UNIVERSIDAD NACIONAL (UNA)

- *Carta de Gerencia Cg 1-2014*
- *Informe final*

Heredia, 23 de octubre del 2015.

Señores
Universidad Nacional (UNA)

Estimados señores:

Según nuestro contrato de servicios, efectuamos la auditoría externa correspondiente al período 2014, 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 CG1-2014.

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 2014.
- Solicitamos los informes de auditoría interna con fecha de corte al 31 de diciembre del 2014.
- Solicitamos y revisamos los libros legales de la Universidad Nacional al 31 de diciembre del 2014.
- Solicitamos la correspondencia enviada y recibida por la Contraloría General de la República al 31 de diciembre del 2014.
- 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.

Resultado de la revisión:

Como resultado de la evaluación del control interno de la Universidad Nacional (UNA), se determina que existen 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 HITÓRICOS.

CONDICIÓN:

Al realizar la auditoría de los estados financieros de la Universidad Nacional al 31 de diciembre del 2014, determinamos que no se guardan reportes físicos históricos de los saldos como por ejemplo:

- Reportes o conciliaciones de las cuentas por cobrar matricula.
- 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 específico, 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, MANUALES Y PROCEDIMIENTOS.

CONDICIÓN:

Al realizar la revisión de las políticas, manuales y procedimientos de la Universidad Nacional al 31 de diciembre del 2014, determinamos que para las cuentas de inversiones y cuentas por cobrar se carece de los mismos, 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 administración y el Consejo Universitario deben gestionar la realización de políticas, manuales y procedimientos, para que los actos de la gestión institucional queden respaldados, además para que se establezcan los tratamientos contables necesarios para el correcto registro y documentación de las mismas.

b) Caja y bancos

- Realizamos cédulas sumarias comparativas y revisamos lo movimientos importantes de la cuenta.

- Revisamos las conciliaciones bancarias de las diferentes cuentas corrientes que posee la Universidad, al 31 de diciembre del 2014.

- 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.

- Realizamos un arqueo de los cheques en blanco y los cheques en cartera que mantiene la Universidad.

- Solicitamos confirmaciones bancarias para las cuentas utilizadas durante el periodo de la auditoria.

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 2014, y revisamos variaciones importantes de la cuentas.
- Cotejamos el registro auxiliar con el mayor general, al 31 de diciembre del 2014.
- Realizamos el recálculo de los intereses por cobrar de los títulos al 31 de diciembre del 2014.
- Solicitamos los estados de cuenta de las inversiones al 31 de diciembre del 2014.
- 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, se detectaron debilidades de control que deban informarse en esta carta de gerencia. Ver hallazgo 2 y 11.

d) Cuentas por cobrar

- Realizamos cédulas sumarias comparativas al 31 de diciembre del 2014, y revisamos variaciones importantes de la cuentas.
- Cotejamos el detalle de las cuentas con el mayor contable al 31 de diciembre del 2014.
- Realizamos el cálculo de las razones financieras y las comparamos con el cierre del año anterior, con el fin de revisar el movimiento de la misma.

Resultado de la revisión:

Mediante lo resultados de las pruebas realizadas a la UNA, se determina la existencia de una serie de situaciones que representan un nivel de riesgo medio, las cuales se mencionan a continuación:

HALLAZGO 3: CARENCIA DE POLÍTICAS DE ESTIMACIÓN PARA INCOBRABLES.

CONDICIÓN:

Efectuamos la revisión de las cuentas por cobrar al 31 de diciembre del 2014 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. Por lo que el establecer y registrar una estimación por incobrables es necesaria para la universidad y revelar un saldo depurado de las cuentas por cobrar recuperables.

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 MATRICULA 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 cuya fecha de corte es a mayo 2015, la cual se detalla a continuación:

Antigüedad en días	Saldo	Porcentaje
De 0 a 180	¢24.572.264	4%
De 180 a 360	45.031.664	7%
Más de 360	533.493.356	80%
Créditos 2015	61.261.484	9%
Total	**¢664.358.768**	**100%**

Lo cual nos genera evidencia que al 31 de diciembre del 2014 existen cuentas por cobrar de esta naturaleza cuya antigüedad supera los 180 días.

CRITERIO:

Un adecuado control interno estable lo siguiente: se analizará 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) Gastos pagados por anticipado

- Realizamos cédulas sumarias comparativas al 31 de diciembre del 2014, y revisamos variaciones importantes de la cuentas.

- Realizamos un recálculo de las primas y los descuentos producto de las inversiones al 31 de diciembre del 2014.

- Realizamos una revisión de las pólizas vigentes al 31 de diciembre del 2014.

Resultado de la revisión:

Con base en las pruebas de auditoría realizadas determinamos que el saldo de la cuenta se presenta de manera razonable, por lo que no existen situaciones a ser informadas.

f) Activo propiedad, mobiliario y equipo

- Realizamos cédulas sumarias comparativas al 31 de diciembre del 2014 y revisamos variaciones importantes de las cuentas.

- Realizamos un estudio de registro de los terrenos y los vehículos ante el Registro Nacional de la Propiedad, con el fin de revisar si los mismos se encuentran a nombre de la Universidad.

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.

CONDICIÓN:

Efectuamos nuestras pruebas de auditoría a las partidas de inmueble, maquinaria y equipo al 31 de diciembre del 2014 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 importante que asciende a la suma de ¢539.771 (en miles) la cual se origina debido a que la entrada del activo en el auxiliar no coincide con la fecha de registro contable, ajustes y eliminación de etiquetas, que dan lugar a diferencias del saldo contable con el auxiliar. El detalle se muestra a continuación:

Tipo	Cuenta Contable	Detalle	Saldo según auxiliar	Saldo según Contabilidad	Diferencia
TIPO 01	AO01	Maquinaría y equipo de producción	666.835	638.944	2.109
TIPO 02	AO02	Equipo de Transporte	2.473.070	2.650.679	177.609
TIPO 03	AO03	Equipo de comunicación	3.115.537	3.115.630	93
TIPO 04	AO04	Equipo y mobiliario de oficina	3.200.397	3.201.331	934
TIPO 05	AO05	Equipo y programa de computo	6.649.101	6.413.111	(235.990)
TIPO 06	AO06	Equipo sanit, laborat e investig	6.746.970	6.779.011	32.041
TIPO 07	AO07	Eq y mob educ, depo, y recreat	206.275	279.732	73.457
TIPO 08	AO08	Maquinaria y equipo diverso	1.985.713	1.987.245	1.532
TIPO 09	AO11	Terrenos	2.728.643	2.728.876	(111)
TIPO 10	AO10	Edificios	11.898.863	12.369.876	471.013
TIPO 14	AO17	Otros bienes duraderos	---	17.085	17.085
	Total		**39.641.405**	**40.181.176**	**539.771**

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 2014 y se presenta una diferencia material por un monto de ¢1.439.265(en miles) con respecto al saldo contable.

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.

Saldo Auxiliar	Saldo Recalculo	Diferencia
15.014.590	16.453.855	1.439.265

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.

HALLAZGO 6: DEBILIDADES DE CONTROL INTERNO DETECTADAS EN LA TOMA FISICA DE PROPIEDAD PLANTA Y EQUIPO

CONDICION

Efectuamos una toma física de activos, de una muestra seleccionada al azar y detectamos las siguientes debilidades de control interno:

a) Activos dañados y deteriorados en la espera para darse de baja.

Placa	Descripción	Costo
N00121237	Pila para elaborar pulpas	1.218.000
N00120279	Máquina fotocomponedora	21.910.034

b) Activos que no son utilizados

Placa	Descripción	Costo
N00138281	Cámara fotográfica	2.289.883
N00138148	Central telefónica	3.907.163
N00121371	Prensa grabado	2.700.000
N00116674	Máquina para fabricar alfombras	4.567.544

c) Activos no plaqueados

Placa	Descripción	Costo
N00138281	Cámara fotográfica	2.289.883
N00138148	Central telefónica	3.907.163
N00138111	Proyector de multimedia	1.409.720
N00138040	Televisor	1.200.000
N00121371	Prensa grabado	2.700.000

d) Activos identificados con número de placa diferente a la del auxiliar

Placa	Descripción	Costo
N00131349	Equipo para medición de luz	1.662.657
N00116674	Máquina para fabricar alfombras	4.567.544

e) Custodios desconocen cuales activos se encuentra bajo su responsabilidad.

CRITERIO

Un adecuado control interno establece que se debe controlar el retiro, traspasos y mejoras de los activos, para de esta manera efectuar un uso eficiente de los recursos de la universidad.
Del mismo modo la custodia del activo debe establecerse de manera clara, donde las personas responsables queden obligadas a reportar cualquier cambio en cuanto a pérdida, venta, traspaso, bajas, obsolescencia y traslados tanto de custodio, como dentro y fuera de las instalaciones autorizadas del activo.
Los activos deben ser correctamente plaqueados para de este modo evitar confusiones que incidan en errores o represente un riesgo de pérdida.

RECOMENDACIÓN

Se recomienda realizar una actualización de los custodios de los diferentes activos, realizar tomas físicas periódicas con el objetivo de subsanar debilidades de control interno detectadas. Y de esta manera verifica el uso adecuado de los recursos de la universidad

g) Documentos por pagar

- Realizamos cédulas sumarias comparativas al 31 de diciembre del 2014 y revisamos variaciones importantes de la cuentas.
- Realizamos una conciliación de saldos al 31 de diciembre del 2014.
- Solicitamos las tablas de pago de la deuda al 31 de diciembre del 2014.
- Revisamos el gasto por intereses de la cuenta al 31 de diciembre del 2014.
- Realizamos el pago posterior del saldo adeudado al 31 de diciembre del 2014.
- Solicitamos confirmaciones de saldos a los diferentes entes bancarios al 31 de diciembre del 2014.

Resultado de la revisión:

Conforme las verificaciones efectuadas se considera que esta cuenta presenta un nivel de riesgo bajo y que en los saldos mostrados en los estados financieros se presentan razonable, por lo que no se detectaron desviaciones que deban ser informadas en esta carta de gerencia.

h) Cuentas por pagar

- Realizamos cédulas sumarias comparativas al 31 de diciembre del 2014 y revisamos variaciones importantes de la cuenta.
- Realizamos un memorándum explicativo de la cuenta.
- Revisamos los pagos posteriores de las deducciones y los gastos acumulados al 31 de diciembre del 2014.

Resultado de la revisión:

Los resultados de las pruebas realizadas indican que las cuentas por pagar de la Universidad se presentan en forma razonable, ya que no existen situaciones que deba ser informada para este periodo.

i) Patrimonio

- Realizamos cédulas sumarias comparativas al 31 de diciembre del 2014 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.
- Revisamos mediante cédulas analíticas los principales movimientos de la cuenta al 31 de diciembre del 2014.

Resultado de la revisión:

Los resultados de las pruebas realizadas indican que las cuentas de patrimonio de la Universidad Nacional (UNA), se presenta en forma razonable al 31 de diciembre de 2014.

j) Ingresos y Gastos

- Realizamos cédulas sumarias comparativas al 31 de diciembre del 2014 revisamos variaciones importantes de la cuenta.

- Solicitamos el movimiento de las principales cuentas de ingresos y gastos al 31 de diciembre del 2014.

- Verificamos una muestra de movimientos relevantes de ingresos y gastos del periodo 2014.

- Realizamos una prueba de planilla, 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 (Liberia).
- Sede Regional Brunca.

De acuerdo al programa de trabajo se efectuó la siguiente:

- Solicitamos los últimos arqueos de caja realizados a las Sedes Regionales.

- Realizamos una toma física de los activos (bienes) mantenidos en las Sedes Regionales.

Resultado de la revisión:

Con base en las pruebas de auditoría realizadas determinamos que la existen situaciones que se deben informar en la carta de gerencia y que corresponde a un nivel de riesgo medio y las cuales se detallan de la siguiente manera:

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

CONDICIÓN:

Efectuamos la revisión de los activos fijos de la Sede Chorotega, campus Liberia y determinamos las siguientes debilidades de control interno:

- Determinamos que el custodio de algunos activos fijos se encuentra desactualizados

Etiqueta permanente	Descripción	Valor en libros	Fecha adquisición	Nombre	Cédula
N00128993	Microbús	12.135.159	05/11/11	Esteban Araya Salazar	111130688
N00118169	Automóvil	12.135.159	28/10/08	Esteban Araya Salazar	111130688
N00134874	Paneleria en melamina	12.135.159	01/10/13	Esteban Araya Salazar	111130688
N00134735	Estación de recepción	12.135.159	01/10/13	Esteban Araya Salazar	111130688
106905	Automóvil	12.135.159	14/06/07	Esteban Araya Salazar	111130688
N00113629	Automóvil	12.135.159	04/02/08	Orlando De La O Castañeda	502460011
N00113841	Automóvil	12.135.159	04/02/08	Orlando De La O Castañeda	502460011
N00125192	Aire acondicionado	12.135.159	23/11/09	Esteban Araya Salazar	111130688

- Activos que no se pudieron identificar, algunos ejemplos de los mismos se detallan de la siguiente manera:

Etiqueta permanente	Descripción	Valor en libros	Fecha adquisición	Nombre	Cédula
N00134874	Paneleria en melamina	4.659.450	01/10/13	Esteban Araya Salazar	111130688
N00134735	Estación de recepción	3.515.291	01/10/13	Esteban Araya Salazar	111130688

- En el momento en que un funcionario deja de ejerce sus labores por distintas razones no se le realiza una entrega formal de los activos a su cuidado, para de este modo determinar algún daño o pérdida, y bien para que pasen a ser controlados por el funcionario que corresponde.

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 Liberia, efectuar la revisión de activos no plaqueados e identificarlos. Además solicitar de manera obligatoria el inventario de activos fijos bajo custodia de los funcionarios que por razones independientes dejan de laborar para la universidad.

HALLAZGO 8: DEBILIDADES DE CONTROL INTERNO ENCONTRADAS EN LA SEDE DE PÉREZ ZELEDÓN.

CONDICIÓN:

Al realiza la revisión de la partida de propiedad, planta y equipo en la Sede Regional de Liberia determinamos algunas situaciones referentes a debilidades de control interno, las cuales se presentan a continuación:

- No se maneja un control de la ubicación de los activos.
- En cuanto al detalle del registro auxiliar, existen activos no presentan información importante como marca, modelo y serie.

CRITERIO:

Las Normas contables y de control interno establecen la importancia de identificar, controlar y monitorear los registros auxiliares de los registros de activo fijo permanentemente según su naturaleza.

RECOMENDACIÓN:

Revisar y asegurar las medidas de control interno para los activos de la entidad, además de mantener depurado el registro auxiliar.

RESULTADOS ENCONTRADOS DE LA EVALUACIÓN AL DEPARTAMENTO DE TECNOLOGÍAS DE INFORMACIÓN

HALLAZGOS Y RECOMENDACIONES
UNIVERSIDAD NACIONAL

HALLAZGO 9: NO SE REALIZAN EVALUACIONES SOBRE EL DESEMPEÑO A LOS COLABORADORES DE T.I. RIESGO BAJO.

CONDICIÓN:

Producto de la revisión efectuada, se corroboró la inexistencia de evaluaciones sobre el desempeño de los colaboradores de la Dirección de Tecnologías de la Información y Comunicación, según se nos informó, esta tarea la tiene asignada el departamento de recursos humanos, sin embargo, no se suministró evidencia al respecto.

Lo anterior puede provocar que no se logre hacer una estimación cuantitativa y cualitativa, por parte de los jefes inmediatos, del grado de eficacia con que los trabajadores llevan a cabo las actividades, objetivos y responsabilidades en sus puestos de trabajos.

CRITERIO:

El apartado 2.4 Independencia y recurso humano de la Función 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 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:

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:
    - La evaluación del desempeño debe estar unida al desarrollo de las personas en la organización o área de trabajo.
    - Los estándares de la evaluación del desempeño deben estar fundamentadas en información relevante del puesto de trabajo.
    - Deben definirse claramente los objetivos del sistema de evaluación del desempeño.
    - El sistema de evaluación del desempeño requiere el compromiso y participación activa de todos los trabajadores.

- El papel de juez del supervisor-evaluador debe considerarse la base para aconsejar mejoras.

HALLAZGO 10: NO IMPLEMENTACIÓN DE TODOS LOS PLANES DE CONTINGENCIA DEFINIDOS. RIESGO MEDIO.

CONDICIÓN:

Durante el proceso de auditoría se determinó que la Universidad Nacional posee planes de contingencia y continuidad para firewall, enrutadores, telefonía-IP, equipo CORE, así como planes de contingencia para el sistema BANNER y NX, sin embargo, en el 2014 solo se probaron los planes para enrutadores y firewall, a los demás planes no se les han realizado las pruebas correspondientes.

El no implementar planes de contingencia puede conllevar a la materialización de los siguientes riesgos: imposibilidad de recuperar los sistemas de T.I., y servicios de manera oportuna, falta de alternativas de decisión relacionadas a procesos, ausencia de recursos de recuperación necesarios y poca comunicación a lo interno y externo de las partes involucradas. Además al no existir planes de recuperación de desastres y de contingencias, puede provocar que no se obtengan correctamente los datos que han sido respaldados por la organización ante la ocurrencia de una eventualidad.

CRITERIO:

Según el criterio 1.4.7 Continuidad de los servicios de TI, sobre las Normas Técnicas para la Gestión y Control de las Tecnologías de Información emitidas por la Contraloría General de la Republica, menciona lo siguiente: "La organización debe mantener una continuidad razonable de sus procesos y su interrupción no debe afectar significativamente a sus usuarios. Como parte de ese esfuerzo debe documentar y poner en práctica, en forma efectiva y oportuna, las acciones preventivas y correctivas necesarias con base en los planes de mediano y largo plazo de la organización, la evaluación e impacto de los riesgos y la clasificación de sus recursos de TI según su criticidad".

RECOMENDACIONES:

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.

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).

3. Documentar los resultados de las pruebas realizadas, determinando los ajustes que sean necesarios e indicando lo funcional o no del plan.

HALLAZGO 11: DEBILIDADES EN EL SISTEMA INTEGRADO DE INVERSIONES (SICOI). RIESGO MEDIO.

CONDICIÓN:

Durante el proceso de auditoría se determinó que el sistema integrado de inversiones no genera un registro auxiliar, el mismo se lleva a cabo por medio de una hoja de Excel. El sistema únicamente se encarga de generar el asiento contable.

Lo anterior puede llevar a la materialización de los siguientes riesgos: generación de un registro auxiliar poco confiable, ya que no se puede validar que la información suministrada sea la correcta.

CRITERIO:

Según el criterio 3.2 Implementación de software, sobre las Normas Técnicas para la Gestión y Control de las Tecnologías de Información emitidas por la Contraloría General de la República, menciona lo siguiente: "La organización debe implementar el software que satisfaga los requerimientos de sus usuarios y soporte efectivamente sus procesos, para lo cual debe:

a. Observar lo que resulte aplicable de la norma 3.1anterior.
b. Desarrollar y aplicar un marco metodológico que guíe los procesos de implementación y considere la definición de requerimientos, los estudios de factibilidad, la elaboración de diseños, la programación y pruebas, el desarrollo de la documentación, la conversión de datos y la puesta en producción, así como también la evaluación postimplantación de la satisfacción de los requerimientos.
c. Establecer los controles y asignar las funciones, responsabilidades y permisos de acceso al personal a cargo de las labores de implementación y mantenimiento de software.
d. Controlar la implementación del software en el ambiente de producción y garantizar la integridad de datos y programas en los procesos de conversión y migración.
e. Definir los criterios para determinar la procedencia de cambios y accesos de emergencia al software y datos, y los procedimientos de autorización, registro, supervisión y evaluación técnica, operativa y administrativa de los resultados de esos cambios y accesos.
f. Controlar las distintas versiones de los programas que se generen como parte de su mantenimiento".

RECOMENDACIONES:

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:

- Número de operación.
- Puesto de bolsa.
- Rendimiento.
- Serie.
- Emisión.
- Instrumento.
- Tasa facial.
- Monto facial.
- Costo.
- Interés comprado.
- Tipo de vector.
- Fecha de compra.
- Fecha de vencimiento.
- Fechad de último pago.
- Fecha de próximo pago.
- Interés acumulado.
- Valor de libros.
- Precio de mercado.
- Valor de mercado.

HALLAZGO 12: EL SISTEMA BANNER NO GENERA UN REPORTE DE ANTIGÜEDAD DE SALDOS DE CUENTAS POR COBRAR Y CUENTAS POR PAGAR. RIESGO MEDIO.

CONDICIÓN:

El sistema BANNER utilizado por la Universidad Nacional no genera un reporte de antigüedad de saldos de cuentas por cobrar y cuentas por pagar.
Lo anterior puede llevar a la materialización de los siguientes riesgos: se podría no tener un detalle exacto de la mora que poseen los registros de cuentas por cobrar y cuentas por pagar, además no se lleva un control de las cuentas que están clasificadas como irrecuperables.

CRITERIO:

Según el criterio *3.2* Implementación de software, sobre las Normas Técnicas para la Gestión y Control de las Tecnologías de Información emitidas por la Contraloría General de la República, menciona lo siguiente: "La organización debe implementar el software que satisfaga los requerimientos de sus usuarios y soporte efectivamente sus procesos, para lo cual debe:

a. Observar lo que resulte aplicable de la norma 3.1anterior.
b. Desarrollar y aplicar un marco metodológico que guíe los procesos de implementación y considere la definición de requerimientos, los estudios de factibilidad, la elaboración de diseños, la programación y pruebas, el desarrollo de la documentación, la conversión de datos y la puesta en producción, así como también la evaluación postimplantación de la satisfacción de los requerimientos.
c. Establecer los controles y asignar las funciones, responsabilidades y permisos de acceso al personal a cargo de las labores de implementación y mantenimiento de software.
d. Controlar la implementación del software en el ambiente de producción y garantizar la integridad de datos y programas en los procesos de conversión y migración.
e. Definir los criterios para determinar la procedencia de cambios y accesos de emergencia al software y datos, y los procedimientos de autorización, registro, supervisión y evaluación técnica, operativa y administrativa de los resultados de esos cambios y accesos.
f. Controlar las distintas versiones de los programas que se generen como parte de su mantenimiento".

RECOMENDACIÓN:

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.

2. Para la actividad anterior se debe de generar los requerimientos necesarios por parte de las áreas usuarias para su presentación a la DTIC.

COMENTARIOS ADMINISTRACIÓN:

Se aclara que se solicitó en el oficio PGF-SC-622-2010, de octubre 2010 y nuevamente se retoma en el oficio PGF-D-758--2014, agosto 2014.

HALLAZGO 13: EL SISTEMA BANNER NO GENERA UN REPORTE DEL VALOR HISTÓRICO DE LOS ACTIVOS. RIESGO MEDIO.

CONDICIÓN:

El sistema BANNER utilizado por la Universidad Nacional no genera un reporte del valor histórico de los activos. Para la generación de dicho reporte se deben establecer las fechas de inicio y final en los campos "De la fecha y A la fecha", sin embargo, el campo "A la fecha" permite digitar una fecha antigua determinada, no realizando la validación el sistema, lo que hace es tomar la fecha actual, imposibilitando la generación de reportes de meses o años anteriores.

Lo anterior puede provocar que no se tenga conocimiento del valor histórico de los activos y su respectiva depreciación.

CRITERIO:

Según el criterio 3.2 Implementación de software, sobre las Normas Técnicas para la Gestión y Control de las Tecnologías de Información emitidas por la Contraloría General de la República, menciona lo siguiente: "La organización debe implementar el software que satisfaga los requerimientos de sus usuarios y soporte efectivamente sus procesos, para lo cual debe:

a. Observar lo que resulte aplicable de la norma 3.1anterior.
b. Desarrollar y aplicar un marco metodológico que guíe los procesos de implementación y considere la definición de requerimientos, los estudios de factibilidad, la elaboración de diseños, la programación y pruebas, el desarrollo de la documentación, la conversión de datos y la puesta en producción, así como también la evaluación postimplantación de la satisfacción de los requerimientos.
c. Establecer los controles y asignar las funciones, responsabilidades y permisos de acceso al personal a cargo de las labores de implementación y mantenimiento de software.
d. Controlar la implementación del software en el ambiente de producción y garantizar la integridad de datos y programas en los procesos de conversión y migración.
e. Definir los criterios para determinar la procedencia de cambios y accesos de emergencia al software y datos, y los procedimientos de autorización, registro, supervisión y evaluación técnica, operativa y administrativa de los resultados de esos cambios y accesos.
f. Controlar las distintas versiones de los programas que se generen como parte de su mantenimiento".

RECOMENDACIÓN:

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.

HALLAZGO 14: NO SE DOCUMENTAN LAS REVISIONES NI PRUEBAS DE CADA ETAPA DEL CICLO DE DESARROLLO DE SOFTWARE. RIESGO MEDIO.

CONDICIÓN:

Producto de la revisión efectuada, se corroboró que no se documentan las revisiones ni pruebas de cada etapa del ciclo de desarrollo de software, sin embargo, estas si se están llevando a cabo.

Lo anterior podría llevar a la materialización de los siguientes riesgos: no se realizan las validaciones necesarias para asegurar el correcto funcionamiento de los sistemas, y por lo tanto, no se establecen planes de acción y controles que permitan mitigar los efectos de posibles errores en el funcionamiento de nuevas implementaciones.

CRITERIO:

Según el criterio 3.2 Implementación de software, sobre las Normas Técnicas para la Gestión y Control de las Tecnologías de Información emitidas por la Contraloría General de la República, menciona lo siguiente: "La organización debe implementar el software que satisfaga los requerimientos de sus usuarios y soporte efectivamente sus procesos, para lo cual debe:

a. Observar lo que resulte aplicable de la norma 3.1anterior.
b. Desarrollar y aplicar un marco metodológico que guíe los procesos de implementación y considere la definición de requerimientos, los estudios de factibilidad, la elaboración de diseños, la programación y pruebas, el desarrollo de la documentación, la conversión de datos y la puesta en producción, así como también la evaluación postimplantación de la satisfacción de los requerimientos.
c. Establecer los controles y asignar las funciones, responsabilidades y permisos de acceso al personal a cargo de las labores de implementación y mantenimiento de software.
d. Controlar la implementación del software en el ambiente de producción y garantizar la integridad de datos y programas en los procesos de conversión y migración.
e. Definir los criterios para determinar la procedencia de cambios y accesos de emergencia al software y datos, y los procedimientos de autorización, registro, supervisión y evaluación técnica, operativa y administrativa de los resultados de esos cambios y accesos.
f. Controlar las distintas versiones de los programas que se generen como parte de su mantenimiento".

RECOMENDACIONES:

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.

2. Establecer un plan de pruebas posterior a la implementación para garantizar la aceptación por parte de las áreas usuarias.

3. Documentar las revisiones y pruebas de cada etapa del ciclo de desarrollo de software.

4. Es deseable que el Centro de Gestión Informática (CGI) lleve a cabo la aprobación formal de la metodología de desarrollo de sistemas.

HALLAZGO 15: NO SE HA APROBADO FORMALMENTE LA POLÍTICA DE RESPALDOS DE LA INFORMACIÓN. RIESGO BAJO.

CONDICIÓN:

Producto de la revisión efectuada a los lineamientos de respaldos de la información, se corroboró la existencia de dichos lineamientos, sin embargo, estos lineamientos no están aprobados formalmente. Cabe mencionar que estos lineamientos están en proceso de aprobación por parte de la Dirección de Tecnologías de Información y Comunicación (DTIC).

Al no estar aprobada formalmente una política de respaldos de la información, no se garantiza que los procesos de restauración utilizados cuenten con un estándar adecuado.

CRITERIO:

Según el criterio 3 4.2 Administración y operación de la plataforma tecnológica, sobre las Normas Técnicas para la Gestión y Control de las Tecnologías de Información emitidas por la Contraloría General de la República, menciona lo siguiente: "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:

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.
2. Enviar a todos los funcionarios involucrados, por correo electrónico o algún otro medio válido, el comunicado oficial de la política o procedimiento aprobada.

3. Verificar el cumplimiento de la política o procedimiento periódicamente.

HALLAZGO 16: DEFICIENCIAS EN LA SEGURIDAD LÓGICA DE ALGUNOS SISTEMAS DE LA UNIVERSIDAD NACIONAL. RIESGO MEDIO.

CONDICIÓN:

Producto de la revisión efectuada, se determinó que los sistemas LDAP y NX no poseen controles de seguridad lógica adecuados.

Los controles no implementados son los siguientes:

1. La clave del sistema LDAP expira una vez al año.
2. El sistema NX no posee un mecanismo automático para el cambio de contraseña.
3. Los sistemas LDAP y NX no guardan un registro histórico de las claves.
4. El sistema LDAP utiliza claves no alfanuméricas.

Lo citado anteriormente puede conllevar a la materialización de los siguientes riesgos: vulnerabilidad de la información y suplantación de identidad.

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.
i. Establecer controles de acceso a la información impresa, visible en pantallas o almacenada en medios físicos y proteger adecuadamente dichos medios.
j. Establecer los mecanismos necesarios (pistas de auditoría) que permitan un adecuado y periódico seguimiento al acceso a las T.I.
k. Manejar de manera restringida y controlada la información sobre la seguridad de las TI".

RECOMENDACIONES:

1. Tomar las acciones necesarias para asegurar que los sistemas implantados en la Universidad Nacional cuenten con una seguridad lógica adecuada.
2. Las medidas de seguridad lógica deben verse reflejadas en una política de seguridad.
3. Realizar revisiones periódicas formales a la seguridad lógica implementada.

OPORTUNIDADES DE MEJORA

OPORTUNIDAD DE MEJORA 01: NO SE DOCUMENTAN PROYECCIONES CON BASE EN LAS CAPACIDADES DE LA PLATAFORMA TECNOLÓGICA ACTUAL DE LA UNIVERSIDAD NACIONAL. RIESGO BAJO.

CONDICIÓN:

Producto de la revisión efectuada, se determina que la Universidad Nacional lleva a cabo un proceso de monitoreo sobre algunos servicios de tecnologías de información y su rendimiento, como por ejemplo, el monitoreo de tráfico en el equipo CORE de la Universidad, así como al servidor de Oracle.

Sin embargo, como parte de la planificación referente la capacidad y desempeño de la plataforma tecnológica, no se considera formalmente la realización de proyecciones, contemplando estrategias, planes del negocio y aumento de las transacciones actuales que pudiesen requerir la implementación de nuevos servicios de tecnologías de información, permitiendo así identificar mejoras de la plataforma actual.

Al no realizarse proyecciones de las capacidades en la plataforma tecnológica, se dificulta la definición de medidas preventivas para disminuir posibles fallos y la atención oportuna de requerimientos del negocio.

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:

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.

OPORTUNIDAD DE MEJORA 02: NO SE REVISA EL CUMPLIMIENTO DE LA POLÍTICA DE SEGURIDAD. RIESGO BAJO.

CONDICIÓN:

Producto de la revisión efectuada, se corroboró que si bien se revisa la configuración de la seguridad de la plataforma tecnológica de forma periódica por parte de la DTIC, no se revisa el cumplimiento de la política de seguridad como tal. Al no efectuarse revisiones periódicas no se garantiza de manera razonable, la confidencialidad, integridad y disponibilidad de la información.

CRITERIO:

El apartado 1.4 Gestión de la seguridad de la información, 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 garantizar, de manera razonable, la confidencialidad, integridad y disponibilidad de la información, lo que implica protegerla contra uso, divulgación o modificación no autorizados, daño o pérdida u otros factores disfuncionales.
Para ello debe documentar e implementar una política de seguridad de la información y los procedimientos correspondientes, asignar los recursos necesarios para lograr los niveles de seguridad requeridos y considerar lo que establece la presente normativa en relación con los siguientes aspectos:
- La implementación de un marco de seguridad de la información.
- El compromiso del personal con la seguridad de la información.
- La seguridad física y ambiental.
- La seguridad en las operaciones y comunicaciones.
- El control de acceso.
- La seguridad en la implementación y mantenimiento de software e infraestructura tecnológica.
- La continuidad de los servicios de TI.
Además debe establecer las medidas de seguridad relacionadas con:
- El acceso a la información por parte de terceros y la contratación de servicios prestados por éstos.
- El manejo de la documentación.
- La terminación normal de contratos, su rescisión o resolución.
- La salud y seguridad del personal.
Las medidas o mecanismos de protección que se establezcan deben mantener una proporción razonable entre su costo y los riesgos asociados".

RECOMENDACIONES:

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.

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

CONDICIÓN:

Producto de la revisión efectuada, se corrobora que no existe un procedimiento o una política que indique como pasar a producción los cambios realizados por los desarrolladores de la DTIC. En la práctica los cambios a producción se realizan con el sistema iTop, mediante los servicios (SubCategoría) de ejecución de scripts y extraer, compilar reportes y formas, sin embargo no bajo un procedimiento estándar y formal.

Lo anterior puede provocar que no se registren, evalúen y autoricen los cambios adecuadamente previos a la implantación, y por ende, no se puedan revisar contra los resultados planeados después de la implantación.

CRITERIO:

La Normativa "Consideraciones Generales de la Implementación 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, dice: "Adoptar políticas sobre la justificación, autorización y documentación de solicitudes de implementación o mantenimiento de TI".

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.

OPORTUNIDAD DE MEJORA 04: NO SE HA ESTABLECIDO LA PROPIEDAD INTELECTUAL DEL SOFTWARE DESARROLLADO INTERNAMENTE. RIESGO BAJO.

CONDICIÓN:

Producto de la revisión efectuada, se corrobora que la Universidad Nacional para los programas y aplicaciones desarrolladas por el personal de la DTIC, no ha establecido la propiedad intelectual del código fuente ni las obligaciones de quien las desarrolla, lo anterior como parte de un contrato de trabajo, manuales de puestos u otro documento válido que proteja los intereses de la universidad.

Lo anterior puede provocar que no se implementen los procedimientos apropiados para asegurar la propiedad de los productos de software desarrollados a lo interno de la organización.

CRITERIO:

La Normativa 1.4.6 Seguridad en la implementación y mantenimiento de software e infraestructura 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, dice: "La organización debe mantener la integridad de los

procesos de implementación y mantenimiento de software e infraestructura tecnológica y evitar el acceso no autorizado, daño o pérdida de información.
Para ello debe:
a. Definir previamente los requerimientos de seguridad que deben ser considerados en la implementación y mantenimiento de software e infraestructura.
b. Contar con procedimientos claramente definidos para el mantenimiento y puesta en producción del software e infraestructura.
c. Mantener un acceso restringido y los controles necesarios sobre los ambientes de desarrollo, mantenimiento y producción.
d. Controlar el acceso a los programas fuente y a los datos de prueba".

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.

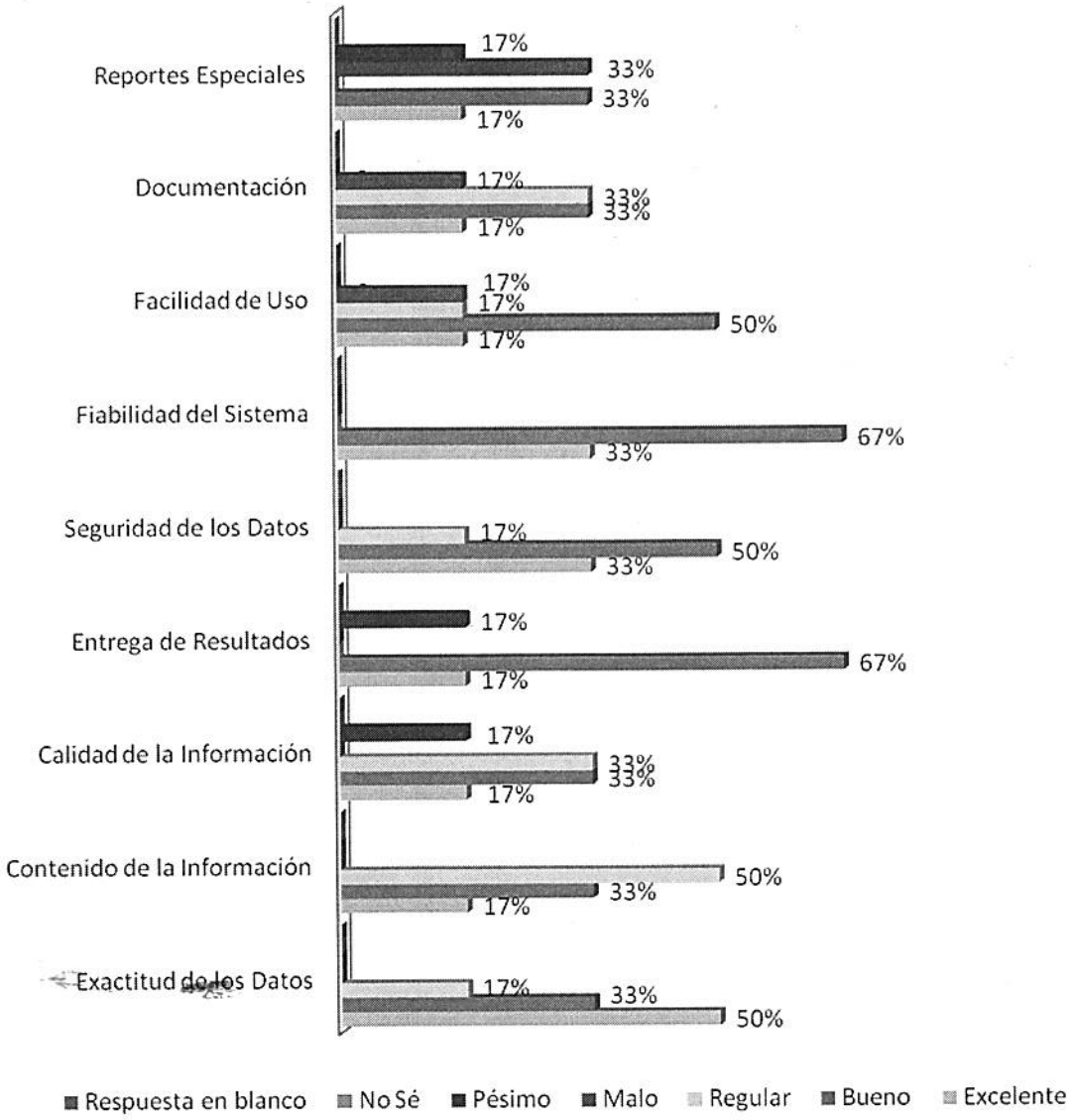
EVALUACIÓN FUNCIONAL DE LOS SISTEMAS DE INFORMACIÓN IMPLANTADOS EN LA UNIVERSIDAD NACIONAL (UNA).

En este apartado se muestra el resultado de la evaluación realizada respecto a la calidad funcional de los sistemas de información implantados en la UNA, según la percepción de los usuarios finales.

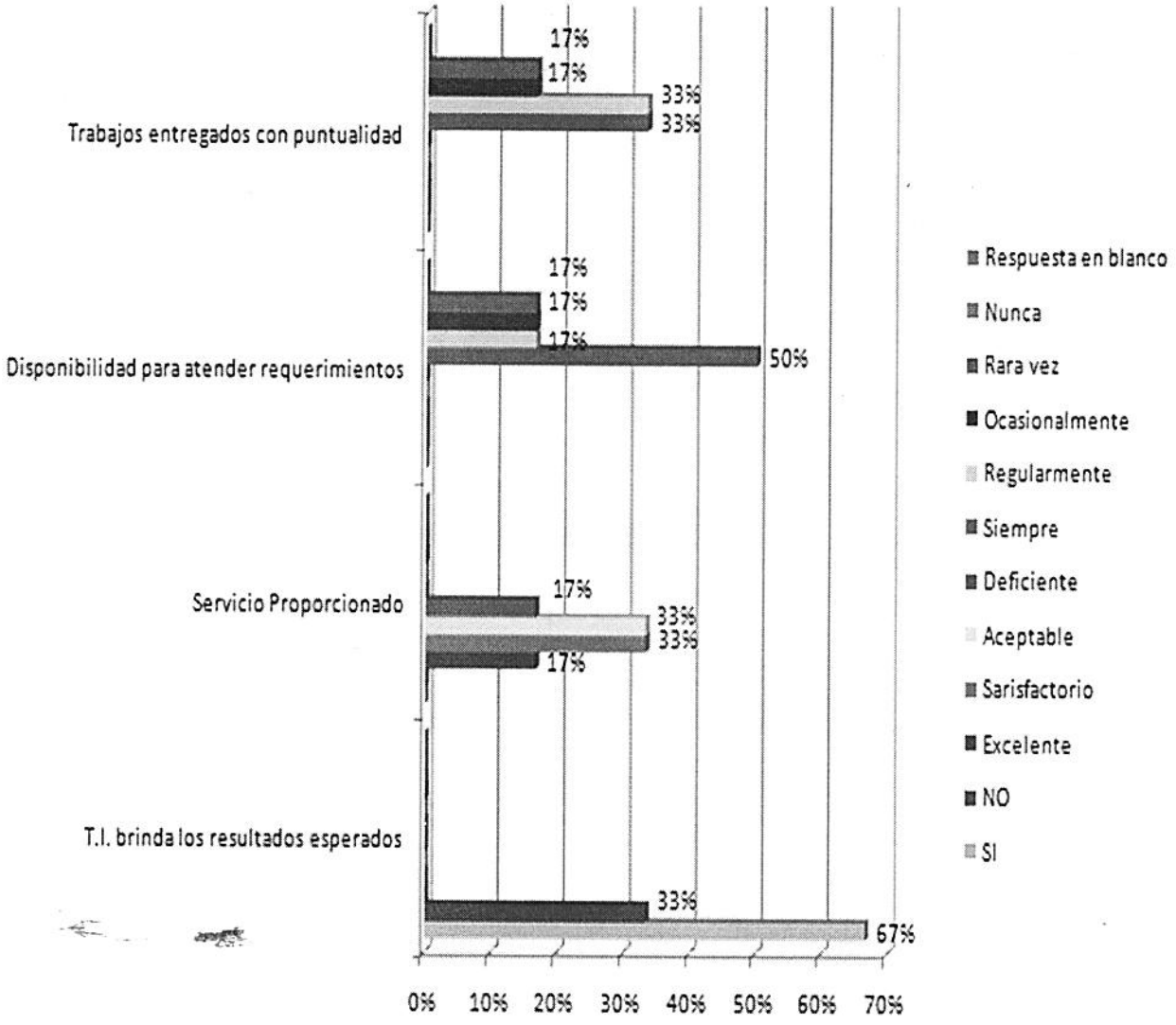
Los módulos evaluados y las personas entrevistadas en el proceso de evaluación de la calidad funcional se muestran en la tabla siguiente:

Sistema a Valorar		*Usuario Final*
BANNER	Registro Contable	Rafael Vargas Ramírez
	Finanzas - Cuentas por pagar	Laura Lobo Chacón
	Cuentas por cobrar	Lina Watson
	Módulo Activos Fijos	Allan Ramírez Sanabria
Admisión	Postulantes, carreras, colegios, pruebas específicas, cupos, reportes, etiquetas y estudiantes regulares	Ana Lorena Camacho Solano
SICOI	Inversiones	Isaac Hernández Sánchez

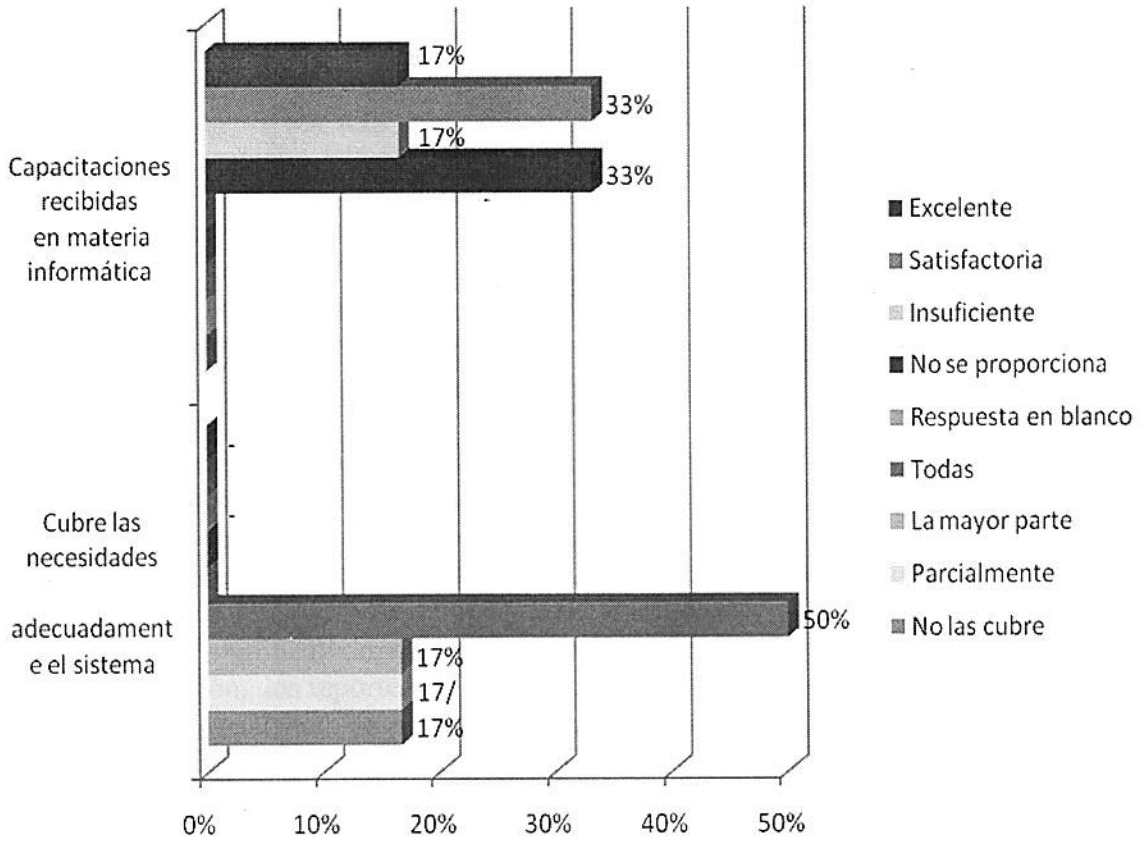
El detalle de la evaluación de la calidad funcional según usuarios a los sistemas de la UNA detallados en el cuadro anterior, se muestran en el gráfico siguiente:



La percepción de los usuarios finales respecto al servicio brindado por parte de la Dirección de Tecnologías de Información y Comunicación de la UNA, se muestran en el gráfico siguiente:



Percepción de los usuarios finales respecto a si los sistemas de información de la UNA cubren satisfactoriamente las necesidades actuales:



Comentarios o mejoras por parte de los usuarios referentes a la valoración de los sistemas de información:

Registro contable:

- En la etapa de digitación del asiento contable una pantalla tipo Excel donde se pueda ver y revisar a la vez toda la información acumulada que se va registrando y no por línea como está actualmente.

Finanzas - Cuentas por pagar:

- Desarrollar un manual de uso del sistema.
- Listar las "FORMAS BANNER" para el mejor aprovechamiento del sistema.
- Implementar un reporte que determine el "Estado" de cada trámite para dar seguimiento.
- Implementar las condiciones a nivel de sistema, que requiere una adecuada gestión de las cesiones de facturas recibidas.
- Ampliar los detalles de información de las facturas con el fin de que pueda ver en pantalla todos los valores pagados. Caso específico de aquellos proveedores que tienen más de 3 registros o que la numeración de sus facturas es muy larga.
- Mejorar significativamente y para efecto de manejo e interpretación de la información, los reportes de las retenciones de renta a proveedores.
- Aviso automatizado de pago a los proveedores a través de correo electrónico.
- Generación automática de certificaciones de retención de renta por periodos.
- Capacitación para el aprovechamiento del sistema, ya que su manejo no es amigable ni simple.
- Alguna información que se necesita extraer del sistema no se realiza de forma automáticamente sino que requiere manipular la información a través de las herramientas de WINDOWS.

Cuentas por cobrar:

- Brindar información más resumida de las interfaces por cajero.

Postulantes, carreras, colegios, pruebas específicas, cupos, reportes, etiquetas y estudiantes regulares:

- Incluir el proceso de cambio de opciones de carrera y segunda opción de carrera para estudiantes regulares, así como los reportes necesarios para llevar a cabo esta labor de manera eficiente y eficaz.

Módulo Activos Fijos:

- Mejorar la emisión de reportes: datos y presentación.
- Menús más amigables.
- Mejorar suficientemente el módulo para alcanzar a nivel institucional una herramienta que brinda mayor confiabilidad en todos sus extremos.

Admisión:

- Incluir el proceso de cambio de opciones de carrera y segunda opción de carrera para estudiantes regulares, así como los reportes necesarios para llevar a cabo esta labor de manera eficiente y eficaz.

RECOMENDACIÓN:

Es deseable que la Dirección de Tecnologías de Información y Comunicación se reúna con los usuarios de las áreas involucradas, con el fin de llevar a cabo las mejoras que correspondan, levantando los requerimientos necesarios cubriendo ciertas necesidades o debilidades que de una u otra forma, afectan los servicios que brinda la UNA

Análisis de Riesgos T.I.
Dirección de T.I. y Comunicación
Periodo 2014

Tipos de Riesgo	
Alto	A
Medio	M
Bajo	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.

Centro computo		Condición	Vulnerabilidad		Comentarios	Observaciones	Tipo Riesgo
			Sí	No			
		Seguridad Física	SI	NO			
☐	☐	Proceso de autorización de ingreso	☐	√	Solo 7 personas ingresan al data center, mediante tarjetas electrónicas, además se debe ingresar por medio de un código que se le asigna a la persona que esté debidamente autorizada.		B
☐	☐	Personal interno y externo debidamente identificado	☐	√	Se encuentran debidamente identificados.		B
☐	☐	Revisión de equipos de ingreso y salida	☐	√	Si se realizan revisiones, el encargado de CGI valora la solicitud y la aprueba, con el visto bueno del director de T.I.		B
☐	☐	Bitácoras de acceso al edificio y centro de cómputo	☐	√	Se lleva un registro por medio de bitácoras físicas para el ingreso al Data Center.		B
☐	☐	Acceso restringido a personal de informática definido	☐	√	Existe restricción de personal que no competen con el Data Center.		B
☐	☐	Una sola vía de acceso	☐	√	Existe una sola vía de ingreso una a través del departamento de TI .		B
☐	☐	Externos son acompañados por internos	☐	√	Si lo realizan de esta forma.		B
☐	☐	Puerta de acceso segura	☐	√	Tiene una puerta, están debidamente protegida.		B
☐	☐	Acceso con tarjeta electrónica al centro de datos	☐	√	Tienen tarjeta electrónica.		B
☐	☐	Alarmas de detección de intrusos	☐	√	Si poseen.		B
☐	☐	Monitoreo de la entrada por cámara de seguridad	☐	√	Existen5 cámaras, una enfocada en la puerta de ingreso del Data Center, otra en el pasillo y las demás en el resto del edificio.		B
☐	☐	Ubicación en un sitio seguro (lugares colindantes)	☐	√	Si se encuentra seguro.		B
☐	☐	Lugar completamente cerrado	☐	√	Si está cerrado.		B

☐	☐	Paredes de concreto	☐	√	Paredes de cemento y un costado es de gypsum.		B
☐	☐	Cielo raso sellado	☐	√	Se encuentra cerrado.		B
☐	☐	Equipos ubicados en rack	☐	√	Así se encuentran.		B
☐	☐	Los rack están asegurados	☐	√	Están debidamente asegurados.		B
☐	☐	Cableado de datos independiente del eléctrico	☐	√	En la parte superior se encuentra los cables de datos.		B
☐	☐	Cableado entubado y canaleteado	☐	√	Si se encuentra el cableado entubado y canaleteado (cableado estructurado).		B
☐	☐	Cableado debidamente rotulado	☐	√	Si se encuentra rotulado.		B
☐	☐	Hay un sitio alterno	☐	√	Se encuentra en el edificio de Financiero y Registro, en la planta baja, de la UNA.		B
		Instalación eléctrica					
☐	☐	Hay pararrayos	☐	√	El edificio cuenta con pararrayos en la azotea.		B
☐	☐	Circuito eléctrico independiente	☐	√	Es independiente.		B
☐	☐	Interruptor de emergencia en la sala de cómputo	☐	√	Si cuentan con interruptor (caja breaker).		B
☐	☐	Cableado eléctrico debidamente entubado o cubierta contra incendios	☐	√	Se encuentra canaleteado, en tubo MT.		B
☐	☐	Conexión de los equipos a UPS	☐	√	Los UPS se encuentran conectados a la planta eléctrica.		B
☐	☐	UPS ubicada en un sitio seguro	☐	√	Se encuentran en el Data Center.		B
☐	☐	Pruebas periódicas de la UPS	☐	√	Se realizan cuando se les da mantenimiento.		B
☐	☐	UPS en contrato de mantenimiento preventivo y correctivo	☐	√	Se manejan con el proveedor (Soporte crítico).		B
☐	☐	Conexión a Planta eléctrica	☐	√	Las UPS alimentan mientras la planta eléctrica entra en funcionamiento.		B
☐	☐	Planta eléctrica ubicada en un sitio seguro	☐	√	Si se encuentra en un sitio seguro, fuera del edificio.		B
☐	☐	Pruebas periódicas de la Planta eléctrica	☐	√	Si se realizan revisiones periódicas, dichas		B

					pruebas las hace el área de mantenimiento.		

	☐	Planta eléctrica en contrato de mantenimiento preventivo y correctivo	☐	√	Si lo realizan		B
☐	☐	Luces de emergencia en el centro de cómputo o cercanías	☐	√	Si se encuentran luces de emergencia cerca del Data Center		B
☐	☐	Pruebas periódicas de sistema de iluminación de emergencias	☐	√	Se realizan pruebas cada vez que se va la luz.		B
		Instalación aire acondicionado					
☐	☐	Equipo de aire acondicionado independiente para el centro de datos	☐	√	Si son independientes.		B
☐	☐	Equipo de respaldo para el aire acondicionado	☐	√	Si existe equipo de respaldo para el aire acondicionado.		B
☐	☐	Contrato de mantenimiento preventivo y correctivo	☐	√	Se contrata anualmente para el aire y la UPS.		B
☐	☐	Control y monitoreo de humedad y temperatura	☐	√	Si cuentan con un monitoreo de temperatura.		B
		Desastres Naturales					
☐	☐	Brigada de emergencias	☐	√	Si hay brigadas a nivel de la institución.		B
☐	☐	Capacitación del personal	☐	√	Si se han realizado.		B
☐	☐	Rutas de evacuación y salidas de emergencia	☐	√	Si cuentan.		B
☐	☐	Señalización	√	☐	Si cuentan con señalización.		B
☐	☐	Simulaciones periódicas	☐	√	Si se realizan simulaciones.		B
☐	☐	Fácil acceso por Unidades de Bomberos	☐	√	Tienen un pasaje amplio para ello.		B
☐	☐	Sistemas de detección de humo/calor/fuego	☐	√	Si cuentan con sistema de detección de humo.		B

☐	☐	Sistemas automáticos y manuales de alarma	☐	√	Si cuentan con alarma manual de la oficina.		B
☐	☐	Extinguidores cercanos portátiles (revisados al día)	☐	√	Si están al día y cercano al Data Center		B
☐	☐	Uso de aspersores (detector de incendio, rocía agua en caso de incendio)	☐	√	Si tienen.		B
☐	☐	Pisos falsos	☐	√	Si cuenta con piso falso.		B
☐	☐	Desnivel en el piso	☐	√	No cuenta con desnivel		B
		Fallas en Hardware					
☐	☐	Redundancia de servidores críticos	☐	√	Si existe redundancia.		B
☐	☐	Mantenimiento preventivo	☐	√	Si se da mantenimiento a los servidores y estaciones de trabajo, se realizan semestralmente, o mensualmente dependiendo del servidor		B
☐	☐	Mantenimiento correctivo	☐	√	Si se da mantenimiento a los servidores y estaciones de trabajo, se realiza semestralmente.		B
		Fallas en Software					
☐	☐	Política de uso de recursos	☐	√	Si cuentan con una política de uso de recursos.		B
☐	☐	Control de cambios	☐	√	Realizan control de cambios al software.		B
		Fallas en Comunicaciones					
☐	☐	Redundancia de equipos y enlaces	☐	√	Existen enlaces con el ICE a diferentes velocidades (internet), y correos y envío de información de la nube.		B
☐	☐	Mantenimiento preventivo	☐	√	Se realiza por medio del ICE.		B
☐	☐	Mantenimiento correctivo	☐	√	Se realizan por medio del ICE.		B

		Respaldos y recuperación					
☐	☐	Política de respaldos	☐	√	Si cuentan con política de respaldos.		B
☐	☐	Procedimientos para respaldo y recuperación	☐	√	Si cuentan con procedimiento de respaldos y recuperaciones, cuando se solicita una clonación lo hacen por medio del ITOP.		B
☐	☐	Almacenamiento de información	☐	√	Se realizan en cintas, de un servidor a otro, y en la nube la parte de correos.		B
☐	☐	Traslado de respaldos	☐	√	Se trasladan a cintas y luego se llevan al sitio alterno cuando se requiera.		B
☐	☐	Configuración de programas para respaldo	☐	√	Los respaldos se hacen automáticos, además existe un robot que realiza respaldos de disco a cinta.		B
		Ataques por virus					
☐	☐	Política de antivirus	☐	√	Si cuentan.		B
☐	☐	Programa antivirus	☐	√	Si cuentan con programa antivirus llamado Karpeski.		B
☐	☐	Actualización del antivirus	☐	√	El registro del antivirus se hace diario por medio de la consola de antivirus.		B
☐	☐	Administración de incidentes y problemas	☐	√	Si cuentan y lo administran por medio del ITOP.		B

		Intrusión					
☐	☐	Política de acceso lógico	☐	√	Si tienen procesos establecidos para los accesos		B
☐	☐	Control de acceso a aplicaciones	☐	√	Si cuentan con control de acceso.		B
☐	☐	Monitoreo de usuarios y accesos	☐	√	Si cuentan con dichos monitoreos.		B
		Administración de Operaciones					
☐	☐	Capacitación personal técnico	☐	√	Si se imparten capacitaciones.		B
☐	☐	Segregación de funciones	☐	√	Existe segregación de funciones.		B

		Riesgos de la gestión de TI					
☐	☐	¿Se tienen definido un plan estratégico para IT alineado con el de la organización?	☐	√	Sí existe y se encuentra alineado.		B
☐	☐	¿El Plan estratégico ha sido divulgado a los niveles que corresponde?	☐	√	Se encuentra aprobado por la alta gerencia.		B
☐	☐	¿Se tienen definidas las políticas y procedimientos para IT?	☐	√	Sí se cuentan con políticas y procedimientos de tecnologías de información.		B
☐	☐	¿Se tiene definido el apetito de riesgos para IT?	☐	√	Si cuentan con una metodología de riesgos.		B
☐	☐	¿Los riesgos que la organización se encuentra dispuesta a aceptar se encuentran aprobados formalmente por la Administración y el Comité de Auditoría?	☐	√	Si se encuentran aprobados.		B
☐	☐	¿El mapa de riesgos es revisado y actualizado periódicamente?	☐	√	Si se define el mapa de riesgos.		B
☐	☐	¿La evaluación de riesgos considera elementos cualitativos y cuantitativos?	☐	√	Si se han definido los riesgos de TI.		B
☐	☐	¿Los riesgos de IT son revisados con los usuarios del sistema?	☐	√	Si son revisados con los usuarios.		B
☐	☐	¿Se han implementado anti virus y firewalls?	☐	√	Si se han implementado.		B
☐	☐	¿Se han establecido los protocolos para la	☐	√	Si se han establecido los protocolos.		B

		realización de copias de seguridad?					
☐	☐	¿La seguridad de la información es un tema de seguimiento para la alta gerencia como para el Comité de Auditoría?	☐	√	Es correcto.		B
☐	☐	¿Las políticas y procedimientos relacionados son revisados y actualizados periódicamente, considerando los cambios en la industria y la regulación externa?	☐	√	Si se realizan revisiones periódicamente.		B
☐	☐	¿Se tiene definido el perfil para cada cargo de IT y los colaboradores vinculados cumplen con el mismo?	☐	√	Si se tiene definido.		B
☐	☐	¿Se tienen definido un plan estratégico para IT alineado con el de la organización?	☐	√	Si se tiene definido.		B
☐	☐	¿Se tienen definidas y divulgadas las funciones y responsabilidades de cada colaborador del área?	☐	√	Es correcto		B
☐	☐	¿Las responsabilidades de cada nivel y colaborador, parten del principio de segregación de funciones?	☐	√	Es correcto.		B
☐	☐	¿La creación de usuarios y la asignación de los permisos y/o perfil en los aplicativos es solicitada y aprobada formalmente por cada Líder de área?	☐	√	Se realiza de esta manera.		B
☐	☐	¿Los usuarios de las herramientas conocen formalmente sus responsabilidades con el uso de las mismas?	☐	√	Si las conocen.		B
☐	☐	¿Las herramientas de IT permiten tener la trazabilidad de las operaciones realizadas así como de los usuarios (logs)?	☐	√	Las herramientas si permiten tener la trazabilidad.		B
☐	☐	¿Se monitorea el estado de los equipos (Hardware)?	☐	√	Se monitorea a través de la herramienta NAGIOS.		B
☐	☐	¿La seguridad física de las instalaciones donde operan los equipos y personas de IT, es evaluada y revisada periódicamente, cumplimiento con los protocolos establecidos?	☐	√	Si es revisada periódicamente.		B

□	□	¿La organización desarrolla un plan de formación integral tanto para los miembros de IT como para los usuarios de la herramienta, orientado al uso, seguridad y ética en la utilización de las mismas?	□	√	Si existe un plan de capacitación.		B
□	□	¿Se han establecido indicadores de gestión que permitan medir el desempeño de las herramientas como de los colaboradores del área ?	√	□	No se realizan evaluaciones de desempeño al personal de T.I.		M
□	□	¿Se han implementado planes de acción correctivos, para aquellos casos en que los indicadores presentar resultados inferiores a los esperados?	√	□	No se establecen planes de acción con base en las evaluaciones de desempeño del personal, ya que éstas no se realizan.		M
□	□	¿Se han adquirido pólizas de seguro para eventos de riesgos en el área de IT?	□	√	Si se han adquirido pólizas de seguro.		B
□	□	¿Cada proyecto de IT tienen definidos y documentos los riesgos tanto de su desarrollo como de la puesta en marcha, así como tiene la proyección de recursos financieros a invertir?	□	√	Si los tienen definidos.		B
□	□	¿ Se hace un seguimiento periódico al cumplimiento contractual de las obligaciones adquiridas por los proveedores de IT y dicho seguimiento es documentado?	□	√	Si se realiza un seguimiento periódico.		B
□	□	¿ Todos los cambios desarrollados en las aplicaciones y/o software son documentados y custodiados?	□	√	Si son documentados y custodiados.		B
□	□	¿Se ha establecido el plan de continuidad para los procesos de IT?	√	□	Si poseen un plan de continuidad establecido, sin embargo no se han llevado a cabo todos los planes de contingencia definidos.		M
□	□	¿Se solicita el apoyo de consultores externos para los proyectos estratégicos?	□	√	Si se solicita el apoyo de consultores externos.		B