caso de los analistas desarrolladores de sistemas, indicó:

> *"Para cada proyecto hay un analista y un líder, el analista es quien dice que es lo que se requiere para cada proyecto; a partir de ahí se efectúan reuniones para empezar a trabajar en la estructura de datos".*

3. La plataforma de IBM–AS/400, es la más antigua y en ella se concentra aproximadamente el 80% de los sistemas institucionales, como por ejemplo: Sistema Financiero Contable, Sistema de Administración de Estudiantes, Sistema de Presupuesto y Planillas (Sistemas Legados). En contraste con la importancia de esta plataforma institucional, el Administrador de Base de Datos, Mag. Rodríguez Benavides expresó en acta de entrevista efectuada el 16 de agosto del 2011, lo siguiente:

> *"Como DBA no administro esta plataforma"*

Sobre este particular, se consultó al Director de la DTIC sobre las razones existentes para que el único DBA de la UNED no administre esta plataforma, y mediante entrevista del 26 de agosto del 2011 señaló:

> *"A la fecha se ha llevado así; sin embargo hay un proyecto para separación de los ambientes".*

Igualmente reveló que:

> *"Los analistas son quienes realizan las modificaciones que sean requeridas y son fiscalizados por los líderes de proyecto".*

El escenario descrito anteriormente, representa la situación tipificada desde el punto de vista del control interno como "incompatibilidad de funciones", dado que los analistas no deben efectuar modificaciones a nivel de programación en la base de datos; menos contando la UNED con un Administrador de Bases de Datos desde el 26 de octubre de 2000, según acción de personal N°0222718, ya que el DBA, en razón de su experiencia y formación académica, debería tener asignada la responsabilidad de mantener y operar todas las bases de datos que conforman el o los sistema de información de la institución.

Según el Manual de Descriptivo de Puestos, dentro de las tareas típicas del puesto Administrador de Base de Datos, están las siguientes:

> *"1. Supervisar y controlar el diseño e implementación de las bases de datos institucionales. Asegurar la Integridad y consistencia de las bases de datos.*
>
> *2. Monitorear el desempeño de las Bases de Datos, y aplicar los conocimientos técnicos para identificar y resolver los problemas que se deriven en el desarrollo de su trabajo".* (**El subrayado es nuestro**).

4. Ya que el encargado de Bases de Datos (DBA) no administra todas las Bases de Datos que la UNED tiene en funcionamiento, se verificaron los controles de seguridad para el registro de transacciones, encontrado que las bitácoras de acceso únicamente se manejan en ambiente SQL server y Oracle; al respecto, el Mag. Rodríguez Benavides, en acta de entrevista realizada el 16 de agosto del 2011, indicó:

> *"aunque están activas, no son verificadas ya que nunca se ha llegado a un consenso de quien debe efectuar ese control y cuáles son los procedimientos a seguir en caso de encontrar alguna anomalía, es decir intentos fallidos de ingreso o ingresos injustificados".* (**El subrayado es nuestro**).

Estas bitácoras no aplican a todas las tablas de esos motores de bases de datos, ni se tiene respuesta del criterio técnico utilizado o valoración del riesgo para su selección, así como la razón por la cual las que sí tienen bitácora no se verifican.

La carencia de controles, y el no aprovechar al máximo el recurso humano especializado que dispone la DTIC para la asignación de la totalidad de funciones relacionadas con la administración de Bases de Datos en el equipo AS/400, genera debilidades de control, máxime cuando es la base de datos que maneja el 80% de los Sistemas de Información de la Institución.

Debe considerarse que el contar únicamente con un funcionario encargado de la administración de las bases de datos a nivel institucional, no solo representa una alta carga laboral, sino que aumenta el riesgo de dependencia, situación que expone a la institución, por lo que deberá valorarse el reforzar esa área funcional, con recursos adicionales.

Para el desarrollo de la actividad fiscalizadora desplegada por esta Auditoría Interna, se produce una clara afectación que tiene origen no solo en la ausencia de controles suficientes y pertinentes aplicadas a las BD institucionales, sino que también encuentra asidero en la falta de implementación de bitácoras históricas de control de acceso y transaccionales, que deben ser definidas a partir de estudios técnicos de sensibilidad y criticidad de la información o de un análisis de riesgos; situación que debilita el Control Interno de la UNED y brinda condiciones que podrían exponer a la Administración a que se realicen actividades no autorizadas sobre la información guardada en la Base de Datos, y se podrían favorecer eventualmente condiciones para la materialización de actividades ilícitas, tales como encubrimientos, o incluso delitos informáticos.

5. Otro aspecto evaluado en este estudio es la suscripción de “acuerdos o contratos con terceros sobre la confidencialidad de la información”, tomando en cuenta que la institución tiene servicios contratados para el mantenimiento en Bases de Datos y equipos instalados en el “Data Center”, adjudicados a empresas externas (“Outsourcing” o tercerización).

Sobre este particular, se consultó al Director de la DTIC, si son establecidos y revisados periódicamente acuerdos de confidencialidad, indicando que: “no existen este tipo de estipulaciones dentro de los mismos” según respuesta consulta efectuada el 1 de julio del 2011.

Según revisión efectuada a los contratos de mantenimiento enviados con

oficio DTIC-2011-245 de 22 de noviembre del 2011, a saber: Oracle (mantenimiento); Citrix (contratación); IBM (mantenimiento GBM); Sistema Datamedix (contratación y/o mantenimiento); Checkbox (contratación y/o mantenimiento); Cisco Smartnet o equivalente (mantenimiento), se evidenció que efectivamente no se cuenta con estas disposiciones aplicables a las personas externas que prestan servicio privado de mantenimiento en los servidores de información de la institución.

Según consulta efectuada al Director de la DTIC, con respecto a las capacitaciones del personal encargado de seguridad digital y base de datos indicó que:

> *"En el año 2010 el encargado de seguridad Mag. Johnny Saborío, se capacitó en el curso Programa de Gestión de la Seguridad de la Información, que abarca el tema de seguridad de la información y los riesgos informáticos y en el año 2011 llevó el curso de Introducción al Control Interno, que imparte la UNED, y en este se ve los temas de los Controles en la Gestión administrativa y poco de la Valoración del Riesgo Institucional. En el caso de nuestro compañero Gonzalo Rodríguez, DBA, en los últimos dos años no ha llevado cursos de capacitación".*

Con lo anterior, se incumple lo establecido en las normas 1.4.1 "Implementación de un marco de seguridad de la información" incisos b y c; 1.4.5 "Control de acceso"; 4.3 "Administración de datos", todas del manual de Normas Técnicas para la gestión y el control de las tecnologías de información de la Contraloría General de la República que indica:

> *"1.4.1 "La organización debe implementar un marco de seguridad de la información, para lo cual debe:*
> ***...***
> *b. Mantener una vigilancia constante sobre todo el marco de seguridad y definir y ejecutar periódicamente acciones para su actualización.*
> *c. Documentar y mantener actualizadas las responsabilidades tanto del personal de la organización como de terceros relacionados"* **(El subrayado es nuestro)**".
>
> *"1.4.5 La organización debe proteger la información de accesos no autorizados. Para dicho propósito debe:*
>
> *a. Establecer un conjunto de políticas, reglas y procedimientos relacionados con el acceso a la información, al software de base y la aplicación, a las bases de datos y a las terminales y otros recursos de comunicación".*

> *4.3 "La organización debe asegurarse de que los datos que son procesados mediante TI corresponden a transacciones válidas y debidamente autorizadas, que son procesados en forma completa, exacta y oportuna, y transmitidos, almacenados y desechados en forma íntegra y segura."*

Igualmente las normas 4.5.1 "Supervisión constate"; 5.6 "Calidad de la información"; 5.6.1 "Confiabilidad"; 5.6.2 "Oportunidad"; 5.6.3 "Utilidad"; todas del manual de Normas de Control Interno para el Sector Público N-2-2009-CO-DFOE de la CGR que establecen:

> *4.5.1 "El jerarca y los titulares subordinados, según sus competencias, deben ejercer una supervisión constante sobre el desarrollo de la gestión institucional y la observancia de las regulaciones atinentes al SCI, así como emprender las acciones necesarias para la consecución de los objetivos".*
>
> *5.6 "El jerarca y los titulares subordinados, según sus competencias, deben asegurar razonablemente que los sistemas de información contemplan los procesos requeridos para recopilar, procesar y generar información que responda a la necesidades de los distintos usuarios. Dichos procesos deben estar basados en un enfoque de efectividad y mejoramiento continuo.*
>
> *Los atributos fundamentales de la calidad de la información están referidos a la confiabilidad, oportunidad y utilidad".*
>
> *5.6.1 "La información debe poseer las cualidades necesarias que la acrediten como confiable, de modo que se encuentre libre de errores, defectos, omisiones y modificaciones no autorizadas, y sea emitida, de acuerdo con los fines institucionales".*
> *5.6.2"Las actividades de recopilar, procesar y generar información, debe realizarse y darse en tiempo a propósito y en el momento adecuado, de acuerdo con los fines institucionales".*
>
> *5.6.3 "La información debe poseer características que la hagan útil para los distintos usuarios, en términos de pertinencia, relevancia, suficiencia y presentación adecuada, de acuerdo con los fines institucionales".*

Como complemento a la normativa expuesta, el estándar de mejores prácticas Cobit, expresa en su apartado 6.2.3 "Tratamiento de la seguridad en acuerdos con terceros", lo siguiente:

> *"Los acuerdos o contratos con terceros que involucran el acceso, procesamiento, comunicación o manejo de la información o medios*

> *de procesamiento de información de la compañía, o agregan producto o servicios a los medios de procesamiento de información debieran abarcar todos los requerimientos de seguridad relevantes.*
>
> ***Lineamiento de implementación***
> *El acuerdo debiera asegurar que no existan malos entendidos entre la organización y la otra parte. Las organizaciones debieran estar satisfechas con relación a la indemnización de las otras partes".*

Igualmente el Estándar ISO/IEC 17799 indica en su ítem AI5.2 "Administración de Contratos con Proveedores" lo siguiente:

> *"Formular un procedimiento para establecer, modificar y concluir contratos para todos los proveedores. El procedimiento debe cubrir, como mínimo, responsabilidades y obligaciones legales, financieras, organizacionales, documentales, de desempeño, de seguridad, de propiedad intelectual y responsabilidades de conclusión, así como obligaciones (que incluyan cláusulas de penalización). Todos los contratos y las modificaciones a contratos las deben revisar asesores legales".*

La falta de implementación de la normativa vigente y la ausencia de controles en la actividad contratada a una persona externa (outsourcing) que presta servicios de mantenimiento o de otro tipo a las Bases de Datos de la UNED, podría favorecer la consumación de riesgos y exponer a la Institución a pérdidas no solo económicas y de información, sino de imagen. Igualmente se pueden generar modificaciones no autorizadas en la base de datos por parte de un tercero contratado, o utilizarse información sensible para su comercialización u otros fines no autorizados; además se expone la Institución a que información que guarde limitaciones de propiedad intelectual o atributos de confidencialidad, pudieran ser cedida a terceros en forma desautorizada, con resultados adversos para la UNED.

2.4 Sobre la existencia de un lugar alterno para respaldo y recuperación de las operaciones en la Institución.

La UNED carece de un sitio alterno y de planes de recuperación de la información, con el objetivo de garantizar la continuidad de las operaciones y procesos críticos, ante un eventual desastre, ya sea natural (terremoto, huracán etc.) o provocado por el hombre (Vandalismo).

Sobre este particular, ante consulta formulada al Director de la DTIC, indicó que: "Existe un lugar que es utilizado básicamente para guardar cintas de respaldo en el CU de Heredia, sin embargo este no cuenta con la seguridad requerida", respuesta a entrevista efectuada el 22 de noviembre de 2011.

Adicionalmente, se nos informó que: "se está trabajando en un proyecto para contar con los recursos necesarios para poder tener un lugar alterno en el CONARE para que en una eventualidad sea respaldo de la información de la UNED y así recuperar sus labores en el menor tiempo posible".

A mayor abundancia, no solo es necesario contar con un sitio alterno, deben formularse planes de respaldo y estrategias de recuperación, considerando requerimientos de resistencia, procesamiento alternativo, y capacidad de recuperación de todos los servicios críticos de TI.

Sobre este particular la norma 1.4.4 "Seguridad en las operaciones y comunicaciones" inciso b, y 1.4.7 "Continuidad de los servicios de TI" ambas del Manual de normas técnicas para la gestión y el control de las tecnologías de información de la CGR que indican:

> *1.4.4 "Seguridad en las operaciones y comunicaciones". La organización debe implementar las medidas de seguridad relacionadas con la operación de los recursos de TI y las comunicaciones, minimizar su riesgo de fallas y proteger la integridad del software y de la información. Para ello debe:*
> ***..."***
> *b. Establecer procedimientos para proteger la información almacenada en cualquier tipo de medio fijo o removible (papel, cintas, discos, otros medios), incluso los relativos al manejo y desecho de esos medios."*
>
> *1.4.7 "Continuidad de los servicios de TI". La organización debe mantener continuidad razonable de sus procesos y su interrupción no debe afectar significativamente a sus usuarios.*
>
> *Como parte de ese esfuerzo debe documentar y poner en práctica, en forma efectiva y oportuna, las acciones preventivas y correctivas necesarias con base en los planes de mediano y largo plazo de la organización, la evaluación e impacto de los riesgos y la clasificación de sus recursos de TI según su criticidad."*

En línea con lo anterior, el estándar internacional de mejores prácticas de control en tecnologías de información, denominado "COBIT", en su apartado DS4 "Garantizar la Continuidad del Servicio" indica:

> *DS4.1 "Marco de Trabajo de Continuidad de TI"*
> *"Desarrollar un marco de trabajo de continuidad de TI para soportar la continuidad del negocio con un proceso consistente a lo largo de toda la organización. El objetivo del marco de trabajo es ayudar en la determinación de la resistencia requerida de la infraestructura y de guiar el desarrollo de los planes de recuperación de desastres y de contingencias."*
>
> ….
>
> *DS4.8 "Recuperación y Reanudación de los Servicios de TI"*
> *"Planear las acciones a tomar durante el período en que TI está recuperando y reanudando los servicios. Esto puede representar la activación de sitios de respaldo, el inicio de procesamiento alternativo, la comunicación a clientes y a los interesados, realizar procedimientos de reanudación, etc. Asegurarse de que los responsables del negocio entienden los tiempos de recuperación de TI y las inversiones necesarias en tecnología para soportar las necesidades de recuperación y reanudación del negocio."*
>
> *DS4.9 "Almacenamiento de Respaldos Fuera de las Instalaciones"*
> *"Almacenar fuera de las instalaciones todos los medios de respaldo, documentación y otros recursos de TI críticos, necesarios para la recuperación de TI y para los planes de continuidad del negocio. "*

Ante un evento adverso de la naturaleza o provocado por el hombre, la falta de planeamiento y definición de acciones concretas para la creación y aplicación de estrategias de resguardo de la información, sumado a la inexistencia de planes de recuperación y de continuidad de las operaciones, podrían provocar interrupciones prolongadas en procesos críticos de la Universidad, con un impacto alto en actividades claves, afectando a sus diferentes usuarios, tanto internos como externos, pudiendo llegar a una negación de servicios; con el deterioro de imagen respectivo.

3. CONCLUSIONES

3.1 El área denominada "Granja de Servidores", ubicada en el Edificio B, 3er. Piso, dentro de la DTIC, es el principal centro de procesamiento de información de la UNED, y aloja más de 40 servidores y equipo diverso de comunicación tales como "switch", "firewalls", "routers" y una UPS de gran tamaño entre otros; sin estos sería imposible contar con los servicios web, de red institucional para acceso a los sistemas de información y correo

electrónico, para funcionarios como a estudiantes, en aras de cumplir con su labor sustantiva.

No obstante, se observó en el diseño e implementación de este "Data Center", la ausencia de aplicación de un modelo o guía de mejores prácticas para la construcción, diseño y distribución de Centros de Cómputo, aspecto que se refleja en la inadecuada planificación del espacio existente entre los "racks", instalación de equipos de aire acondicionado no diseñados para realizar una climatización controlada para este tipo de áreas, carencia de un piso elevado para mejorar la distribución del aire, distribución de pasillos que dificulta la escasa circulación del aire, construcción de paredes y cielorrasos no aislantes de calor y fuego, ni sellados para reducir la aparición de polvo y estática, equipo de detección de humo ausente de pruebas periódicas, ausencia de sistemas de ductos, puertas de acceso desprovistas de sistemas automatizado o biométrico, ausencia de salidas de emergencia, entre otras debilidades denotadas, y adicionalmente, se destaca a simple vista una excesiva cantidad de equipos que no solo provoca hacinamiento, sino que por su peso ha generado dudas a la misma Dirección de la DTIC, sobre la capacidad de resistencia de esta área ubicada en el tercer piso, para soportar el peso concentrado de los equipos instalados, aspecto que es conocido por el Consejo de Rectoría. (Resultado 2.1.1)

3.2 Para el control de acceso a la DTIC, se utiliza un libro de anotaciones o bitácora, no obstante se observó que los datos del visitante, en algunos casos, no son registrados en su totalidad y se comprobó la ausencia de asignación formal para fiscalizar este registro. (Resultado 2.1.2)

3.3 Los datos sobre el inventario de Servidores existentes en el "Data Center" proporcionados por la DTIC no concilian con los registros contables. Se detectaron errores contables de registro y clasificación, que impiden determinar certeramente la cantidad y el costo de los equipos asignados en la DTIC. (Resultado 2.1.3).

3.4 El registro de salida de activos utilizado en la DTIC, carece de la firma del funcionario que autoriza tal transacción, además esta función no está formalmente asignada, y cualquier funcionario de la DTIC puede hacer entrega de activos a funcionarios de la UNED o a personal externo de empresas outsourcing. (Resultado 2.1.4)

3.5 Mediante inventario realizado por la Auditoría Interna, se concluye que el listado de activos con que cuenta la DTIC está desactualizado, localizándose en esa Dirección, equipos que no coinciden con el número de placa y activos que todavía aparecen en lista, cuando algunos ya fueron dados de baja y otros ubicados en distintas dependencias de la UNED. (Resultado 2.1.5).

3.6 La UNED actualmente paga contratos de seguro por "¢548.664.844,00. Equipo Fijo Sabanilla y ¢5.647.289,00 en Discos Duros Sabanilla" entre otros; con el agravante que no se identifican por número de placa, serie y marca, los activos que están asegurados, condición que hace muy difícil hacer efectivo el resarcimiento económico a causa de un reclamo ante la entidad aseguradora. (Resultado 2.2).

3.7 La Institución carece de un procedimiento escrito, debidamente aprobado, actualizado y divulgado, para la creación e inhabilitación de usuarios a nivel de sistemas de información en la red de datos, que norme las actividades de control, mantenimiento, entrega, y reasignación de contraseñas, entre otras. (Resultado 2.3.1)

Adicionalmente se confirmó la existencia del documento denominado "*Uso de correo electrónico*", aprobado por el Consejo de Rectoría en Sesión N°1605, Artículo IV, inciso 2), celebrada el 26 de agosto del 2009, norma que regula únicamente la exclusión de cuentas de correo electrónico, dejando al descubierto la inhabilitación de accesos a la red de datos institucional, por cese de labores de funcionarios. No obstante, se determinó no solo el incumplimiento a esta norma al detectarse diecisiete casos de personas que continúan con el servicio de correo electrónico habilitado siendo ex funcionarios de la UNED, sino que además se encontraron dieciocho (18) casos de ex funcionarios que aún mantienen su acceso a la plataforma del AS/400. (Resultado 2.3.1).

3.8 La DTIC no cuenta con la información o un listado de los usuarios de la UNED que tienen acceso a cada uno de los Sistemas de Información en producción en el ambiente del AS/400, plataforma que reside a la mayoría de los sistemas sensibles de la UNED, tales como SAE, Financiero-Contable, Presupuesto, Planillas, entre otros, aspecto que representó una limitante en la aplicación de las pruebas que planeó realizar esta Unidad Fiscalizadora. (Resultado 2.3.2.).

3.9 La información aportada por el Director de la DTIC, contiene el detalle de los accesos concedidos a los funcionarios de la DTIC a los sistemas de información en producción y sus roles correspondientes, sin embargo, no concuerda con la misma información proporcionada por el señor Gonzalo Rodriguez Benavides, Administrador de Base de Datos (DBA) de la DTIC. (Resultado 2.3.2.).

3.10 La plataforma de IBM–AS/400, es la más antigua y en ella se concentra el 80% de los sistemas institucionales, pero no es administrada por el único Administrador de Bases de Datos de la UNED, incumpliéndose no solo con una función que establece el Manual Descriptivo de Puestos, que define esta tarea como típica del DBA, sino que provoca que los analistas de la DTIC sean quienes modifican a nivel de programación las bases de datos, función considerada como incompatible desde el punto de vista de control interno, a pesar de que se argumente una supervisión posterior ejercida por parte del líder de proyectos, a cualquier cambio que se realice en las bases de datos. (Resultado 2.3.2.).

3.11 Al evidenciarse la presencia de funciones incompatibles, se revisaron los controles de seguridad para el registro de transacciones, determinándose que las bitácoras no están activas para las cuatro plataformas de Bases de Datos que operan en la UNED. Únicamente se mantienen activas dos bitácoras para los ambientes SQL Server y ORACLE, no obstante, no son verificadas, debido a que tal función de control no ha sido asignada y hay carencia de procedimientos a seguir en caso de detectarse ingresos no autorizados a los sistemas u otras anomalías. (Resultado 2.3.2).

3.12 No se encontró evidencia de que en la UNED se establezcan “acuerdos o contratos de confidencialidad”, aplicables a personal externo de empresas privadas que realizan funciones de mantenimiento o de otra índole, en las bases de datos, vía outsourcing o tercerización. (Resultado 2.3.2).

3.13 La UNED carece de un sitio alterno adecuado y planes de recuperación para garantizar la continuidad de sus operaciones sustantivas y salvaguardar los procesos críticos, ante el acaecimiento de un desastre natural o vandalismo. (Resultado 2.4.).

4. RECOMENDACIONES

Al RECTOR

Girar instrucciones a las dependencias que corresponda para:

4.1 Fundamentar en criterios técnicos y en estándares internacionales de mejores prácticas, para el diseño e implementación de Centros de Cómputo, las mejoras a realizar en las instalaciones del "Data Center" actual, ya sea en materia de infraestructura, seguridad física y en protección contra factores ambientales. (Resultado 2.1.1).

4.2 Continuar con las acciones emprendidas por el Consejo de Rectoría, a fin de brindar una solución oportuna al Centro de Datos ("DATA CENTER") de la UNED, de conformidad con el informe "Análisis y Valoración de propuestas de soluciones para el centro de datos" presentado a ese Consejo por el Ing. Carlos Morgan Marín. (Resultado 2.1.1)

4.3 Definir una metodología de control de acceso físico basada en un análisis de riesgos, que no solo guarde el registro de la entrada y salida del personal a áreas criticas o sensibles de la DTIC, sino que considere un marco regulatorio y estudios de factibilidad que permitan dotar a esta Dirección de un sistema automatizado de control de acceso y monitoreo, se definan responsables de las actividades de supervisión sobre los controles instaurados, procedimientos, recursos presupuestarios, entre otros. (Resultado 2.1.2)

4.4 Fortalecer el control utilizado en la DTIC para la salida de activos, incluyendo como punto de control la firma del funcionario que autoriza esa transacción y el sello de la DTIC, u otros controles que la Administración considere convenientes para mitigar los riesgos asociados a esta debilidad. El Director debe asignar formalmente la función de entrega de activos y el procedimiento a seguir. (Resultado 2.1.4).

4.5 Realizar los ajustes contables correspondientes, a fin de reclasificar los servidores registrados actualmente como switch, con el propósito de reflejar

la exactitud en la información contable que sirve de base para la toma de inventarios físicos. (Resultados 2.1.3.)

4.6 Realizar un inventario de activos en el Data Center, y conciliar los datos con los registros contables. (Resultado 2.1.5).

4.7 Velar por que se incluyan los activos sensibles ubicados en el Data Center de la UNED (Servidores, enrutadores, "Firewall", "Switch" principal, entre otros.), dentro de la nueva póliza de seguros que la Institución está por suscribir con el INS, y verificar que tales activos sean registrados por placa de inventario, marca, número de serie y descripción. (Resultado 2.2).

4.8 Formular un procedimiento que regule las actividades de creación, mantenimiento e inhabilitación de usuarios a nivel de sistemas de información en la red de datos. Posteriormente, someterlo a la aprobación del Consejo de Rectoría, implementarlo y velar por su adecuada divulgación. (Resultado 2.3.1)

4.9 Hacer cumplir el documento denominado "Uso del Correo Electrónico", aprobado por el Consejo de Rectoría en Sesión No. 1605, Artículo IV, inciso 2), celebrada el 26 de agosto del 2009. (Resultado 2.3.1)

4.10 Requerir a la DTIC para que cuente con información, o un listado de todos los usuarios que tienen acceso a los sistemas institucionales en producción en el AS/400, roles y perfiles. (Resultado 2.3.2)

4.11 Conciliar la información en poder del director de la DTIC, sobre el acceso a los sistemas y roles de los funcionarios de esa dependencia, con la misma información que maneja el DBA. (Resultado 2.3.2).

4.12 Realizar los estudios que correspondan a fin de determinar la factibilidad de dotar con más recursos humanos y tecnológicos a las áreas funcionales de Seguridad lógica y Administración de Bases de Datos de la Institución, de acuerdo con los requerimientos de recursos que demanden las gestiones respectivas para su buen funcionamiento. Asimismo asignar al DBA de la UNED, la tarea de administrar todas las bases de datos institucionales; en caso de ser necesario, deberá valorar la contratación de un DBA adicional, con el fin de evitar incompatibilidad de funciones con los analistas que efectúan modificaciones a nivel de programación en las mismas bases de datos. (Resultado 2.3.2).

4.13 Ordenar la activación de las bitácoras en las Bases de Datos Institucionales, previa determinación de la sensibilidad y criticidad de la información, y priorizando de acuerdo al nivel de riesgos asociados a la información almacenada en estas. Asignar la función de monitoreo en un funcionario o área competente de la DTIC, con conocimientos de seguridad digital. Asimismo, definir el procedimiento y acciones a seguir en caso de detectarse anomalías. (Resultado 2.3.2).

4.14 Solicitar la asesoría de la Oficina Jurídica de la UNED, con la finalidad de incluir cláusulas de confidencialidad, propiedad de la información y cláusulas de indemnización en los contratos de mantenimiento suscritos con empresas externas, cuyo personal tiene acceso a las bases de datos, equipos e información sensible de la institución. (Resultado 2.3.2).

4.15. Determinar los recursos de capacitación en materia de seguridad física y lógica, que requiere el personal con responsabilidades en esta materia en la DTIC, y asignar recursos en el presupuesto institucional, que permitan contar con una formación especializada y apoyen la gestión de seguridad a desarrollar. (Resultado 2.3.2)

4.16 Realizar los estudios técnicos y financieros, y de valoración de riesgos, que conduzcan a establecer un sitio de procesamiento alterno, con el propósito de afrontar contingencias, y elaborar estrategias de respaldo y recuperación de la información, para garantizar la continuidad de las operaciones y los procesos críticos institucionales, ante un eventual desastre natural o provocado por el hombre. Considerar entre las acciones a realizar la coordinación de áreas competentes en la materia como son Cuerpo de Bomberos, Comisión Nacional de Emergencias, suplidores de servicios (energía eléctrica, comunicaciones) Cruz Roja, entre otros (Resultado 2.4.).

ANEXOS

Anexo 1

Foto1: Aire acondicionado de confort en el techo del “DATA CENTER”. 8/3/2011

Foto2: Entrada principal al “DATA CENTER” sin seguridad 8/3/2011

Foto3: Extintores ubicados en mal lugar dentro del “DATA CENTER”.

Foto4: Cintas de respaldos en el “DATA CENTER”, sin resguardo.

Tel: 2527 2276
Telefax: 2224 9684
Apdo. 474-2050
San Pedro de Montes de Oca

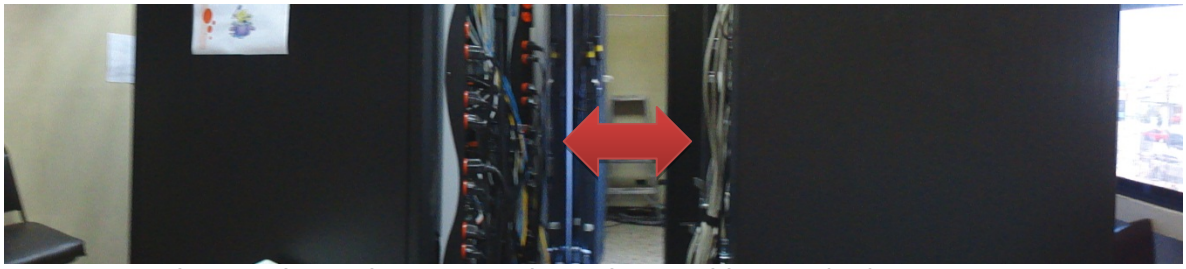

Foto5: Espacio entre los racks que mantienen los servidores. 8/03/2011

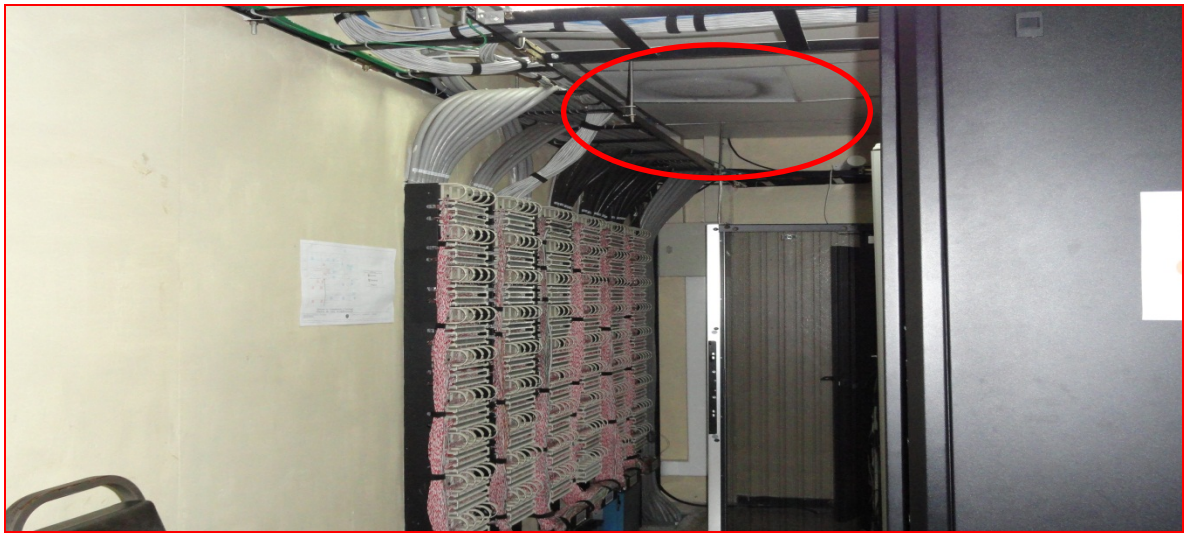

Foto6: Rastros de alguna humedad en el cielorraso sobre cableado “DATA CENTER”. 8/03/2011

Tel: 2527 2276
Telefax: 2224 9684
Apdo. 474-2050
San Pedro de Montes de Oca

Foto7: Rastros de humedad en el cielorraso sobre servidores “DATA CENTER”. 8/03/2011

AUDITORIA INTERNA

Tel: 2527 2276

Telefax: 2224 9684

Apdo. 474-2050

San Pedro de Montes de Oca

Anexo 2

DIRECCIÓN DE TECNOLOGÍA, INFORMACIÓN

Y COMUNICACIONES

ENTRADA O SALIDA
DE ACTIVOS

Entrada: _____ **Salida:** __x___

Nombre de la persona que despacha: Francisco Durán Montoya

Tipo de material o mercadería: **PANDA Gate Defender Performa 9500**

Número de serie: **IOSN-0924QB DOBE5**

Persona que recibe:

Nombre Hansel Granados B **Firma** _____ **Céd.** 1-973-614

Fecha de recibido: 16/04/10

Se entrega equipo en calidad de préstamo al personal de PANDA para realización de pruebas.

- FALTA FIRMA Y SELLO DTIC.
- INDICAR CARGO DE QUIEN DESPACHA EL ACTIVO.

C: (1)
Interesado

AUDITORIA INTERNA

Tel: 2527 2276

Telefax: 2224 9684

Apdo. 474-2050

San Pedro de Montes de Oca

DIRECCIÓN DE TECNOLOGÍA, INFORMACIÓN Y COMUNICACIONES

ENTRADA O SALIDA DE ACTIVOS

Entrada: _____ **Salida:** __x__

Nombre de la persona que despacha: Andrea Zamora ✓ FALTA FIRMA CARGO Sello.

Tipo de material o mercadería: **Portátil Mini HP**

Número de serie: **Activo No 24269M**

Persona que recibe:

Nombre Oscar Alvarado **Firma** _____ **Céd.** 1-1035-459

Fecha de recibido**: 03/12/10**

Se entrega equipo a la Unidad de Almacén General para su revisión y reparación.

C: (1)
Interesado

AUDITORIA INTERNA

Tel: 2527 2276

Telefax: 2224 9684

Apdo. 474-2050

San Pedro de Montes de Oca

DIRECCIÓN DE TECNOLOGÍA, INFORMACIÓN

Y COMUNICACIONES

ENTRADA O SALIDA
DE ACTIVOS

Entrada: _____ **Salida: __x___**

Nombre de la persona que despacha: Vigny Alvarado Castillo ✓ FIRMA

Tipo de material o mercadería: **Computadora Portátil Dell**

Número de activo: **25287**

Persona que recibe:

Nombre William Morales **Firma** _____ **Céd.** 1-767-476

Fecha de recibido:

Se entrega Computadora Portátil y cargador a la Unidad de Mantenimiento para su revisión y reparación, dado que presenta problemas con la memoria y se encuentra en garantía. Según solicitud de trabajo enviada el 30/05/2011

NOTA: FALTA FIRMA DE QUIEN DESPACHA EL ACTIVO Y SELLO DE LA DTIC.//

C: (1)
Interesado