

***UNIVERSIDAD NACIONAL (UNA)***

---

+ *Carta de Gerencia CG 1-2015*

+ *Informe final*

Heredia, 16 de setiembre del 2016.

Señores  
Universidad Nacional (UNA)

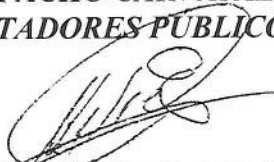
Estimados señores:

Según nuestro contrato de servicios, efectuamos la auditoría externa correspondiente al período 2015, a la Universidad Nacional (UNA) y con base en el examen efectuado notamos ciertos aspectos referentes al sistema de control interno y procedimientos de contabilidad, los cuales sometemos a consideración de ustedes en esta carta de gerencia CG1-2015.

Considerando el carácter de pruebas selectivas en que se basa nuestro examen, ustedes pueden apreciar que se debe confiar en métodos adecuados de comprobación y de control interno, como principal protección contra posibles irregularidades que un examen basado en pruebas selectivas puede no revelar, si es que existiesen. Las observaciones no van dirigidas a funcionarios o colaboradores en particular, sino únicamente tienden a fortalecer el sistema de control interno y los procedimientos de contabilidad.

Agradecemos una vez más la colaboración recibida de los funcionarios y empleados de la Universidad Nacional (UNA) y estamos en la mejor disposición de ampliar y/o aclarar el informe que se adjunta en una sesión conjunta de trabajo cuando nos convoquen.

***DESPACHO CARVAJAL & COLEGIADOS  
CONTADORES PÚBLICOS AUTORIZADOS***



Lic. Ricardo Montenegro Guillén  
Contador Público Autorizado número 5607  
Póliza de Fidelidad número 0116 FIG 7  
Vence el 30 de setiembre del 2016

“Exento de timbre de Ley número 6663 del Colegio de Contadores Públicos de Costa Rica, por disposición de su artículo número 8”.

### **TRABAJO REALIZADO**

A continuación presentamos los procedimientos de evaluación de control interno y pruebas sustantivas de auditoría, aplicados durante nuestra visita a la Universidad Nacional (UNA), así como los resultados obtenidos:

#### ***a) Procedimientos generales***

- Dimos lectura a las actas del Consejo Universitario del período 2015.
- Solicitamos los informes de auditoría interna con fecha de corte al 31 de diciembre del 2015.
- Estudiamos, revisamos y evaluamos los procedimientos de control interno, contables, administrativos e informáticos, existentes.
- Evaluamos el sistema de control interno de acuerdo con el “Manual sobre Normas y Técnicas y Control Interno para la Contraloría General de la República”, así como de acuerdo a las normas y procedimientos de auditoría aplicables, de acuerdo con lo establecido por el Colegio de Contadores Públicos de Costa Rica.
- Durante la revisión de los riesgos de auditoría en las cuentas que se detallan más adelante, donde evaluamos la posibilidad de que los procedimientos de control interno contable y administrativo existentes en cada área fuesen adecuados para evitar o detectar irregularidades.
- Dimos seguimiento a los hallazgos de las cartas de gerencia de periodos anteriores

#### ***Resultado de la revisión:***

Como resultado de la evaluación del control interno de la Universidad Nacional (UNA), se determina que existe una serie de situaciones que afectan el control interno y que presentan un nivel de riesgo medio, las mismas se detallan a continuación:

## **HALLAZGO 1: NO SE GUARDAN REPORTES FÍSICOS Y ELECTRÓNICOS HISTÓRICOS.**

### **CONDICIÓN:**

Al realizar la auditoría de los estados financieros de la Universidad Nacional al 31 de diciembre del 2015, determinamos que no se guardan reportes físicos históricos de los saldos como por ejemplo:

- Reportes o conciliaciones de las cuentas por cobrar matrícula.
- Reportes o conciliaciones físicas de la cuenta propiedad, planta y equipo
- Reportes físicos de la cuenta de inventarios.

Lo anterior puede conllevar a que no se tenga la certeza de los saldos a una fecha en específica, ya que no se cuenta con el respaldo suficiente sobre dichas cuentas.

### **CRITERIO:**

Según las Normas de Control Interno aplicables para el Sector Público la administración, según sus competencias, debe 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.

### **RECOMENDACIÓN:**

La administración debe girar las instrucciones necesarias para que a la fecha de corte de los estados financieros de la Universidad se deje evidencia física y/o electrónica de los saldos que respaldan las partidas de los estados financieros, de manera que se detalle la fuente que da origen a los datos contenidos.

## **HALLAZGO 2: CARENCIA DE POLÍTICAS Y PROCEDIMIENTOS FORMALMENTE APROBADAS PARA LA ADMINISTRACIÓN DE CUENTAS POR COBRAR E INVERSIONES.**

### **CONDICIÓN:**

Al realizar la revisión de las políticas, manuales y procedimientos de la Universidad Nacional al 31 de diciembre del 2015, determinamos que para las cuentas de inversiones y cuentas por cobrar se carecen de los mismos documentos, ya que están en una etapa de aprobación final por parte de la administración, lo cual afecta en la revisión de dichas cuentas, ya que no se tiene un parámetro de medición y tratamiento contable definido.

**CRITERIO:**

Las Normas de Control Interno establecen la importancia de documentar todas las regulaciones en manuales de procedimientos, además determinan que esta documentación debe estar disponible, en forma ordenada conforme a criterios previamente establecidos, para su uso, consulta y evaluación.

**RECOMENDACIÓN:**

La Universidad como parte de la realización y actualización de las políticas y procedimientos internos que realiza de forma anual debe tomar en cuenta la implementación de las mismas para **la administración de las cuentas por cobrar e inversiones.**

**b) Caja y bancos**

- Realizamos cédulas sumarias comparativas y revisamos los movimientos relevantes de la cuenta.
- Revisamos las conciliaciones bancarias de las diferentes cuentas corrientes que posee la Universidad, al 31 de diciembre del 2015.
- Solicitamos a la Administración de la UNA los estados de cuenta bancarios posteriores a la fecha del balance general, con el propósito de verificar que los cheques han sido cancelados.
- Solicitamos los resultados de los últimos arqueos de fondos de trabajo efectuados por el Departamento de Tesorería de la Universidad.
- Seleccionamos una muestra de los desembolsos de efectivo para el periodo que es objeto la auditoría, revisamos la documentación respaldo de las mismas al cierre del periodo de la auditoría
- Seleccionamos una muestra de depósitos de efectivo para el periodo que es objeto la auditoría y obtuvimos los comprobantes relacionados y documentación de respaldo.
- Solicitamos confirmaciones a los bancos para comprobar los saldos, la existencia y propiedad de las cuentas, las personas autorizadas y cualquier otra relación con las entidades bancarias.

***Resultado de la revisión:***

Con base en las pruebas de auditoría realizadas se determina que no existen situaciones de control interno, que deban informarse en esta carta de gerencia.

***c) Inversiones***

- Realizamos cédulas sumarias comparativas al 31 de diciembre del 2015, y revisamos variaciones importantes de la cuentas.
- Cotejamos el registro auxiliar con el mayor general, al 31 de diciembre del 2015.
- Realizamos el recálculo de los intereses por cobrar de los títulos al 31 de diciembre del 2015.
- Solicitamos los estados de cuenta de las inversiones al 31 de diciembre del 2015.
- Solicitamos confirmaciones de saldos a los diferentes entes bancarios con los que la Universidad mantiene inversiones.

***Resultado de la revisión:***

El sistema de control interno aplicado a las partidas de inversiones presenta un riesgo bajo, sin embargo se detectaron debilidades de control que se muestran en el hallazgo 2.

***d) Cuentas por cobrar***

- Realizamos cédulas sumarias comparativas al 31 de diciembre del 2015, y revisamos variaciones importantes de la cuentas.
- Cotejamos lo registros auxiliares de las cuentas por cobrar contra el mayor contable al 31 de diciembre del 2015.

***Resultado de la revisión:***

Mediante lo resultados de las pruebas realizadas a la UNA, se determina una diferencia entre el registro auxiliar y la cuenta mayor de ¢1.867.534,09. Es importante mencionar que esta es la misma diferencia que se obtuvo hace varios años en una de las primeras conciliaciones efectuadas y es igual a diferencia determinada en la última conciliación realizada el pasado 08 de agosto del 2016.

Se determina la existencia de una serie de situaciones que representan un nivel de riesgo medio, las cuales se mencionan a continuación:

### HALLAZGO 3: POLÍTICA DE INCOBRABLES PENDIENTE DE APROBACIÓN.

#### CONDICIÓN:

Efectuamos la revisión de las cuentas por cobrar al 31 de diciembre del 2015 y determinamos que la Universidad no efectúa una estimación para incobrables. Las cuentas por cobrar, principalmente las matrículas presentan una antigüedad superior a los 180 días. A la fecha de este informe la política de estimación para incobrables se encuentra pendiente de aprobación por parte de la administración.

#### CRITERIO:

Las instituciones del sector público deben incluir en su catálogo de cuentas la estimación por incobrables, la cual tiene como objetivo registrar los movimientos de las estimaciones por posibles contingencias a causa de la incobrabilidad de las cuentas por cobrar (Directriz de la Contabilidad Nacional CN-01-2007, art No.02). Se pueden usar tres métodos % ventas a crédito, análisis de cuentas por cobrar con base en la antigüedad de saldos y % sobre el saldo de cuentas por cobrar.

#### RECOMENDACIÓN:

Confeccionar la normativa y procedimiento para implementar una adecuada estimación para incobrables que permita una mejor razonabilidad de los saldos pendientes de cobro de la universidad.

### HALLAZGO 4: LAS CUENTAS POR COBRAR POR MATRÍCULA PRESENTAN UNA ANTIGÜEDAD SUPERIOR A LOS 180 DÍAS.

#### CONDICIÓN:

Efectuamos el análisis de antigüedad de las cuentas por cobrar cuya naturaleza son las matrículas con el detalle suministrado al 31 de diciembre 2015 y se cotejó con el saldo anterior a mayo 2015, el detalle se presenta a continuación:

Antigüedad en días	Saldo a mayo 2015	Porcentaje	Saldo a diciembre 2015	Porcentaje
De 0 a 180	¢24.572.264	4%	¢24.712.220	3%
De 180 a 360	45.031.664	7%	43.974.112	6%
Más de 360	533.493.356	80%	554.399.597	78%
Créditos 2015	61.261.484	9%	91.129.334	13%
<b>Total</b>	<b>¢639.786.504</b>	<b>100%</b>	<b>¢714.215.263</b>	<b>100%</b>

## **CRITERIO:**

Un adecuado control interno establece lo siguiente: se analizarán los valores a cobrar efectuado por un empleado que no tenga acceso al manejo del efectivo, ni participación en la aprobación de créditos, o en la determinación de los ingresos tributarios. El análisis y evaluación de los valores a cobrar se efectuará periódicamente, de preferencia en forma mensual, para comprobar la eficiencia de las recaudaciones y la cobranza de las cuentas vencidas, indicando su antigüedad.

## **RECOMENDACIÓN:**

Establecer normas y procedimientos para el control u administración de las cuentas por cobrar vencidas y antiguas.

### ***e) Inventario***

- Realizamos cédulas sumarias comparativas al 31 de diciembre del 2015.
- Cotejamos los registros auxiliares del inventario y de la mercadería en tránsito con los saldos contables al 31 de diciembre del 2015.
- Participamos en la toma física que realiza proveeduría y contabilidad en las bodegas de la UNA.

### ***Resultado de la revisión:***

De acuerdo con la revisión efectuada, concluimos que la cuenta de inventario presenta un nivel de riesgo bajo y no se presentan situaciones que deban informarse a la administración.

### ***f) Gastos pagados por anticipado***

- Realizamos cédulas sumarias comparativas al 31 de diciembre del 2015.
- Realizamos un recálculo de las primas y los descuentos producto de las inversiones al 31 de diciembre del 2015.

### ***Resultado de la revisión:***

De acuerdo con la revisión efectuada, concluimos que la cuenta de gastos pagados por anticipado presenta un nivel de riesgo bajo y no se presentan situaciones que deban informarse a la administración.



**g) Activo propiedad, mobiliario y equipo**

- Realizamos cédulas sumarias comparativas al 31 de diciembre del 2015 y revisamos variaciones importantes de las cuentas.
- Cotejamos el registro auxiliar con el mayor general al 31 de diciembre del 2015.
- Realizamos una prueba global de la depreciación acumulada y el gasto por depreciación al 31 de diciembre del 2015.
- Seleccionamos una muestra de las adiciones y retiros efectuada durante el periodo y revisamos con la documentación soporte.

**Resultado de la revisión:**

Los resultados de las pruebas realizadas indican que la cuenta de activo fijo de la UNA, presenta debilidades de control interno y que **muestran un nivel de riesgo alto, las cuales se detallan de la siguiente manera:**

**HALLAZGO 5: DEBILIDADES DE CONTROL INTERNO EN LA CUENTA DE INMUEBLE, MAQUINARIA Y EQUIPO.**

Efectuamos nuestras pruebas de auditoría a las partidas de inmueble, maquinaria y equipo al 31 de diciembre del 2015 y determinamos las siguientes debilidades de control:

- a) Procedimos a cotejar el saldo del reporte generado por el departamento de contabilidad con el saldo registrado contablemente, con lo cual determinamos una diferencia que asciende a la suma de ¢61.260 (en miles) la cual se origina debido a:
- Registros de diferenciales cambiarios por parte de la Proveduría, que generaron un registro a la cuenta de mayor pero no al auxiliar, no obstante, al remitir la Proveduría la documentación para aumentar el valor del activo y al ingresar a la forma de ajuste en el auxiliar, se aumentaba el valor al activo, que también generaba un aumento en la cuenta de mayor; significando esto un doble registro en la cuenta de mayor.
  - Casos en los que la Proveduría anuló placas de activos que ya se habían registrado en el auxiliar, y estos nunca generaron un registro desde esa instancia a la cuenta de mayor, sin embargo, al remitir la documentación a esta oficina para la anulación y generar el documento "m" de eliminación, genero un registro en el mayor por esa eliminación.
  - Registros desde la Proveduría que generaron cargos en cuentas de mayor, es decir cuentas de activos, cuyos bienes no correspondían al tipo de activo registrado en el auxiliar, es decir, cargos a cuenta de activos cuya orden compra indicaba varios tipos de activos, sin embargo, el sistema lo cargaba a un solo tipo de activo.

- Registros manuales en el mayor de activos fijos, por sumas que no correspondían a activos fijos, es decir se cargo a las cuentas de activos (mayor) montos de bienes de consumo, los cuales se aumentaron por el monto correcto en el auxiliar. Se generó un cargo superior en la cuentas de mayor y en el auxiliar un aumento menor (el correcto).

- Registros duplicados por remisión doble de documentación en dos vías.
- Activos donados no registrados en la cuenta mayor.
- Activos cuyos procesos de capitalización quedaron inconclusos.

El detalle se muestra a continuación:

Tipo	Cuenta Contable	Detalle	Saldo en Libros ajustado	Saldo Auxiliar ajustado	Diferencia Miles
TIPO 01	AO01	Maquinaria y equipo de producción	676.386	676.028	357
TIPO 02	AO02	Equipo de Transporte	3.725.485	3.725.483	2
TIPO 03	AO03	Equipo de comunicación	3.389.407	3.391.899	(2.492)
TIPO 04	AO04	Equipo y mobiliario de oficina	3.361.953	3.346.415	15.538
TIPO 05	AO05	Equipo y programa de computo	7.123.227	7.130.011	(6.783)
TIPO 06	AO06	Equipo sanit, laborat e investig	7.814.612	7.913.496	(98.884)
TIPO 07	AO07	Eq y mob educ, depo, y recreat	289.148	361.105	(71.957)
TIPO 08	AO08	Maquinaria y equipo diverso	2.147.205	2.103.298	43.907
TIPO 09	AO11	Terrenos	3.194.659	3.194.548	111
TIPO 10	AO10	Edificios	25.230.063	25.048.602	181.461
<b>Total</b>			<b>56.952.145</b>	<b>56.890.885</b>	<b>61.260</b>

El sistema de información financiera no guarda históricos por lo que se nos comenta que la conciliación siempre va a presentar diferencias, lo que de igual manera representa una debilidad de control interno.

- b) Realizamos el re-cálculo de la depreciación acumulada al 31 de diciembre del 2015 y se presenta una diferencia material por un monto de ¢863.829( en miles) con respecto al saldo auxiliar.

El encargado de activos nos comenta que esta diferencia se genera debido a que el proceso interno para la entrada de los activos no se completa en el sistema por lo que existen activos que no se están depreciando o el cálculo se realiza con parámetros errados.

- c) No se efectúan revaluaciones de inmueble, maquinaria y equipo.

## **CRITERIO:**

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.

Además el jerarca y los titulares subordinados, según sus competencias, deben establecer actividades de control que orienten la ejecución eficiente y eficaz de la gestión institucional. Lo anterior, tomando en cuenta, fundamentalmente, el bloque de legalidad, la naturaleza de sus operaciones y los riesgos relevantes a los cuales puedan verse expuestas.

Con posterioridad a su reconocimiento inicial como activo, todos los elementos de la Propiedad, planta y equipo, deben ser contabilizados a su costo de adquisición menos la depreciación acumulada practicada y el importe acumulado de cualesquiera pérdidas por deterioro del valor que hayan sufrido a lo largo de su vida útil. Con posterioridad al reconocimiento inicial como activo, todo elemento de a Propiedad, planta y equipo, debe ser contabilizado a su valor revaluado, que viene dado por su valor razonable, en el momento de la revaluación, menos la depreciación acumulada practicada posteriormente y el importe acumulado de las pérdidas por deterioro de valor que haya sufrido el elemento. Las revaluaciones deben ser hechas con suficiente regularidad, de manera que el importe en libros, en todo momento, no difiera significativamente del que podrá determinarse utilizando el valor razonable en la fecha de los estados financieros.

## **RECOMENDACIÓN:**

Es importante que el departamento de proveeduría en conjunto con el departamento de contabilidad concrete un procedimiento de conciliación, de manera que se determinen oportunamente las diferencias que se puedan presentar, así como tener las debidas justificaciones sobre el origen de las mismas.

La administración debe realizar las gestiones necesarias para cada uno de los activos incluidos en el registro auxiliar contable, con el fin de determinar el valor de la depreciación acumulada y el valor en libros actual, así como efectuar la ajustes considerados pertinente para mostrar un valor actual de la propiedad, planta y equipo.

La administración también debe realizar revaluaciones periódicas para que de este modo revelar un saldo contable a valor razonable en la fecha de estados financieros.

***h) Documentos por pagar***

- Realizamos cédulas sumarias comparativas al 31 de diciembre del 2015.
- Realizamos una conciliación de saldos al 31 de diciembre del 2015.
- Solicitamos las tablas de pago de la deuda al 31 de diciembre del 2015.
- Revisamos el gasto por intereses de la cuenta al 31 de diciembre del 2015.
- Solicitamos confirmaciones de saldos a los diferentes entes bancarios al 31 de diciembre del 2015.

***Resultado de la revisión:***

De acuerdo con la revisión efectuada, concluimos que la cuenta de documentos por pagar presenta un nivel de riesgo bajo y no se presentan situaciones que deban informarse a la administración.

***i) Cuentas por pagar***

- Realizamos cédulas sumarias comparativas al 31 de diciembre del 2015 y revisamos variaciones importantes de la cuenta.
- Cotejamos el saldo de los registros auxiliares contra los saldos de la contabilidad al 31 de diciembre del 2015.
- Realizamos un memorándum explicativo de la cuenta.

***Resultado de la revisión:***

Los resultados de las pruebas realizadas indican que las cuentas por pagar de la Universidad se presentan en con un nivel de riesgo bajo, sin embargo se presentas debilidades de control que se detallan a continuación:

## **HALLAZGO 6: DEFICIENCIAS DE CONTROL EN EL REGISTRO AUXILIAR DE LAS CUENTAS POR PAGAR.**

### **CONDICIÓN:**

Al realizar la revisión de las cuentas por pagar al 31 de diciembre del 2015, se determinaron una serie de deficiencias de control referentes al registro auxiliar de las cuentas por pagar, dichas deficiencias se detallan a continuación:

- No se observa el detalle de las facturas pendientes de pago por parte de la UNA.
- No se identifica la antigüedad de las cuentas por pagar.

### **CRITERIO**

De acuerdo con las Normas de Control Interno para el Sector Público, referentes a la exigencia de confiabilidad y oportunidad de la información, la Administración debe diseñar, adoptar, evaluar y perfeccionar las actividades de control pertinentes a fin de asegurar razonablemente que se recopile, procese, mantenga y custodie información de calidad sobre el funcionamiento de un Sistema de Control Interno y sobre el desempeño institucional. Lo anterior incluye la constitución de registros auxiliares que permitan la conciliación de los registros contables así como su constante actualización.

### **RECOMENDACIÓN**

Constituir un registro auxiliar para las cuentas por pagar, que muestre apropiadamente las características de cada uno de los documentos sujetos de pago, con suficiente detalle para realizar los análisis que se requieran.

#### ***j) Patrimonio***

- Realizamos cédulas sumarias comparativas al 31 de diciembre del 2015 revisamos variaciones importantes de la cuenta.
- Revisamos el estado de cambios en el patrimonio con el fin de revisar los movimientos importantes de la cuenta.

#### ***Resultado de la revisión:***

De acuerdo con la revisión efectuada, concluimos que la cuenta de patrimonio un nivel de riesgo bajo y no se presentan situaciones que deban informarse a la administración.

***k) Ingresos y Gastos***

- Realizamos cédulas sumarias comparativas al 31 de diciembre del 2015 revisamos variaciones importantes de la cuenta.
- Solicitamos el movimiento de las principales cuentas de ingresos y gastos al 31 de diciembre del 2015.
- Verificamos una muestra de movimientos relevantes de ingresos y gastos del periodo 2015.
- Realizamos una prueba de planillas, que consiste en la comparación de la información contable relativa a los sueldos y salarios, el reporte de la planilla de la CCSS y el reporte del INS. Adicionalmente, se verificó mediante el recálculo de dichas cifras, aquellos saldos de pasivo o gasto relacionados con la planilla de la Universidad.

***Resultado de la revisión:***

Como resultado de nuestra revisión de los documentos antes descritos, determinamos que la cuenta posee un nivel de riesgo bajo, ya que no detectamos situaciones que afectan el control interno.

**TRABAJO REALIZADO EN LAS GIRAS A LAS DIRECCIONES REGIONALES**

Como parte de nuestros procedimientos de auditoría realizamos una visita a las siguientes Sedes Regionales:

**Sede Regional Chorotega (Nicoya)**

- Realizamos un memorándum de conocimiento del funcionamiento de la Sede, además de los procesos realizados.
- Solicitamos y revisamos los últimos arqueos de caja chica, realizados a la Sede.
- Verificamos el control interno de la cuenta de propiedad, planta y equipo.
- Solicitamos el registro auxiliar de activos y realizamos la toma física de una muestra de los mismos.

**Sede Regional Sarapiquí**

- Realizamos un memorándum de conocimiento del funcionamiento de la Sede, además de los procesos realizados.

- Solicitamos y revisamos los últimos arqueos de caja chica, realizados a la Sede.
- Verificamos el control interno de la cuenta de propiedad, planta y equipo.
- Solicitamos el registro auxiliar de activo fijo y realizamos la toma física de una muestra de los mismos.

**Resultado de la revisión:**

De acuerdo a las pruebas de auditoría realizadas a las Sedes se identificaron deficiencias de control en el manejo de activos de la Sede de Sarapiquí, aparte de esto no se presentan otras situaciones que deban ser informadas a la administración.

**HALLAZGO 7: DEBILIDADES DE CONTROL INTERNO EN LAS PARTIDAS DE INMUEBLE, MAQUINARIA Y EQUIPO EN LA SEDE DE SARAPIQUÍ.**

**CONDICIÓN:**

Efectuamos la revisión de los activos fijos de la Campus de Sarapiquí y determinamos las siguientes debilidades de control interno:

- Determinamos que los custodios desconocen los activos que tiene bajo su responsabilidad.
- Se logran identificar activos que no cuentan con su placa respectiva, algunos ejemplos se detallan a continuación:

Etiqueta permanente	Descripción	Valor en libros
N00132296	Tractor	¢ 4.308.351
N00131230	Sistema De Alarma	2.457.667
N00135018	Tuba	1.305.000
N00134934	Hidrante	1.062.547
N00132580	Pizarra Interactiva	861.535
N00124598	Embarcación	780.000
N00135854	Maniquí	777.523
N00135855	Maniquí	777.523
N00135856	Maniquí	777.523

- Activos dañados y fuera de uso, pendientes de traslado o destrucción, algunos ejemplos se detallan a continuación:

<b>Etiqueta permanente</b>	<b>Descripción</b>	<b>Valor en libros</b>
N00121861	Invernadero desmontable	¢3.070.205
N00134932	Bomba contra incendios	1.930.266
N00121863	Equipo de riego	861.025

### **CRITERIO:**

Según las Normas Generales para la Administración y Control de los bienes de la Institución en el inciso III que establece que los Directores o Jefes, al tomar posición de sus cargos, exigirán a sus antecesores y a falta de estos, al superior inmediato, el inventario y entrega de los bienes que queden a su cargo. Si el inventario y la entrega fuesen correctos, se hará constar así, de lo contrario el funcionario entrante hará las observaciones que sean del caso en cuanto a funciones o sea trasladado a otro puesto o sitio de trabajo, tiene la obligación de faltantes o estado de los bienes, y en ambos casos firmará conjuntamente con la devolución por inventario todos los bienes que tenía a su cargo persona que le hace entrega.

Los funcionarios que bajo inventario se hagan cargo de bienes, serán responsables administrativa y fiscalmente, ya sea directa o indirectamente, de la pérdida, daño o depreciación de los mismos, salvo que provengan del deterioro natural por razón del uso legítimo o de otra causa justificada.

Ningún funcionario está obligado a firmar un inventario de bienes, si estos no están bajo su inmediato control o responsabilidad, es decir los que tengan a su cargo para uso, custodia, administración o para el desempeño de sus funciones.

Cuando al elaborar los inventarios se descubran faltantes, daños o deterioros de bienes, que no se deban a dolo o culpa de la persona que los tiene a su cargo, ésta podrá firmar los inventarios, dejando de ello constancia expresa en el mismo documento, y al mismo tiempo debe realizar las gestiones conducentes para que se le exima de toda responsabilidad.

Cuando por olvido u omisión del Director o Jefe de alguna dependencia, entre en funciones o se retire un funcionario, sin firmar el recibo o efectuar la devolución de los bienes a su cargo, o si cualquiera de estos funcionarios no firmen los inventarios correspondientes, los faltantes o daños que se encuentren posteriormente quedarán bajo la responsabilidad del Director o Jefe respectivo.

Además según las Normas Generales para la Administración y Control de los bienes de la Institución contabilidad tiene la responsabilidad de elaborar listas de los bienes registrados contablemente con el fin de enviarlos al Centro de Cómputo para su procesamiento. Estas listas deben contener la información necesaria que permita identificar la localización y descripción de todos y cada uno de los bienes.

Un adecuado control interno establece las siguientes regulaciones en la administración de



activo fijo:

- El registro y custodia de la documentación asociada a la adquisición, la inscripción, el uso, el control y el mantenimiento de los activos.
- El control de los activos asignados a dependencias desconcentradas o descentralizadas.
- El cumplimiento de requerimientos legales asociados a determinados activos, tales como inscripción, placas y distintivos.

**RECOMENDACIÓN:**

Efectuar una actualización de los custodios de los activos fijos mantenidos en el campus de Sarapiquí, efectuar la revisión de activos no plaqueados e identificarlos.

**Asientos de reclasificación aplicados por la auditoría externa (expresado en miles de colones):**

Ref. PT	N°	Cuenta Contable y Descripción	Balance de Situación		Explicación de Ajuste
			Débito	(Crédito)	
B/N	1	Sobre giro bancario -BCR Cta 2923-8 Sobre giro bancario -BNCR Cta 65373-3 Cuentas por pagar (Sobre giro bancario) ----- // -----	578.456 41.970 <b>620.426</b>	620.426 <b>620.426</b>	Ajuste por sobregiro bancario de dos de las cuentas corrientes de la UNA
E/N	2	Cuenta por cobrar -adelanto de salario Cuenta por cobrar-visa tarjetas Cuentas por pagar ----- // -----	571 1.668 <b>2.239</b>	2.239 <b>2.239</b>	Se reclasifica la cuenta de adelanto de salario y visa tarjetas, ya que no corresponde a su naturaleza contable
N/E	3	Otras cuentas por cobrar Cuentas por pagar sumas comprometidas Planilla por pagar Cuenta por pagar-Intercta estudiantil acreedora ----- // -----	48.914	283 2.906 45.725 <b>48.914</b>	Reclasificar cuentas por pagar con saldo deudor

Ref. PT	N°	Cuenta Contable y Descripción	Balance de Situación		Explicación de Ajuste
			Débito	(Crédito)	
AO-01		Maquinaria y equipo producc	3.500	8.496	Corresponde a la revisión realizada de la cuenta AO-01 contra el registro auxiliar al 31 de diciembre del 2016
CC-01		Inversión de capital	1.952	3.500	
AA-02	4	Equipo de transporte	6.544	---	
		1 ----- // ----- 1	<b>11.996</b>	<b>11.996</b>	
AA-02		Equipo de transporte	269.135	45.831	Corresponde a la revisión realizada de la cuenta AO-02 contra el registro auxiliar al 31 de diciembre del 2016
CC-01	5	Inversión de capital	45.831	269.135	
		1 ----- // ----- 1	<b>314.966</b>	<b>314.966</b>	
AO-03		Equipo de comunicación	8.664	4.284	Corresponde a la revisión realizada de la cuenta AO-03 contra el registro auxiliar al 31 de diciembre del 2016
CC-01		Inversión de capital	4.284	8.664	
	6	1 ----- // ----- 1	<b>327.914</b>	<b>327.914</b>	
AO-04		Equipo y mobiliario de oficina	147.841	147.841	Corresponde a la revisión realizada de la cuenta AO-04 contra el registro auxiliar al 31 de diciembre del 2016
CC-01		Inversión de capital	147.841	147.841	
	7	1 ----- // ----- 1	<b>147.841</b>	<b>147.841</b>	
AO11		Terrenos	466.238	80.687	Corresponde a la revisión realizada de la cuenta AO-011 contra el registro auxiliar al 31 de diciembre del 2016
CC-01		Inversión de capital	80.687	466.238	
		1 ----- // ----- 1	<b>546.925</b>	<b>546.925</b>	

## **RESULTADOS ENCONTRADOS DE LA EVALUACIÓN AL DEPARTAMENTO DE TECNOLOGÍAS DE INFORMACIÓN**

### **ORIGEN DEL ESTUDIO**

Como parte de la evaluación de los estados financieros de la Universidad Nacional (de ahora en adelante, UNA), realizamos la evaluación de los controles generales de la gestión de tecnología de información, con el objetivo de medir el grado de riesgo de la información en lo que respecta a seguridad, integridad, efectividad, eficiencia, confidencialidad, confiabilidad, disponibilidad y continuidad de la plataforma tecnológica.

La evaluación la realizamos basados en el manual de “Normas Técnicas para la Gestión y el Control de las Tecnologías de la Información (N-2-2007-CO-DFOE)” emitidas por la Contraloría General de la República, los Objetivos de Control de Tecnologías de Información (COBIT por sus siglas en inglés) emitidos por la “Information Systems Audit and Control Association” (ISACA por sus siglas en inglés) y en general las mejores prácticas de la industria de tecnología de información.

### **ALCANCE**

En esta visita el trabajo fue enfocado principalmente a las siguientes áreas:

1. Seguimiento a recomendaciones anteriores.
2. Verificación del control interno en materia tecnológica en base a la normativa interna establecida.
3. Recomendaciones identificadas en la evaluación.

El alcance de la auditoría realizada se fundamenta en lo establecido en las “Normas Técnicas para la Gestión y el Control de las Tecnologías de Información (N-2-2007-CO-DFOE)” emitido por la Contraloría General de la República.

### **OBJETIVO DEL ESTUDIO**

1. Establecer un entendimiento integral de la institución, así como de la plataforma tecnológica que soporta sus operaciones y documentación asociada.
2. Con el propósito de cumplir con los requerimientos estipulados en la Norma Internacional de Auditoría 315, Entendiendo de la realidad y su entorno y evaluación de representación errónea de importancia relativa y en la Norma Internacional de Auditoría 330, Procedimientos del auditor en respuesta a los riesgos evaluados, evaluamos la gestión de las tecnologías de información de la UNA.

## **PERIODO DE LA AUDITORÍA.**

El estudio se realizó durante los meses de julio y agosto del presente año y corresponde a la auditoría del periodo 2015.

## **LIMITACIONES DEL ESTUDIO.**

Durante el presente estudio de auditoría no se suministró la siguiente información o detalle sobre el estado del mismo:

1. Usuarios activos en Bases de Datos, únicamente se suministró del sistema BANNER.
  - a. Fechas de solicitud: Requerimientos iniciales 15 de julio de 2016, 27 de julio de 2016, 3 de agosto de 2016 y 5 de agosto de 2015.
  - b. Consecuencia: No se puede verificar la existencia de cuentas de ex funcionarios activos en Bases de Datos, a excepción de Banner.
2. Contratos activos con terceros en el periodo 2015 e informes de seguimiento que DTIC realiza para verificar el cumplimiento de los contratos del periodo 2015.
  - a. Fechas de solicitud: Requerimientos iniciales 15 de julio de 2016, 29 de julio de 2016, 3 de agosto de 2016, 5 de agosto de 2016.
  - b. Consecuencia: No se puede verificar que se realicen seguimiento al cumplimiento contractual de contratos en materia tecnológica, por tanto, se procede a realizar el hallazgo 04 del presente informe.
3. Toda la documentación relacionada al ciclo de vida del desarrollo de software, según la metodología de desarrollo interna, para el proyecto Sistema de Transporte Institucional o Pronósticos de la Demanda de Bienes.
  - a. Fechas de solicitud: esto se solicitó el día 5 de agosto, posterior a recibir la lista de desarrollos del periodo 2015 solicitados el 29 de julio de 2016, y 3 de agosto de 2016, y la metodología relacionada al ciclo de vida del desarrollo solicitada desde los requerimientos iniciales 15 de julio de 2016.
  - b. Consecuencia: No se puede verificar el cumplimiento de la metodología de gestión de desarrollo de software, así como dar seguimiento al hallazgo 14 “NO SE DOCUMENTAN LAS REVISIONES NI PRUEBAS DE CADA ETAPA DEL CICLO DE DESARROLLO DE SOFTWARE” de periodos anteriores.
4. Suministrar para los proyectos “Migración de las bases de datos de SIGESA a versión 12c Enterprise Edition de Oracle” o “Proyecto conjunto con CGT para Implementar sistemas de VDI, para la virtualización de escritorios en ambientes Windows y Linux” los siguiente: FO-DTIC-05-05 Carta Constitutiva del Proyecto,

FO-DTIC-05-07 Plan Gestión del Proyecto, FO-DTIC-05-10 Plantilla EDT o WBS, FO-DTIC-05-12 Roles y Funciones, FO-DTIC-05-15 Cronograma de eventos, FO-DTIC-05-18 Aseguramiento de la Calidad, Plan de administración de riesgos (FO-DTIC-06-18 Gestión de Riesgos de DTIC), FO-DTIC-05-19 Adquisición de Bienes y Servicios, FO-DTIC-05-28 Acta de Recepción.

- a. Fechas de solicitud: esto se solicitó el día 5 de agosto, posterior a recibir la lista de proyectos del periodo 2015 solicitados en requerimientos iniciales 15 de julio de 2016, 27 de julio de 2016, 29 de julio de 2016, 3 de agosto de 2016.
- b. Consecuencia: No se puede verificar el cumplimiento de la normativa relacionada a gestión de proyectos, por tanto, se procede a realizar el hallazgo 05 del presente informe.

## **METODOLOGÍA**

Para llevar a cabo este trabajo utilizamos una modalidad de análisis de la información suministrada por la Dirección de Tecnología de Información y Comunicación, aplicamos cuestionarios de control interno relacionados con la administración del Departamento, seguridad física y lógica de los sistemas de información, continuidad de las operaciones, políticas en cuanto al uso adecuado del equipo de cómputo, internet y correo, planes de capacitación, procesos de mantenimiento y reparación del equipo de cómputo, bitácoras de los sistemas, manuales de puestos, plan operativo anual y sistemas de información que posee la organización.

Además, se formularon preguntas sobre la existencia de controles informáticos, en todos los casos necesarios solicitamos a los funcionarios las evidencias en documentos escritos o en formato digital que respaldaran sus afirmaciones.

## HALLAZGOS Y RECOMENDACIONES

### **HALLAZGO 1: INCUMPLIMIENTO DE LA NORMATIVA RELACIONADA CON LA GESTIÓN DE CALIDAD PARA LOS SERVICIOS DE T.I. RIESGO MEDIO.**

#### **CONDICIÓN:**

Se determinó que la DTIC cuenta con un documento llamado “M-AGDTIC-001-2010 Manual de la calidad”. El documento está basado en la norma INTE-ISO 9001, y el alcance de aplicación del sistema de gestión de calidad (SGC) abarcando los siguientes procesos:

- Implementación Servicios TI en Telecomunicaciones.
- Desarrollo de Sitios WEB.
- Diseño Redes de Datos y Soporte de Servicios TI.
- Desarrollo Sistemas Informáticos.
- Soporte Técnico y Atención de Usuarios.
- Control y Supervisión de Servicios Informáticos.

Este manual de calidad adicionalmente cuenta con procedimientos relaciones sobre la revisión del SGC (P-AGDTIC-002-2010), solicitud y control de las acciones correctivas y preventivas, y emisión de mejoras (P-AGDTIC-002-2010), control de productos no conforme (P-AGDTIC-004-2010), auditorías internas (P-AGDTIC-005-2010) y control de registro (P-AGDTIC-006-2010).

Se solicitó como evidencia al cumplimiento de la normativa interna lo siguiente:

- Todos los planes de calidad del periodo 2015.
- El programa anual de auditorías internas del SGC del periodo 2015.
- Resultados de las mediciones del periodo 2015.
- Encuesta de satisfacción del cliente del periodo 2015.
- Documentación de productos no conformes, acciones correctivas y preventivas, el registro de los resultados de las acciones tomadas y la verificación de la efectividad de las acciones tomadas del periodo 2015.

Sin embargo, dado que el DTIC se encuentra en proceso de revisión y actualización de la documentación, se indicó a esta auditoría que no se tiene la evidencia al cumplimiento debido al proceso de transición que se tuvo en el año 2015 por medio de una consultoría con la empresa GTI. Cabe resaltar que se definió un plan de trabajo, en el cual en el ítem 11 se define el objetivo de clasificación de documentos de calidad, la ejecución de esta tarea es responsabilidad del Comité de Calidad.

Al no cumplir con lo estipulado en el documento M-AGDTIC-001-2010 Manual de la calidad y sus procedimientos relacionados a la gestión de calidad, podría no garantizarse una calidad suficiente en los servicios y productos de T.I., lo que podría provocar fallas, reprocesos e impedimento de la mejora continua.

## CRITERIO:

El apartado 1.2 “**Gestión de la calidad**” presente en el documento N-2-2007-CO-DFOE Normas Técnicas para la Gestión y Control de las Tecnologías de Información emitidas por la Contraloría General de la República menciona: “*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.*”

## RECOMENDACIONES:

### A la Dirección de Tecnología Informática:

Establecer y ejecutar acciones alternas para gestionar la calidad de los productos y servicios de TI mientras se efectúa la actualización de la normativa de gestión de calidad actual.

## **HALLAZGO 2: CUMPLIMIENTO PARCIAL DE LA METODOLOGÍA DEL SISTEMA ESPECÍFICO DE VALORACIÓN DEL RIESGO INSTITUCIONAL. RIESGO MEDIO.**

## CONDICIÓN:

Se verificó que la UNA cuenta con el Sistema Específico de Valoración del Riesgo Institucional (SEVRI), la cual define las etapas de identificación, valoración y administración de riesgos. Esta metodología permite gestionar riesgos de manera tal que se relacionen con las metas del Plan de Mediano Plazo 2013-2017 y cada riesgo se puede clasificar de manera cuantitativa y cualitativa, definiendo aspectos como frecuencia, consecuencia y niveles de riesgo. Adicionalmente permite clasificar niveles de madurez de medidas administrativas para afrontar los riesgos y las opciones de respuesta a los riesgos.

Por otra parte, se identificaron 36 riesgos relacionados con T.I., y para cada uno de estos riesgos se identifican aspectos como tipo de riesgo, escenarios y consecuencias generales del riesgo. Sin embargo, no son identificados para estos riesgos aspectos definidos en el SEVRI como frecuencia, consecuencia, nivel de madurez de medidas administrativas, niveles de riesgo, causas y efectos, riesgos inherentes y residuales, planes de acción, beneficios y costos, entre otros.

Al no cumplir con lo establecido en el marco de gestión de riesgos, no se garantiza que se haya realizado una adecuada administración del riesgo tecnológico en la UNA. Dado lo anterior, podría materializarse algún riesgo relacionado a tecnologías de información, potenciando la interrupción parcial o total de algún proceso crítico, pérdida financiera, fuga de datos, vulnerabilidades de seguridad, daños en la infraestructura, pérdida de calidad de los servicios, entre otros.



## CRITERIO:

El apartado 1.3 “**Gestión de riesgos**” presente en el documento N-2-2007-CO-DFOE Normas Técnicas para la Gestión y Control de las Tecnologías de Información emitida por la Contraloría General de la República menciona lo siguiente: “*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.*”

## RECOMENDACIONES:

### *A la Dirección de Tecnologías de Información y Comunicación:*

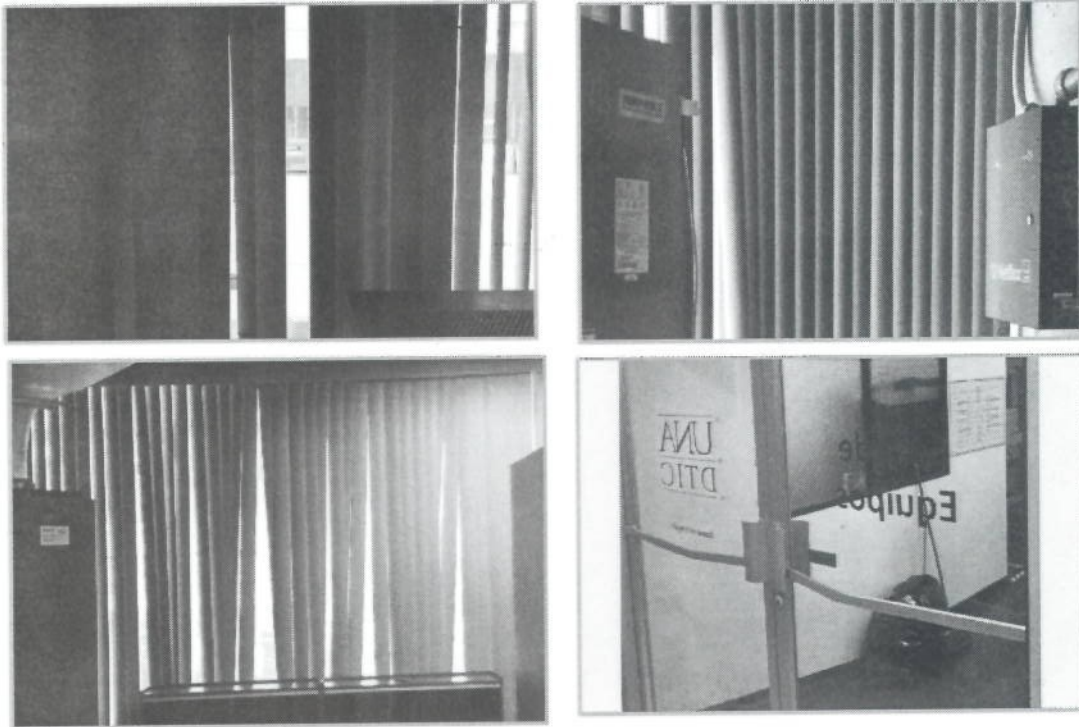
1. Finalizar con las etapas de valoración y administración de riesgos definido en el documento “Metodología del Sistema Específico de Valoración del Riesgo Institucional”.
2. Dar seguimientos periódicos a los riesgos identificados, evaluando la efectividad de los controles definidos. Esta tarea debe quedar documentada.
3. Revalorar los riesgos de forma periódica y actualizarlos de ser necesario.

## HALLAZGO 3: DEFICIENCIAS EN LA SEGURIDAD FÍSICA DE LOS CUARTOS DE SERVIDORES. RIESGO MEDIO.

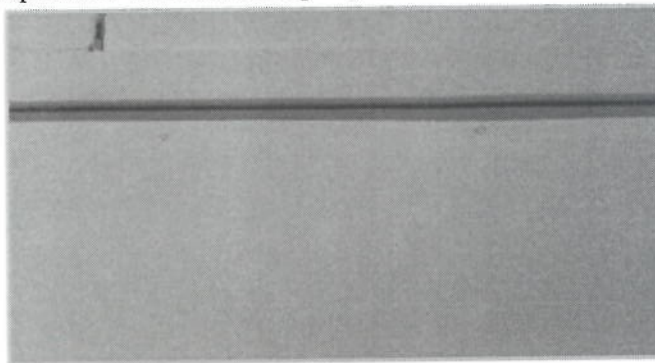
### CONDICIÓN:

Producto de la revisión efectuada a los cuartos de servidores de la UNA, se identificaron un conjunto de deficiencias en la seguridad física, las cuales se detallan a continuación:

- a) **Sobre el Centro de datos ubicado en las oficinas de la DTIC de la UNA en Heredia:**
  1. Existen ventanas en tres de las paredes del centro de datos, las cuales colindan con el exterior del edificio y la puerta de la entrada al centro de datos es de cristal, tal como se muestra en las siguientes imágenes:



2. Una de las paredes está formada por paneles de madera:

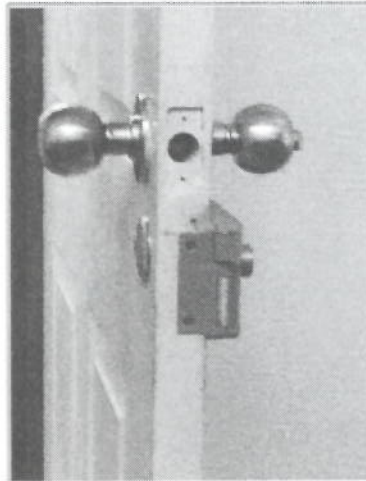


3. Existe equipo en desuso y desordenado en el suelo del centro de datos, como se muestra en la siguiente imagen:



**b) Sobre el cuarto de comunicaciones, el Rack A y Rack B ubicado en el campus de Nicoya**

1. Las puertas de acceso tienen llavines de tipo convencional, como se muestra en la siguiente imagen:



2. Algunas de las paredes son de paneles de madera como se muestra en la siguiente imagen:



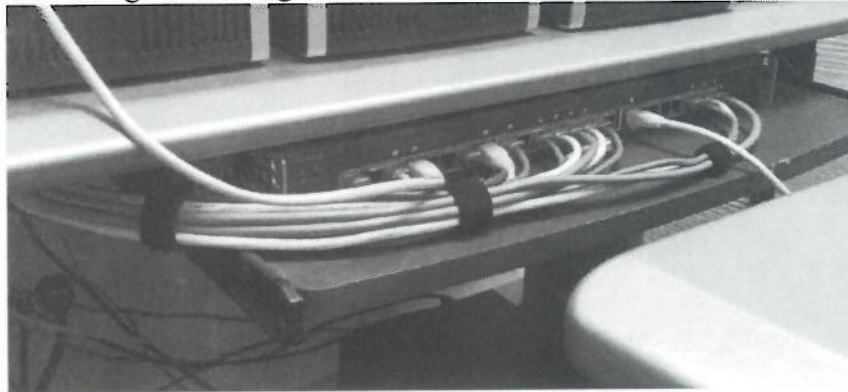
3. Existen ventanas que colindan al exterior, como se muestra en la siguiente imagen:



4. No existen medidores de humedad.
5. No existen detectores de humo.
6. Existen oficinas ubicadas dentro del cuarto de comunicaciones, Rack A y B.
7. Existen equipos en desuso desordenados y ubicados en el suelo en el cuarto de comunicaciones, como se muestra en la siguiente imagen:



8. Existe cableado ordenado, pero sin etiquetar en el cuarto de comunicaciones como se muestra en la siguiente imagen:



9. No se cuenta con bitácoras para el registro del acceso.
10. No se cuenta con contratos de mantenimiento para los equipos de UPS y aires acondicionados, el mantenimiento se realiza por personal interno y no es registrado en bitácoras.

#### **CRITERIO:**

El apartado 1.4.3, “**Seguridad física y ambiental**”, presente en el documento N-2-2007-CO-DFOE Normas Técnicas para la Gestión y Control de las Tecnologías de Información emitidas por la Contraloría General de la República menciona: “*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 esa 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 de TI.
- c. El ingreso y salida de equipos de la organización.
- d. El debido control de los servicios de mantenimiento.
- e. Los controles para el desecho y reutilización de recursos de TI.
- f. La continuidad, seguridad y control del suministro de energía eléctrica, del cableado de datos y de las comunicaciones inalámbricas.
- g. El acceso de terceros.
- h. Los riesgos asociados con el ambiente.”

#### **RECOMENDACIÓN:**

##### **A la Dirección de Tecnologías de Información y Comunicación en coordinación con la Vicerrectoría de Administración:**

Definir e implementar las acciones necesarias para subsanar las deficiencias identificadas en la sección Condición del presente hallazgo para el Centro de datos ubicado en las oficinas de la DTIC de la UNA en Heredia

##### **Al encargado del centro de comunicaciones de la sede de Nicoya:**

Definir e implementar las acciones necesarias para subsanar las deficiencias identificadas en la sección Condición del presente hallazgo para el centro de comunicaciones, Rack A y Rack B ubicado en el campus de Nicoya.

#### **COMENTARIOS ADMINISTRACIÓN:**

La DTIC ha estado gestionando la necesidad de un data center con mejores condiciones de las que tenemos actualmente, ante las autoridades superiores correspondientes (Rectoría, Vicerrectoría de Administración), según oficios UNA-DTIC-OFIC-150-2016, UNA-DTIC-OFIC-104-2016. DTIC-225-2014.

#### HALLAZGO 4: DEBILIDADES EN LA ADMINISTRACIÓN DE LOS CONTRATOS CON PROVEEDORES DE TI. RIESGO MEDIO.

##### CONDICIÓN:

Se verificó que la DTIC cuenta con documentación como plantillas y guías para la gestión formal de los contratos con terceros, en esta documentación se incluyen aspectos como guías de contratación para productos y servicios, guías para la evaluación de acuerdos de servicio, guías de cumplimiento para la contratación de terceros, procedimientos para documentar roles y responsabilidades de terceros y procedimientos para el seguimiento de servicios contratados a terceros, entre otros.

Se determinó que la DTIC cuenta con contratos con proveedores externos como por ejemplo el servicio de consultoría para la actualización de los procesos de TI gestionados en la DTIC, sin embargo, no se evidenció que los contratos cuenten con una estructura formal o que se dé un seguimiento adecuado sobre el cumplimiento de los contratos debido a que esta información no fue suministrada previa solicitud por parte de esta auditoría.

Al no poder revisar que los contratos tuviesen una estructura formal y adecuada y al no tener evidencia de que se realiza un seguimiento del cumplimiento de los contratos podría no garantizarse el cumplimiento de las obligaciones contractuales, plazos y calidad definida en los contratos. Además, podría existir el riesgo de realizar pagos de hitos o productos no finalizados; además de no contar con un seguimiento continuo de principio a fin del contrato que facilite la rendición de cuentas a los órganos superiores.

##### CRITERIO:

El apartado 4.6 “**Administración de servicios prestados por terceros**”, presente en el documento N-2-2007-CO-DFOE Normas Técnicas para la Gestión y Control de las Tecnologías de Información emitidas por la Contraloría General de la República menciona: “*La organización debe asegurar que los servicios contratados a terceros satisfagan los requerimientos en forma eficiente. Con ese fin, debe:*

- a. *Establecer los roles y responsabilidades de terceros que le brinden servicios de TI.*
- b. *Establecer y documentar los procedimientos asociados con los servicios e instalaciones contratados a terceros.*
- c. *Vigilar que los servicios contratados sean congruentes con las políticas relativas a calidad, seguridad y seguimiento establecidas por la organización.*
- d. *Minimizar la dependencia de la organización respecto de los servicios contratados a un tercero.*
- e. *Asignar a un responsable con las competencias necesarias que evalúe periódicamente la calidad y cumplimiento oportuno de los servicios contratados.”*

## RECOMENDACIONES:

### A la Dirección de Tecnologías de Información y Comunicación:

1. Cumplir con los lineamientos establecidos que guían la conformación y seguimiento formal de los contratos de TI con proveedores externos.
2. Mantener evidencia de las revisiones efectuadas a los contratos con terceros.

## HALLAZGO 5: DEBILIDADES EN LA METODOLOGÍA DE ADMINISTRACIÓN DE PROYECTOS DE DTIC. RIESGO BAJO.

### CONDICIÓN:

Se determinó que DTIC cuenta con una metodología y un procedimiento para la administración de proyectos debidamente documentados, con el fin de establecer el detalle de procesos definidos para cada una de las fases del ciclo de vida de desarrollo de proyectos. Adicionalmente se verifica que se definieron diferentes plantillas que permite elaborar los productos de cada etapa (inicio, planificación, ejecución, control y cierre del proyecto).

Por otra parte, se identificó que en el periodo 2015 se llevaron a cabo proyectos, sin embargo, no se evidenció que estos proyectos se ejecutaran apoyándose en la metodología y procedimiento para la gestión de proyectos debido a que no se suministró la evidencia solicitada por esta auditoría.

De no utilizarse la metodología formal para la gestión de proyectos no se garantiza una adecuada gestión de proyectos, potenciando el riesgo de que se tomen decisiones en base a información insuficiente.

### CRITERIO:

El apartado 1.5 “Gestión de proyectos” presente en el documento “Normas Técnicas para la Gestión y el Control de las Tecnologías de Información (N-2-2007-CO-DFOE)” de la Contraloría General de la República, menciona: “La organización debe administrar sus proyectos de TI de manera que logre sus objetivos, satisfaga los requerimientos y cumpla con los términos de calidad, tiempo y presupuesto óptimos preestablecidos”.

## RECOMENDACIÓN:

### A la Dirección de Tecnologías de Información y Comunicación:

Cumplir con lo definido en los documentos “Metodología de Gestión de Proyectos” y “Procedimiento de Gestión de Proyectos”, documentando para cada proyecto aspectos como:

- a. Carta Constitutiva del proyecto.
- b. Plan de gestión del proyecto.
- c. Estructura de desglose de trabajo.
- d. Roles y funciones.
- e. Cronograma de eventos.
- f. Aseguramiento de la calidad.
- g. Gestión de riesgos.
- h. Adquisición de bienes y servicios.
- i. Acta de recepción.

## HALLAZGO 6: DEBILIDADES EN LA EJECUTORÍA DEL COMITÉ DE ESTRATEGIA DE TI. RIESGO MEDIO.

### CONDICIÓN:

#### a) Sobre la ausencia de un reglamento que regule el accionar el CETI:

Mediante la resolución R-0556-R-2013/DTIC-005-2013 del 18 de setiembre de 2013, se creó el Comité de Estrategia de TI (CETI) y el Comité de Gestión de TI (COGETI). Por otra parte, mediante la resolución UNA-R-RESO-697-2015 del 30 de octubre de 2015, resuelve derogar el COGETI y mantener únicamente el CETI.

Ambas resoluciones estuvieron vigentes en el periodo 2015, indicado como se integrarán los comités y sus funciones y responsabilidades; sin embargo, no define los elementos necesarios que regule el accionar de dichos comités, a su vez se evidencia un reglamento adicional que satisfaga dicha necesidad.

#### b) Sobre la poca ejecutoría activa del CETI:

Se evidencia por medio del oficio DTIC-047-2015 del 25 de febrero de 2015 que se comunicó a los miembros del COGETI el cronograma de las próximas sesiones (23 de marzo, 20 de abril, 18 de mayo y 08 de junio).

Por otra parte, se evidencia una minuta con fecha de 5 de junio de 2015 entre el Director CGT, Director CGI y el Coordinador EGTI sobre la presentación de los proyectos de la sesión del 08 de junio; para esta última sesión se evidencia la invitación, la minuta y el oficio.



Sin embargo, solo se evidencia, el cronograma para cuatro sesiones y la ejecución de una sesión por parte del COGETI, y no se evidencia la ejecución de sesiones por parte del CETI antes o después de la resolución de mantener únicamente este comité.

Al no mantener una ejecutoría activa el Comité de Tecnologías de Información, podría darse el riesgo de tener soporte y participación deficiente de la alta dirección en los procesos claves de toma de decisiones tecnológicos, lo que podría conllevar a que no se discutan temas importantes como la priorización de los proyectos de TI, la asignación de recursos y la atención de los requerimientos.

#### **CRITERIO:**

Asimismo el apartado 1.6 “Decisiones sobre asuntos estratégicos de TI” presente en el documento “Normas Técnicas para la Gestión y el Control de las Tecnologías de Información (N-2-2007-CO-DFOE)” de la Contraloría General de la República, menciona: “El jerarca debe apoyar sus decisiones sobre asuntos estratégicos de TI en la asesoría de una representación razonable de la organización que coadyuve a mantener la concordancia con la estrategia institucional, a establecer las prioridades de los proyectos de TI, a lograr un equilibrio en la asignación de recursos y a la adecuada atención de los requerimientos de todas las unidades de la organización”.

#### **RECOMENDACIÓN:**

##### **Al Rector en conjunto con la Dirección de Tecnologías de Información y Comunicación:**

1. Definir, aprobar y divulgar un reglamento que regule el accionar del CETI de la UNA, el mismo debe considerar al menos lo siguiente:
  - a. Objeto del Comité de TI
  - b. Conformación del Comité de TI.
  - c. Funciones y responsabilidades.
  - d. Actas.
  - e. Acuerdos.
  - f. Quórum.
  - g. Sesiones.
  - h. Grupos de trabajo.
  - i. Vigencia.
  
2. Documentar mediante actas las sesiones tanto ordinarias como extraordinarias que realicen el CETI, así como sesionar periódicamente con el fin de garantizar que se cumple con los objetivos para el cual fue creado el mismo. Las actas deben indicar al menos lo siguiente:
  - a. Número de acta.
  - b. Fecha, hora de inicio y hora final.
  - c. Presentes, ausentes e invitados.
  - d. Temas tratados.

- e. Acuerdos tomados, indicando los responsables y las fechas de ejecución.
- f. Seguimiento a acuerdos de sesiones anteriores.
- g. Firmas.

## HALLAZGO 7: INCONSISTENCIAS EN LOS INVENTARIOS DE SOFTWARE GENERAL E INSTALADO POR EQUIPO. RIESGO MEDIO.

### CONDICIÓN:

Producto de la revisión efectuada se identificaron las siguientes situaciones:

1. Se cuenta con un inventario general de licencias adquiridas en el que se detalla el nombre del software, el proveedor y la fecha de vencimiento de la licencia entre otros aspectos, sin embargo, se identificó que no se indica la cantidad de licencias adquiridas para el siguiente software:
  - a. Erwin
  - b. Compilador COBOL – Fujitsu
  - c. Oracle 2 RDBMS SE
  - d. Licencias SQL Server EE
  - e. SQL- server enterprise edition
  - f. Axure RP Pro

El inventario de software instalado por equipo se limita únicamente a tres máquinas virtuales y tres servidores no se incluye otros equipos como computadoras de escritorio y portátiles, se indicó que no se cuenta con herramientas para obtener este tipo de información de los equipos.

2. No se cuenta con un listado de software libre permitido en la Institución.

Esta condición puede presentarse por deficiencias en el proceso de adquisición y control de las licencias de software, lo cual podría provocar eventualmente inconsistencias en la gestión del software instalado en la institución, además el mantener software que no cuenta licencias podría provocar problemas como la falta de soporte por parte de los proveedores. Por otra parte, no se cuenta con una herramienta que pueda identificar el software instalado en cada máquina de la UNA.

### CRITERIO:

El apartado 4.2, “**Administración y operación de la plataforma tecnológica**”, presente en el documento “Normas Técnicas para la Gestión y el Control de las Tecnologías de Información (N-2-2007-CO-DFOE)” de la Contraloría General de la República, menciona:

*“La organización debe mantener la plataforma tecnológica en óptimas condiciones y minimizar su riesgo de fallas. Para ello debe:*

- a. *Establecer y documentar los procedimientos y las responsabilidades asociados con la operación de la plataforma.*
- b. *Vigilar de manera constante la disponibilidad, capacidad, desempeño y uso de la plataforma, asegurar su correcta operación y mantener un registro de sus eventuales fallas.*
- c. *Identificar eventuales requerimientos presentes y futuros, establecer planes para su satisfacción y garantizar la oportuna adquisición de recursos de TI requeridos tomando en cuenta la obsolescencia de la plataforma, contingencias, cargas de trabajo y tendencias tecnológicas.*
- d. *Controlar la composición y cambios de la plataforma y mantener un registro actualizado de sus componentes (hardware y software), custodiar adecuadamente las licencias de software y realizar verificaciones físicas periódicas.*
- e. *Controlar la ejecución de los trabajos mediante su programación, supervisión y registro.*
- f. *Mantener separados y controlados los ambientes de desarrollo y producción.*
- g. *Brindar el soporte requerido a los equipos principales y periféricos.*
- h. *Definir formalmente y efectuar rutinas de respaldo, custodiar los medios de respaldo en ambientes adecuados, controlar el acceso a dichos medios y establecer procedimientos de control para los procesos de restauración.*
- i. *Controlar los servicios e instalaciones externos.”*

## **RECOMENDACIONES:**

### **A la Dirección de Tecnologías de Información y Comunicación:**

1. Mantener un inventario general de software adquirido y permitido, así como otro instalado por equipo actualizado, incluyendo equipos como (servidores, máquinas virtuales, computadoras de escritorio y portátiles, etc.) a nivel institucional.
2. Hacer uso, únicamente de las licencias adquiridas, desinstalando las licencias que no cuentan con los derechos de instalación respectivos o bien, obtener las licencias adicionales, requeridas para suplir las necesidades de la UNA.
3. Reemplazar el software que ya no cuenta con soporte del proveedor o se encuentra vencido, por versiones más actualizadas y que cuenten con soporte en los casos que sea necesario.

## **HALLAZGO 8: AUSENCIA DE UN PROCEDIMIENTO ACTUALIZADO PARA LA ATENCIÓN DE INCIDENTES Y PROBLEMAS DE TECNOLOGÍAS DE INFORMACIÓN. RIESGO MEDIO.**

### **CONDICIÓN:**

Se determinó que el DTIC cuenta con un procedimiento y formulario para la atención de incidentes llamada “P-AGDTIC-030-2011-MANEJO DE INCIDENTES” y “F-AGDTIC-030-2011-MANEJO DE INCIDENTES”, respectivamente, sin embargo, con la entrada a producción de la herramienta iTOP, esta normativa se encuentra desactualizada.

La herramienta iTOP permite gestionar todo el ciclo de vida de este tipo de solicitudes, mediante la circular “CIRCULAR DTIC-CGT-001-2014”, se comunicó a la comunidad universitaria que las solicitudes de requerimientos e incidentes se deben realizar por medio de la herramienta iTOP, remplazándolo por solicitudes de llamadas telefónicas, correo electrónico o de manera verbal.

Sin embargo, no se evidencia la existencia de una metodología o procedimiento actualizado que permita gestionar todo el ciclo de vida de las solicitudes de requerimiento e incidentes por medio de la nueva herramienta, que les provea a los usuarios/agentes una guía para tomar decisiones sobre como clasificar, priorizar, escalar y realizar las demás tareas para la gestión adecuada de este proceso.

Al no poseer una metodología formal para atención de incidentes, no se garantiza que se dé una adecuada administración a los incidentes, minimizando el riesgo de recurrencia y procurando el aprendizaje necesario.

### **CRITERIO:**

El apartado 4.5, “**Manejo de incidentes**” presente en el documento N-2-2007-CO-DFOE Normas Técnicas para la Gestión y Control de las Tecnologías de Información emitidas por la Contraloría General de la República menciona: “*La organización debe identificar, analizar y resolver de manera oportuna los problemas, errores e incidentes significativos que se susciten con las TI. Además, debe darles el seguimiento pertinente, minimizar el riesgo de recurrencia y procurar el aprendizaje necesario*”.

### **RECOMENDACIONES:**

#### **A la Dirección de Tecnologías de Información y Comunicación:**

Actualizar y aprobar formalmente un procedimiento para la gestión de todo el ciclo de atención incidentes y problemas. Este procedimiento debe considerar al menos los siguientes aspectos:

- Roles y responsabilidades (solicitante, administrador/responsable, agente/encargado).
- Información del incidente: asunto, descripción, fecha y hora de apertura del incidente, estados.
- Priorización y categorización.
- Escalamiento.
- KPIs y reportes.
- Auto-Ayuda.
- Encuestas de satisfacción.

### **HALLAZGO 9: AUSENCIA DE UN PLAN DE CAPACITACIÓN FORMAL PARA EL PERSONAL DEL DTIC. RIESGO BAJO.**

#### **CONDICIÓN:**

Se determinó por medio del Programa de Desarrollo de Recursos Humanos que se está implementando de forma paulatina el Sistema de Valoración del Desempeño para el Sector Administrativo, el cual permite generar Planes de Desarrollo Personal.

Sin embargo, a la fecha, la Dirección de Tecnologías de Información y Comunicación no ha tenido cobertura en el sistema, tampoco se evidencia que se hayan aplicado planes de capacitación al equipo de DTIC en el periodo 2015, utilizando otras herramientas o métodos. Pese a lo anterior cabe señalar que se indicó que para el 2015 la Institución invirtió en la capacitación técnica de 36 funcionarios del DTIC, para un total de 58 actividades formativas.

Se indica por parte del Programa de Desarrollo de Recursos Humanos que se espera sea incorporado la DTIC al sistema en el periodo 2017 y la atención de los resultados de los procesos formativos se llevaría a cabo en el 2018.

Cabe mencionar que la DTIC elaboró Planes de Capacitación para el año 2016, como una acción alterna para administrar las capacitaciones en esta dirección, estos planes posteriormente se deben alinear a la estrategia de recursos humanos y a las mejores prácticas.

Al no desarrollar y aprobar formalmente planes de capacitación para el personal de la Dirección de Tecnologías de Información y Comunicación, podría no garantizarse que el Centro de Gestión Tecnológica y Centro de Gestión Informática cuente con una fuerza de trabajo suficientemente motivada y competente, donde se refuerce áreas de conocimiento deficientes, como por ejemplo: estándares mundiales, tecnologías emergentes y habilidades interpersonales.

## CRITERIO:

El apartado 2.4 “**Independencia y recurso humano de la Función de TI**” presente en el documento N-2-2007-CO-DFOE Normas Técnicas para la Gestión y Control de las Tecnologías de Información emitida por la Contraloría General de la República menciona lo siguiente: “*El jerarca debe asegurar la independencia de la Función de TI respecto de las áreas usuarias y que ésta mantenga la coordinación y comunicación con las demás dependencias tanto internas y como externas.*”

*Además, debe brindar el apoyo necesario para que dicha Función de TI cuente con una fuerza de trabajo motivada, suficiente, competente y a la que se le haya definido, de manera clara y formal, su responsabilidad, autoridad y funciones.”*

## RECOMENDACIONES:

### Al Programa de Desarrollo de Recursos Humanos en conjunto con la Dirección de Tecnologías de Información y Comunicación:

Establecer y ejecutar acciones alternas para crear y ejecutar planes de capacitaciones para el personal de la DTIC, mientras se incorpora al CGI y CGT al Sistema de Valoración del Desempeño, debido a que el PDRH prevé que serán incorporados hasta el 2017 y con atención de los resultados de los procesos formativos hasta el 2018, considerando al menos los siguientes aspectos:

- a. Alineación estratégica.
- b. Objetivos del plan de capacitación.
- c. Temas o áreas de conocimiento que se desean abordar.
- d. Priorización de los temas o áreas de conocimiento que se desea abordar.
- e. Cantidad de personal y personal al que va dirigido la capacitación.
- f. Fechas de ejecución de las capacitaciones.
- g. Costos asociados (capacitación, material, entre otros).

## HALLAZGO 10: CUENTAS DE EXFUNCIONARIOS HABILITADAS EN EL SISTEMA BANNER. RIESGO MEDIO.

### CONDICIÓN:

Producto de la revisión efectuada se identificó la existencia de cuentas activas de exfuncionarios en el sistema BANNER. A continuación, se enlistan los exfuncionarios activos.

Nombre de Exfuncionario	Motivo de salida	Fecha de salida
Rosa Adolio Cascante	Renuncia	01/03/2015
Manuel Chávez Núñez	Despido sin responsabilidad patronal	22/09/2015
Rolando Mora Zelada	Cese funciones por pensión o defunción	01/07/2015

Eduardo Saxe Fernández

Cese funciones por pensión o defunción

01/03/2015

De no removerse las cuentas de exfuncionarios en un tiempo oportuno, puede provocarse que personas que ya no pertenecen a la institución puedan acceder a información de la organización.

**CRITERIO:**

El apartado **1.4.5, “Control de acceso”** presente en el documento N-2-2007-CO-DFOE Normas Técnicas para la Gestión y Control de las Tecnologías de Información emitidas por la Contraloría General de la República menciona: *“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 de aplicación, a las bases de datos y a las terminales y otros recursos de comunicación.*
- b. Clasificar los recursos de TI en forma explícita, formal y uniforme de acuerdo con términos de sensibilidad.*
- c. Definir la propiedad, custodia y responsabilidad sobre los recursos de TI.*
- d. Establecer procedimientos para la definición de perfiles, roles y niveles de privilegio, y para la identificación y autenticación para el acceso a la información, tanto para usuarios como para recursos de TI.*
- e. Asignar los derechos de acceso a los usuarios de los recursos de TI, de conformidad con las políticas de la organización bajo el principio de necesidad de saber o menor privilegio. Los propietarios de la información son responsables de definir quiénes tienen acceso a la información y con qué limitaciones o restricciones.*
- f. Implementar el uso y control de medios de autenticación (identificación de usuario, contraseñas y otros medios) que permitan identificar y responsabilizar a quienes utilizan los recursos de TI. Ello debe acompañarse de un procedimiento que contemple la requisición, aprobación, establecimiento, suspensión y desactivación de tales medios de autenticación, así como para su revisión y actualización periódica y atención de usos irregulares.*
- g. Establecer controles de acceso a la información impresa, visible en pantallas o almacenada en medios físicos y proteger adecuadamente dichos medios.*
- h. Establecer los mecanismos necesarios (pistas de auditoría) que permitan un adecuado y periódico seguimiento al acceso a las TI.*
- i. Manejar de manera restringida y controlada la información sobre la seguridad de las TI.”*

## RECOMENDACIONES:

### *Al Programa de Desarrollo de Recursos Humanos en conjunto con DTIC.*

1. Eliminar o inactivar del sistema BANNER, las cuentas de los exfuncionarios de la UNA señalados en la condición de este hallazgo.
2. Establecer un mayor control formal en la gestión de accesos a los sistemas, deshabilitando las cuentas de usuarios que ya no deberían tener acceso a la plataforma tecnológica en un tiempo oportuno, considerando la implementación de un procedimiento mediante el cual Programa de Desarrollo de Recurso Humano le notifique a la Dirección de Tecnologías de Información y Comunicación cada vez que un funcionario abandona la institución.



**MATRIZ DE SEGUIMIENTO A CG ANTERIORES**

<b>Carta a Gerencia 2014</b>	
<b>HALLAZGO 9: NO SE REALIZAN EVALUACIONES SOBRE EL DESEMPEÑO A LOS COLABORADORES DE T.I. RIESGO BAJO.</b>	
<b>RECOMENDACIÓN</b>	<ol style="list-style-type: none"> <li>1. Realizar evaluaciones al desempeño de los colaboradores de la DTIC periódicamente, la cual debe estar fundamentada en una serie de principios básicos que orienten su desarrollo, estos son:               <ul style="list-style-type: none"> <li>• La evaluación del desempeño debe estar unida al desarrollo de las personas en la organización o área de trabajo.</li> <li>• Los estándares de la evaluación del desempeño deben estar fundamentadas en información relevante del puesto de trabajo.</li> <li>• Deben definirse claramente los objetivos del sistema de evaluación del desempeño.</li> <li>• El sistema de evaluación del desempeño requiere el compromiso y participación activa de todos los trabajadores.</li> <li>• El papel de juez del supervisor-evaluador debe considerarse la base para aconsejar mejoras.</li> </ul> </li> </ol>
<b>COMENTARIOS ADMINISTRACIÓN</b>	<b>PENDIENTE</b>
<b>ESTADO</b>	<p>Se indica por parte del Programa de Desarrollo de Recursos Humanos de la UNA, que se está implementando en la Institución de manera paulatina el Sistema de Valoración de Desempeño para el Sector Administrativo(SVDA), por lo que hay instancias que a la fecha no han tenido cobertura, entre ellas la Dirección de Tecnologías de Información y Comunicación, por tanto, no se han realizado evaluación del desempeño para los integrantes del CGI y CGT.</p>
<b>HALLAZGO 10: NO IMPLEMENTACIÓN DE TODOS LOS PLANES DE CONTINGENCIA DEFINIDOS. RIESGO MEDIO.</b>	
<b>RECOMENDACIÓN</b>	<ol style="list-style-type: none"> <li>1. Revisar e implementar todos los planes de contingencia que han sido desarrollados por la UNA y que están bajo la responsabilidad de la DTIC.</li> <li>2. Realizar pruebas al plan de contingencias y continuidad, definiendo aplicaciones o componentes de la prueba, participantes de la prueba, revisión de actividades (nombre de la actividad, fecha, responsable, estado de la actividad, entre otros).</li> <li>3. Documentar los resultados de las pruebas realizadas, determinando los ajustes que sean necesarios e indicando lo funcional o no del plan.</li> </ol>
<b>COMENTARIOS</b>	Responsable: Comité de Seguridad, Jefes de Áreas de Trabajo del CGI y CGT.

<b>Carta a Gerencia 2014</b>	
<b>ADMINISTRACIÓN</b>	Fecha o plazo de implementación: 30/10/2016, 30/01/2017, 30/05/2017
<b>ESTADO</b>	<b>PENDIENTE</b>  Se solicitó evidencia al cumplimiento de la normativa relacionada a contingencia y continuidad, entre otra información, se solicitó los planes de prueba para los Switches-CORE, Routers, Telefonía IP, Firewall, BANNER y NX, sin embargo, estos no fueron suministrados, se indicó “para el año, 2015 (ni ningún otro año) no hubo un plan de pruebas de los procedimientos y planes sobre contingencia y continuidad”.
<b>RECOMENDACIÓN</b>	<b>HALLAZGO 11: DEBILIDADES EN EL SISTEMA INTEGRADO DE INVERSIONES (SICOI). RIESGO MEDIO.</b>  1. Llevar a cabo la implementación de un sistema informático para el control de las inversiones de la Universidad Nacional, en este proyecto debe participar activamente el departamento de tesorería, junto con la Dirección de T.I. y Comunicación, con el fin de lograr una implementación exitosa de dicho sistema.  2. El nuevo sistema debe de generar un registro auxiliar de inversiones que contenga al menos los siguientes campos: <ul style="list-style-type: none"> <li>● Número de operación.</li> <li>● Puesto de bolsa.</li> <li>● Rendimiento.</li> <li>● Serie.</li> <li>● Emisión.</li> <li>● Instrumento.</li> <li>● Tasa facial.</li> <li>● Monto facial.</li> <li>● Costo.</li> <li>● Interés comprado.</li> <li>● Tipo de vector.</li> <li>● Fecha de compra.</li> <li>● Fecha de vencimiento.</li> <li>● Fechad de último pago.</li> <li>● Fecha de próximo pago.</li> <li>● Interés acumulado.</li> <li>● Valor de libros.</li> </ul>

**Carta a Gerencia 2014**

	<ul style="list-style-type: none"> <li>• Precio de mercado.</li> <li>• Valor de mercado</li> </ul>
COMENTARIOS ADMINISTRACIÓN	<p>Dentro del alcance del proyecto SIGESA está desarrollar un nuevo sistema de inversiones. Fecha o plazo de implementación: 31/07/2018</p> <p><b>PROCESO</b></p> <p>Se indica por parte del área usuaria, que actualmente el registro auxiliar de inversiones es un control que se lleva tanto en Excel como en el sistema, de la misma forma como se realizaba en la auditoría del periodo anterior.</p> <p>Sin embargo, se agrega que está en proceso un nuevo sistema de inversiones que se viene trabajando desde el año pasado, todo a través de un grupo de trabajo de la UNA llamado SIGESA. Sobre el avance de las gestiones para subsanar las deficiencias, el área usuaria suministró correos donde se agendan reuniones donde se tratan asuntos relacionados al tema, así como el documento de Especificaciones para el módulo de inversiones.</p> <p>Además, esto es verificado por parte del DTIC, el cual, por medio del Plan de Implementación de Disposiciones Administrativas, indica que esta deficiencia está dentro del alcance del proyecto SIGESA sobre el desarrollo de un nuevo sistema de información, con fecha final de implementación al 2017.</p>
ESTADO	<p><b>HALLAZGO 12: EL SISTEMA BANNER NO GENERA UN REPORTE DE ANTIGÜEDAD DE SALDOS DE CUENTAS POR COBRAR Y CUENTAS POR PAGAR. RIESGO MEDIO.</b></p>
RECOMENDACIÓN	<ol style="list-style-type: none"> <li>1. Confeccionar un registro auxiliar de cuentas por cobrar y cuentas por pagar, en el sistema BANNER, llevando un control de las cuentas que están clasificadas como irrecuperables.</li> <li>2. Para la actividad anterior se debe de generar los requerimientos necesarios por parte de las áreas usuarias para su presentación a la DTIC.</li> </ol>
COMENTARIOS DE LA ADMINISTRACIÓN	<p>Gestiones para minimizar o eliminar efectos: Desarrollar un reporte de antigüedad de CxC y CxP en Banner. Fecha o plazo de implementación: 30/11/2016</p> <p><b>PROCESO</b></p>
ESTADO	<p>Respecto a la deficiencia relacionada a que el sistema BANNER, las áreas usuarias suministraron evidencia y el detalle de las acciones que se han realizado para subsanar dicha evidencia, entre ellas:</p> <ul style="list-style-type: none"> <li>• CxP: dos reportes FZRCUPA y FZRCPLA los cuales detallan las cuentas por pagar pendientes, vencidas y no vencidas para rangos de días o indicando los parámetros requeridos, para ambos casos se suministró un</li> </ul>

**Carta a Gerencia 2014**

	<p>ejemplo como evidencia.</p> <ul style="list-style-type: none"> <li>CxC: dos reportes TZRANSA y TZRDASA los cuales son relacionados a cuentas por cobrar estudiantiles por antigüedad de saldos, para ambos casos se suministró un ejemplo como evidencia.</li> </ul> <p>Además, DTIC suministró dos oficios (UNA-DTIC-CGI-OFIC-296-2016 y UNA-DTIC-CGI-OFIC-297-2016) enviados el 29 de julio de 2016 y 3 de agosto de 2016, en el cual se comunica al CGI sobre el estado de avance de implementación, y se indica que los reportes CxC está en etapa de pruebas para aprobación por parte de los usuarios finales, respecto a los reportes CxP se daba por implementado.</p>
<p><b>HALLAZGO 13: EL SISTEMA BANNER NO GENERA UN REPORTE DEL VALOR HISTÓRICO DE LOS ACTIVOS. RIESGO MEDIO.</b></p>	
<p><b>RECOMENDACIÓN</b></p>	<p>1. Generar un reporte de activos por medio del sistema BANNER, que permita llevar un control del valor histórico de los activos y su respectiva depreciación, para la realización de esta mejora debe participar activamente el encargado de activos, junto con la Dirección de T.I. y Comunicación, con el fin de lograr una implementación exitosa de la mejora solicitada.</p>
<p><b>COMENTARIOS ADMINISTRACIÓN</b></p>	<p>Gestiones para minimizar o eliminar efectos: desarrollar un reporte de valor histórico de los activos Fecha o plazo de implementación: 30/11/2016 <b>PENDIENTE</b></p>
<p><b>ESTADO</b></p>	<p>Se solicitó evidencia sobre las gestiones realizadas para subsanar la deficiencia, sin embargo, el área usuaria indicó que “se comprueba que ninguna de las formas utilizadas para generar reportes, extrae el valor histórico de los activos a una fecha determinada o rango de fecha; falencia del sistema que tendrá nuevamente que solicitarse mediante ITOP a los ingenieros informáticos destacados”.</p> <p>Por otra parte, el DTIC tampoco suministró evidencia del avance de implementación del reporte del valor histórico de los activos, únicamente informó por medio del Plan de Implementación de Disposiciones Administrativas, que esta recomendación será subsanada con un plazo límite a noviembre de 2016.</p>

**Carta a Gerencia 2014**

<b>HALLAZGO 14: NO SE DOCUMENTAN LAS REVISIONES NI PRUEBAS DE CADA ETAPA DEL CICLO DE DESARROLLO DE SOFTWARE. RIESGO MEDIO.</b>	
<b>RECOMENDACIÓN</b>	<ol style="list-style-type: none"> <li>1. Establecer un plan de pruebas para verificar el correcto funcionamiento del sistema antes de ponerlo en producción. Estas pruebas deben ejecutarse sobre un ambiente de pruebas que emule al ambiente en producción en el cual se van a implementar los sistemas de información.</li> <li>2. Establecer un plan de pruebas posterior a la implementación para garantizar la aceptación por parte de las áreas usuarias.</li> <li>3. Documentar las revisiones y pruebas de cada etapa del ciclo de desarrollo de software.</li> <li>4. Es deseable que el Centro de Gestión Informática (CGI) lleve a cabo la aprobación formal de la metodología de desarrollo de sistemas.</li> </ol>
<b>COMENTARIOS ADMINISTRACIÓN</b>	<p>Gestiones para minimizar o eliminar efectos: redactar y distribuir a todos los jefes y coordinadores de desarrollo el apego a los procedimientos de prueba aprobados, los cuales implican documentar y dejar en evidencia de las pruebas que se realicen.</p> <p>Fecha o plazo de implementación: 29/07/2016</p>
<b>ESTADO</b>	<b>PROCESO</b>
	<p>Se solicitó evidencia de toda la documentación del ciclo de vida para uno de los proyectos Sistema de Transporte Institucional o Pronósticos de la Demanda de Bienes, sin embargo, esto no fue suministrado. Para la verificación de las acciones para la definición de un procedimiento para la atención de cambios a los sistemas en producción se constató que se realizaron pruebas y especificación de casos de pruebas para el proyecto de migración/actualización del sistema BANNER.</p>
<b>HALLAZGO 15: NO SE HA APROBADO FORMALMENTE LA POLÍTICA DE RESPALDOS DE LA INFORMACIÓN. RIESGO BAJO.</b>	
<b>RECOMENDACIÓN</b>	<ol style="list-style-type: none"> <li>1. Definir fechas de revisión y aprobación de los lineamientos de respaldos de la información. La Dirección de Tecnologías de Información y Comunicación (DTIC) es la encargada de llevar a cabo dicha aprobación.</li> <li>2. Enviar a todos los funcionarios involucrados, por correo electrónico o algún otro medio válido, el comunicado oficial de la política o procedimiento aprobada.</li> <li>3. Verificar el cumplimiento de la política o procedimiento periódicamente.</li> </ol>
<b>COMENTARIOS ADMINISTRACIÓN</b>	<p>Elaborada y aprobada el 26 de mayo de 2016.</p>

**Carta a Gerencia 2014**

	<p><b>CORREGIDO</b></p> <p>Se informa que la política de respaldos del DTIC fue aprobado formalmente por el Director del CGI, Director del CGT y Director del DTIC en mayo de 2016 por medio del documento PO-DTIC-02-03, por tanto, la deficiencia se encuentra corregido.</p> <p><b>HALLAZGO 16: DEFICIENCIAS EN LA SEGURIDAD LÓGICA DE ALGUNOS SISTEMAS DE LA UNIVERSIDAD NACIONAL. RIESGO MEDIO.</b></p>
<p><b>RECOMENDACIÓN</b></p>	<ol style="list-style-type: none"> <li>1. Tomar las acciones necesarias para asegurar que los sistemas implantados en la Universidad Nacional cuenten con una seguridad lógica adecuada.</li> <li>2. Las medidas de seguridad lógica deben verse reflejadas en una política de seguridad.</li> <li>3. Realizar revisiones periódicas formales a la seguridad lógica implementada.</li> </ol> <p>Gestiones para minimizar o eliminar efectos: 1. Identificar los sistemas con deficiencias en la seguridad lógica, 2. Actualizar las políticas de seguridad, 3. Documentar para normar cómo se realizan las revisiones lógicas formales de los sistemas.</p> <p>Fecha o plazo de implementación: 30/09/2016</p>
<p><b>COMENTARIOS ADMINISTRACIÓN</b></p>	<p><b>PROCESO</b></p> <p>No se evidencia que se hayan realizado acciones para subsanar las siguientes deficiencias:</p> <ul style="list-style-type: none"> <li>• LDAP: vencimiento una vez al año y no guarda histórico de contraseñas.</li> <li>• NX: mecanismo para el vencimiento de clave, histórico de contraseñas o composición de contraseña, se indica por parte del DTIC que este sistema no cuenta con ninguna norma, política o lineamiento con respecto a la composición y administración de las contraseñas.</li> </ul> <p>Para el caso de LDAP que se indicaba en el hallazgo que las claves no son alfanuméricas, se suministró evidencia de las reglas de cambio de clave y se subsana esta deficiencia.</p>
<p><b>ESTADO</b></p>	

### Carta a Gerencia 2014

## OPORTUNIDAD DE MEJORA 1: NO SE DOCUMENTAN PROYECCIONES CON BASE EN LAS CAPACIDADES DE LA PLATAFORMA TECNOLÓGICA ACTUAL DE LA UNIVERSIDAD NACIONAL. RIESGO BAJO.

1. Identificar y documentar posibles impactos a futuro sobre la capacidad y el desempeño de la plataforma tecnológica, los cuales deben ser incluidos en el plan para tal efecto, considerando entre otros los siguientes factores:
  - a. Los objetivos, planes y estrategias de la Universidad Nacional y el rol de las tecnologías de información en su soporte.
  - b. Los nuevos servicios, sistemas y procesos de tecnologías de información por implementar.
  - c. Capacidad actual de la plataforma tecnológica.
2. Definir los planes de acción necesarios para solventar cualquier deficiencia de capacidad y desempeño identificada en el análisis de las proyecciones realizadas.
3. Establecer un plan formal para la administración de la capacidad y desempeño de la plataforma tecnológica de la UNA, el cual incluya factores como los siguientes:
  - Administración de la capacidad de la plataforma tecnológica:
    - Promedios de tiempos de respuesta.
    - Cantidad de transacciones diarias.
    - Generación de informes.
  - Monitoreo de la capacidad de procesamiento de los servidores principales.
  - Evaluación periódica del rendimiento de los equipos principales de la plataforma tecnológica.
  - Evaluaciones y motivos de la interrupción de los servicios.
  - Administración de las operaciones y configuraciones.
  - Programación calendarizada de las tareas.
  - Monitoreo del crecimiento de la configuración de la plataforma tecnológica.
  - Mecanismos de control que garanticen la ausencia de software o hardware no autorizado.
  - Asignación de responsabilidad por la administración de la configuración.
  - Identificación de los distintos elementos de la configuración de la plataforma tecnológica.

### RECOMENDACIÓN

**Carta a Gerencia 2014**

COMENTARIOS ADMINISTRACIÓN	<p>Una vez elaborado el POA de la DTIC, entre los siguientes dos meses calendario, se realizará:</p> <ul style="list-style-type: none"> <li>• Presentar propuesta de inversión anual de ampliación de la plataforma tecnológica.</li> <li>• Presentar propuesta de aumento anual de los servicios de telecomunicaciones arrendados.</li> <li>• Informe del estado de los equipos principales de infraestructura y su capacidad presente y futura.</li> </ul> <p>Con base en lo anterior, se hará solicitud de presupuesto de inversión para el siguiente año calendario. Se establecerá una directriz para definir los elementos de la infraestructura que requerirá ser monitoreada, evaluada y administrada</p> <p>Se elaborará un procedimiento para el seguimiento de la directriz anterior.</p> <p>Fecha o plazo de implementación: 30/09/2016, 30/11/2016,28/02/2017 y 30/05/2017 respectivamente.</p>
ESTADO	<p><b>PENDIENTE</b></p> <p>Se indica por parte del DTIC que no se cuenta con ninguna herramienta para documentar las proyecciones de crecimiento de la plataforma tecnológica, tampoco se proporcionó evidencia sobre el avance en la implementación de la recomendación. Según el Plan de Implementación de Disposiciones Administrativas define las acciones a realizar, el responsable y la fecha de comunicar avances y de implementación con un conjunto de fechas de septiembre 2016 a mayo 2017.</p>
<b>OPORTUNIDAD DE MEJORA 2: NO SE REVISÓ EL CUMPLIMIENTO DE LA POLÍTICA DE SEGURIDAD. RIESGO BAJO.</b>	
RECOMENDACIÓN	<p>Realizar revisiones periódicas (al menos una vez al año o cuando se requiera) de la política de seguridad de la información de la Universidad Nacional, documentando los resultados.</p>
COMENTARIOS ADMINISTRACIÓN	<p>Gestiones para minimizar o eliminar efectos: Revisión del cumplimiento de la política de seguridad.</p> <p>Fecha o plazo de implementación: 30/11/2016</p>
ESTADO	<p><b>PENDIENTE</b></p> <p>Durante el proceso de revisión no fue posible evidenciar que se diera cumplimiento a la política de seguridad, se proporcionó un plan de implementación de las recomendaciones emanadas por la auditoría externa, sin embargo, el informe de avance para la implementación de la recomendación continuaba pendiente para la fecha definida el plan.</p>



**Carta a Gerencia 2014**

**OPORTUNIDAD DE MEJORA 3: INEXISTENCIA DE UN PROCEDIMIENTO FORMAL PARA LA IMPLEMENTACIÓN DE CAMBIOS EN PRODUCCIÓN. RIESGO BAJO.**

**RECOMENDACIÓN**  
Establecer una política o procedimiento relacionado con la implementación de cambios en los sistemas en producción de la Universidad Nacional. Esta política o procedimiento debe ser comunicado al personal para su conocimiento y debido cumplimiento, con el fin de determinar la procedencia y prioridades de los cambios o mejoras, implementando una evaluación técnica para garantizar la calidad y el debido cumplimiento de los requerimientos que previamente fueron solicitados.

**COMENTARIOS DE LA ADMINISTRACIÓN**  
Gestiones para minimizar o eliminar efectos: documentar lo requerido y aprobarlo, así como comunicarlo  
Fecha o plazo de implementación: 30/11/2016

**PENDIENTE**  
Se suministró un documento relacionado con cambios en los sistemas llamado "F-AGSI-006 Gestión de Solicitudes de Cambio de Sistemas de Información" el cual contiene formularios plantillas sobre la atención de solicitudes de cambio en sistemas, además se suministraron ejemplos donde se visualiza que se atienden cambios, sin embargo, no se suministró evidencia sobre la existencia de un procedimiento formal para la implementación de cambios en producción.

**OPORTUNIDAD DE MEJORA 4: NO SE HA ESTABLECIDO LA PROPIEDAD INTELECTUAL DEL SOFTWARE DESARROLLADO INTERNAMENTE. RIESGO BAJO.**

**RECOMENDACIÓN**  
1. Establecer una política o directriz institucional donde se norme la propiedad del código fuente desarrollado por los colaboradores de la DTIC, así como las obligaciones de quién las desarrolla. Dichos lineamientos pueden incluirse dentro del contrato de trabajo, manuales de puestos u otro documento válido que proteja los intereses de la institución.

**COMENTARIOS DE LA ADMINISTRACIÓN**  
Gestiones para minimizar o eliminar efectos: Consultar al ente competente (PDRH, Asesoría Jurídica) de lo que corresponde hacer en este caso.  
Definir la política.  
Fecha o plazo de implementación: 30/11/2016

**CORREGIDO**  
Se determinó la existencia de dos políticas institucionales relacionadas a este tema "POLÍTICAS PARA LA PROTECCIÓN Y FOMENTO DE LA PROPIEDAD INTELECTUAL GENERADA EN LA UNIVERSIDAD NACIONAL" y "CREACIÓN DE UNA POLÍTICA INSTITUCIONAL PARA EL USO DEL SOFTWARE

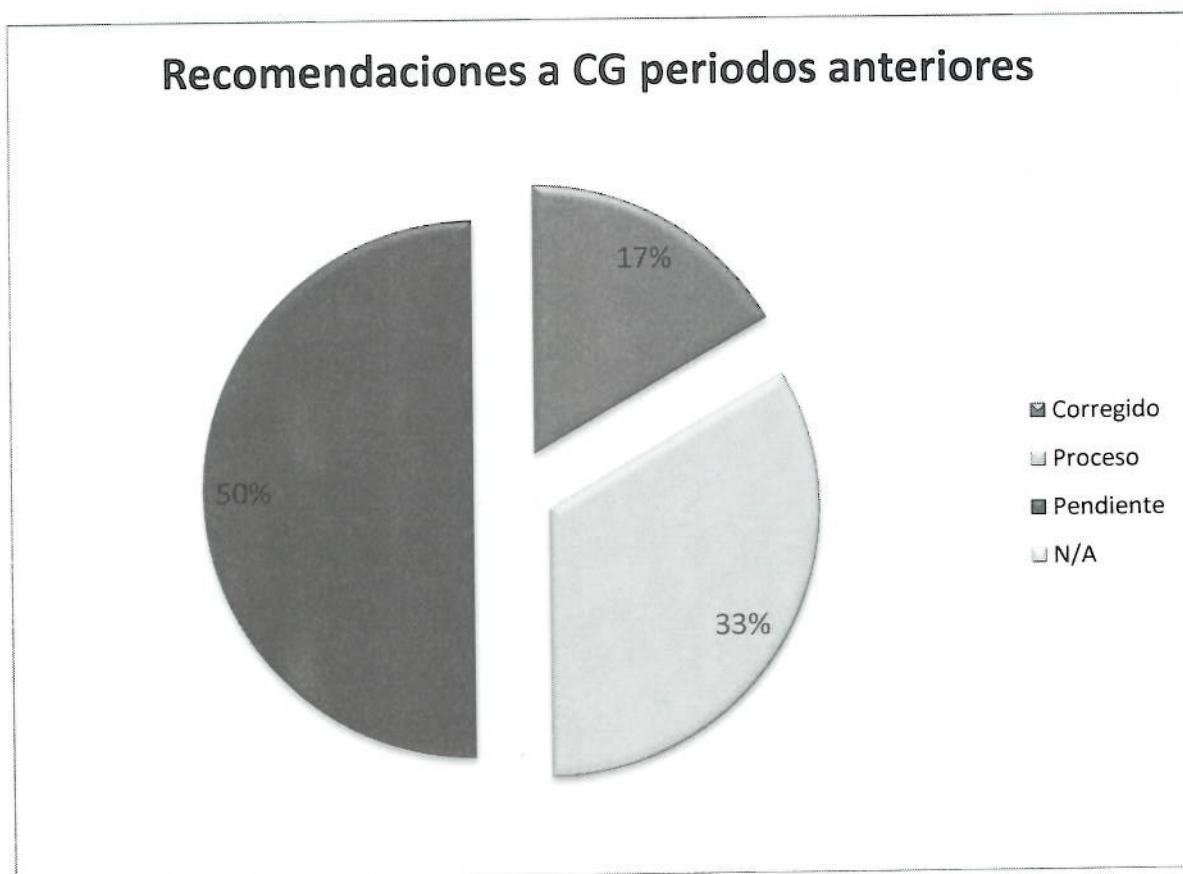
### Carta a Gerencia 2014

LIBRE EN LA UNIVERSIDAD NACIONAL”. Si bien, en estas políticas no se define tan específico el tema de código fuente, si son relacionadas a propiedad intelectual y al quehacer académico, además hacen alusión a cualquier tipo de conocimiento; estableciendo que el conocimiento generado en la academia le pertenece a la institución.

Uno de los párrafos indicados en la primera política es “III. Protege las creaciones intelectuales derivadas del quehacer del personal universitario, producto de su vinculación laboral con la institución y cualquiera que sea la naturaleza de esta”.

A continuación se resume el cumplimiento de las recomendaciones emitidas en el informe de auditoría del periodo anterior:

Estado	Total año 2014
Corregidas	2
Proceso	4
Pendientes	6
N/a	0
<b>Total</b>	<b>12</b>



**ANEXO I**

**Análisis de Riesgos T.I.  
Dirección de Tecnologías de Información y Comunicación  
Periodo 2015**

Tipos de Riesgo	
ALTO	<b>A</b>
MEDIO	<b>M</b>
BAJO	<b>B</b>

**Alto**

Requiere una atención inmediata por su impacto en seguridad, integridad, efectividad, eficiencia, confidencialidad, confiabilidad, disponibilidad y continuidad de la plataforma tecnológica. No se han establecido controles en este nivel de riesgo.

**Medio**

Requiere una atención intermedia ya que su impacto representaría riesgos sobre seguridad, integridad, efectividad, eficiencia, confidencialidad, confiabilidad, disponibilidad y continuidad de la plataforma tecnológica. Se han establecido controles insuficientes en este nivel de riesgo.

**Bajo**

Requiere una atención no prioritaria ya que su impacto no es directamente sobre seguridad, integridad, efectividad, eficiencia, confidencialidad, confiabilidad, disponibilidad y continuidad de la plataforma tecnológica. Se han establecido controles adecuados en este nivel de riesgo.

**A. SEGURIDAD FÍSICA**

Centro de Cómputo	Condición	Vulnerabilidad		Comentarios	Observaciones	Tipo de riesgo
		SÍ	NO			
A.1	Proceso de autorización de ingreso		✓	Todos los accesos al edificio y al centro de datos deben ser autorizados		B
A.2	Personal interno y externo debidamente identificado (gafete)		✓	El personal interno y externo está debidamente identificado		B
A.3	Revisión de equipos de ingreso y salida		✓	Se cumple con esta condición		B
A.4	Bitácoras de acceso al edificio y centro de cómputo		✓	Existen bitácoras electrónicas y físicas		B
A.5	Acceso restringido a personal de informática definido		✓	El acceso es restringido, solo se permite personal autorizado		B
A.6	Una sola vía de acceso		✓	Solo existe una vía de acceso al centro de datos.		B
A.7	Externos son acompañados por internos		✓	Se cumple con esta condición.		B
A.8	Puerta de acceso segura		✓	Se cumple con esta condición.		B
A.9	Acceso con tarjeta electrónica al centro de datos		✓	Se cumple con esta condición.		B
A.10	Alarmas de detección de intrusos		✓	Se cumple con esta condición.		B
A.11	Monitoreo de la entrada por cámara de seguridad		✓	Se cumple con esta condición.		B
A.12	Ubicación en un sitio seguro (lugares colindantes)		✓	Se cumple con esta condición.		B
A.13	Lugar completamente cerrado		✓	Se cumple con esta condición.		B
A.14	Paredes de concreto	X		Existe una pared de paneles de madera		B
A.15	Cielo raso sellado		✓	Se cumple con esta condición.		B
A.16	Equipos ubicados en rack		✓	Se cumple con esta condición.		B

Centro de Cómputo	Condición	Vulnerabilidad		Comentarios	Observaciones	Tipo de riesgo
		SÍ	NO			
A.17	Los racks están asegurados		✓	Se cumple con esta condición.		B
A.18	Cableado de datos independiente del eléctrico		✓	Se cumple con esta condición.		B
A.19	Cableado entubado y canaletado		✓	Se cumple con esta condición.		B
A.20	Cableado debidamente rotulado		✓	Se cumple con esta condición.		B
A.21	Hay un sitio alternativo		✓	Existe un sitio alternativo en otro edificio en el campus de la UNA		B

Fin del documento.