IMPRENTA NACIONAL

ÁREA AUDITADA: INFORMÁTICA

INFORME – AU-014-2012

ESTUDIO SOBRE EQUIPOS DE COMUNICACIÓN Y SERVIDORES

NOVIEMBRE 2012

CONTENIDOS

I. INTRODUCCIÓN

1.1 Origen

Plan Anual de la Auditoría Interna de la Imprenta Nacional 2012.

1.2 Objetivo

Evaluar el uso, rendimiento y administración de los Equipos de Comunicación y Servidores.

1.3 Alcance

El estudio comprende el análisis de toda la documentación y opiniones de expertos o responsables hasta mayo del 2012, ampliándose en los casos que se estimó conveniente.

1.4 Limitación

No hubo limitaciones importantes.

1.5 Metodología

El presente estudio se realizó en apego a las disposiciones emitidas por la Contraloría General de la República, Ley General de Control Interno, Normas Técnicas para la Gestión y el Control de las Tecnologías de Información, Normas de Control Interno para el Sector Público, Directrices Generales para el SEVRI y toda la legislación de la Imprenta Nacional.

Se obtuvo los criterios legales y técnicos relativos a tecnologías de información y comunicación aplicables a los procesos informáticos que se realizan en la Imprenta Nacional.

Se aplicaron hojas de observación y tomas de fotografías al Data Center y al Cuarto de Comunicaciones y Servidores en conjunto con el personal de Soporte Técnico para conocer el cumplimiento de la normativa técnica y legal aplicable a los centros de administración de datos digitales de la Imprenta Nacional.

Por último, se solicitó documentación técnica y administrativa al jefe de Informática sobre los procesos para la administración de los centros de datos digitales.

1.6 Antecedentes

La Imprenta Nacional utiliza las tecnologías para apoyar sus procesos administrativos y de producción. La información generada se almacena en bases de datos Oracle, archivos planos y archivos de aplicaciones propietarias.

Como parte de esa administración de datos, la Imprenta Nacional tiene espacios físicos en donde se colocan los equipos de comunicaciones y servidores para centralizar, asegurar y distribuir los datos de todas las aplicaciones informáticas a los usuarios finales.

Es importante mencionar que ambos lugares tienen servidores con aplicaciones sin replicación y también servidores en donde se da una replicación de aplicaciones y bases de datos para asegurar la disponibilidad del servicio por medio de la redundancia.

Por último, es transcendental manejar la información aquí expuesta con muchísimo celo profesional y apegado a las más estrictas prácticas de confidencialidad por necesidades de seguridad informática.

1.7 Recordatorio

Conforme lo dispone la Contraloría General de la República, de seguido se cita textualmente lo dispuesto en los artículos Nos. 36, 37, 38 y 39 de la Ley General de Control Interno, que indica lo siguiente:

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

por la auditoría interna, estarán sujetas, en lo conducente, a lo dispuesto en los artículos siguientes.
c) El acto en firme será dado a conocer a la auditoría interna y al titular subordinado correspondiente, para el trámite que proceda.

Artículo 37. —Informes dirigidos al jerarca. Cuando el informe de auditoría esté dirigido al jerarca, este deberá ordenar al titular subordinado que corresponda, en un plazo improrrogable de treinta días hábiles contados a partir de la fecha de recibido el informe, la implantación de las recomendaciones. Si discrepa de tales recomendaciones, dentro del plazo indicado deberá ordenar las soluciones alternas que motivadamente disponga; todo ello tendrá que comunicarlo debidamente a la auditoría interna y al titular subordinado correspondiente.

Artículo 38. —Planteamiento de conflictos ante la Contraloría General de la República. Firme la resolución del jerarca que ordene soluciones distintas de las recomendadas por la auditoría interna, esta tendrá un plazo de quince días hábiles, contados a partir de su comunicación, para exponerle por escrito los motivos de su inconformidad con lo resuelto y para indicarle que el asunto en conflicto debe remitirse a la Contraloría General de la República, dentro de los ocho días hábiles siguientes, salvo que el jerarca se allane a las razones de inconformidad indicadas.
La Contraloría General de la República dirimirá el conflicto en última instancia, a solicitud del jerarca, de la auditoría interna o de ambos, en un plazo de treinta días hábiles, una vez completado el expediente que se formará al efecto. El hecho de no ejecutar injustificadamente lo resuelto en firme por el órgano contralor, dará lugar a la aplicación de las sanciones previstas en el capítulo V de la Ley Orgánica de la Contraloría General de la República, N° 7428, de 7 de setiembre de 1994.

Artículo 39. —Causales de responsabilidad administrativa. El jerarca y los titulares subordinados incurrirán en responsabilidad administrativa y civil, cuando corresponda, si incumplen injustificadamente los deberes asignados en esta Ley, sin perjuicio de otras causales previstas en el régimen aplicable a la respectiva relación de servicios.
El jerarca, los titulares subordinados y los demás funcionarios públicos incurrirán en responsabilidad administrativa, cuando debiliten con sus acciones el sistema de control interno u omitan las actuaciones necesarias para establecerlo, mantenerlo, perfeccionarlo y evaluarlo, según la normativa técnica aplicable…"

II HALLAZGOS

2.1 Firmas de aprobación en los procedimientos.

La documentación sobre los procedimientos de los procesos de la administración técnica del Data Center y del Cuarto de Comunicaciones y Servidores no registran los nombres, firmas, fechas y horas de las personas con la potestad para realizarlas, revisarlas y aprobarlas.

Sobre lo anterior, las Normas de Control Interno para el Sector Público de la CGR, establece lo siguiente:

> *"2.5 Estructura organizativa…*
> *2.5.2. Autorización y aprobación.*
> *La ejecución de los procesos, operaciones y transacciones institucionales debe contar con la autorización y la aprobación respectivas de parte de los funcionarios con potestad para concederlas, que sean necesarias a la luz de los riesgos inherentes, los requerimientos normativos y las disposiciones institucionales.*
> *… "*

Esta condición podría ser causada por una débil gestión técnico-gerencial de los procesos del área de Equipos de Comunicaciones y Servidores ya que los funcionarios de Informática facilitaron algunos procedimientos incompletos o faltando algunos procedimientos de procesos que ya están funcionando.

Esta situación demuestra una informalidad en los procedimientos y no le da el rango de oficialidad requerido. Además, provocaría que los funcionarios de informática una alta complejidad en la atención técnica de los equipos de comunicación y servidores debido a que no se tiene clarificado el último procedimiento oficial. Finalmente, sube el nivel de riesgo de pérdida de la información ó daño de los equipos de comunicaciones y servidores por la compleja administración de los sistemas de información sin autorización oficial.

2.2 Valoración de riesgos.

El departamento de Informática carece de un análisis de riesgos que valore correctamente las amenazas y vulnerabilidades inherentes a su administración técnica del Data Center y del Cuarto de Comunicaciones y Servidores.

Sobre lo anterior, las Normas de Control Interno para el Sector Público de la CGR, establecen lo siguiente:

> *"3.1 Valoración del riesgo.*
> *El jerarca y los titulares subordinados, según sus competencias, deben definir, implantar, verificar y perfeccionar un proceso permanente y participativo de valoración del riesgo institucional, como componente funcional del SCI. Las autoridades indicadas deben constituirse en parte activa del proceso que al efecto se instaure. "*

Esta condición podría ser causada por una débil gestión administrativa de la valoración de riesgos del área de Equipos de Comunicaciones y Servidores ya que el enfoque de riesgos aplicados hasta el momento ha sido solo para los proyectos de integración de los nuevos sistemas de información.

Lo anterior provocaría que los procesos de la administración técnica de los equipos de comunicaciones y servidores se realicen sin conocer las amenazas y vulnerabilidades de los activos de tecnologías de información. Por esto no se podría determinar la distribución de los recursos humanos, financieros y técnicos, al resguardo de los activos con mayores niveles de riesgo y podría conducir a pérdidas de información muy sensible.

2.3 Administración de procesos de seguridad.

El departamento de informática no realiza una completa administración de los procesos de seguridad de la información del Data Center y del Cuarto de Comunicaciones y Servidores en un documentado, controlado y registrado sistema de control de control. La siguiente tabla muestra las debilidades (NO) halladas:

Data Center				
Criterio	**Proceso**	**Doc.**	**Cont.**	**Reg.**
1.4.3	Seguridad física basada en análisis de riesgos	NO	NO	NO
1.4.3.a	Acceso físico a las instalaciones	SI	SI	SI
1.4.3.b	Ubicación segura de los recursos	SI	SI	SI
1.4.3.c	Movimientos de ingreso y salida de los recursos	NO	NO	NO
1.4.3.d	Servicios de mantenimiento	SI	SI	NO
1.4.3.e	Desecho y reutilización de los recursos	NO	SI	NO
1.4.3.f	Respaldo de energía eléctrica	NO	SI	SI
1.4.3.g	Acceso de terceros	NO	SI	SI
1.4.3.h	Riesgos asociados con el ambiente	NO	SI	SI
1.4.6	Seguridad en la implementación y mantenimiento	SI	SI	NO
1.4.6.a	Requerimientos de seguridad	NO	SI	NO
1.4.6.b	Procedimientos para software e infraestructura	SI	SI	NO
1.4.6.c	Acceso restringido a los ambientes de TI	SI	SI	SI
1.4.6.d	Acceso a fuentes y datos de prueba	NO	SI	NO

Cuarto de Comunicaciones y Servidores				
Criterio	**Proceso**	**Doc.**	**Cont.**	**Reg.**
1.4.3	Seguridad física basada en análisis de riesgos	NO	NO	NO
1.4.3.a	Acceso físico a las instalaciones	NO	SI	SI
1.4.3.b	Ubicación segura de los recursos	NO	SI	SI
1.4.3.c	Movimientos de ingreso y salida de los recursos	NO	NO	NO
1.4.3.d	Servicios de mantenimiento	SI	SI	NO
1.4.3.e	Desecho y reutilización de los recursos	NO	SI	NO
1.4.3.f	Respaldo de energía eléctrica	NO	SI	SI
1.4.3.g	Acceso de terceros	NO	SI	SI
1.4.3.h	Riesgos asociados con el ambiente	NO	SI	SI
1.4.6	Seguridad en la implementación y mantenimiento	NO	SI	NO
1.4.6.a	Requerimientos de seguridad	NO	SI	NO
1.4.6.b	Procedimientos para software e infraestructura	NO	SI	NO
1.4.6.c	Acceso restringido a los ambientes de TI	NO	SI	SI
1.4.6.d	Acceso a fuentes y datos de prueba	NO	SI	NO

Sobre lo anterior, las Normas de Control Interno para el Sector Público de la CGR, establece lo siguiente:

> *"1.4 Responsabilidad del jerarca y los titulares subordinados sobre el SCI.*
> *La responsabilidad por el establecimiento, mantenimiento, funcionamiento, perfeccionamiento y evaluación del SCI es inherente al jerarca y a los titulares subordinados, en el ámbito de sus competencias.*
> *En el cumplimiento de esa responsabilidad las autoridades citadas deben dar especial énfasis a áreas consideradas relevantes con base en criterios tales como*

su materialidad, el riesgo asociado y su impacto en la consecución de los fines institucionales, incluyendo lo relativo a la desconcentración de competencias y la contratación de servicios de apoyo. Como parte de ello, deben contemplar, entre otros asuntos, los siguientes:
…
c. La emisión de instrucciones a fin de que las políticas, normas y procedimientos para el cumplimiento del SCI, estén debidamente documentados, oficializados y actualizados, y sean divulgados y puestos a disposición para su consulta.
d. La vigilancia del cumplimiento, la validez y la suficiencia de todos los controles que integran el SCI."

Esta condición podría ser causada por una débil gestión administrativa del sistema de control interno de los procesos del área de Equipos de Comunicaciones y Servidores ya que el enfoque de control interno, aplicado hasta el momento, se ha concentrado en aplicar las mejores prácticas del proveedor del Data Center y no un adecuado proceso de control interno.

Esta situación provoca fuertes amenazas a la seguridad de la información. Además, conlleva a procesos de trabajo más complejos y de baja productividad. También, el personal de soporte podría ejecutar criterios dispares para la administración de la seguridad de la información. Finalmente, la suma de estas condiciones tienen un alto riesgo tecnológico.

2.4 Bitácoras de mantenimientos técnicos.

El departamento de informática realiza los mantenimientos técnicos a los equipos de comunicación y servidores sin realizar reportes o bitácoras en las cuales se detalle el trabajo realizado en el Data Center y el Cuarto de Comunicaciones y Servidores.

Sobre lo anterior, las Normas técnicas para la gestión y el control de las Tecnologías de Información de la CGR, establece lo siguiente:

"1.4.3 Seguridad física y ambiental.
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:
…

d. El debido control de los servicios de mantenimiento.
…"

Esta condición podría ser causada por una desatención de los técnicos al no realizarlas y una incompleta supervisión del jefe al no exigir esa información sobre cada uno de todos los mantenimientos realizados, ya que existen las boletas físicas para almacenar esas bitácoras con la información de cada mantenimiento.

Esta situación provocaría a los funcionarios de informática un aumento de la complejidad en la atención técnica de los equipos de comunicación y servidores, debido a que no se tiene el historial de los trabajos de mantenimiento técnico realizados. Además, no se tienen estadísticas para realizar acciones preventivas y no solo las correctivas típicas de un ambiente no administrado. También, tiende a subir el nivel de riesgo de pérdida de la información ó daño de los equipos, por las pocas acciones preventivas aplicadas y el posible aumento de las interrupciones, en el momento de corregir los daños.

2.5 Fuente alterna de electricidad.

El Data Center y el Cuarto de Comunicaciones y Servidores no cuentan con una fuente alterna de producción de energía eléctrica para dar continuidad a sus servicios digitales ni a las aplicaciones de uso institucional. A pesar de contar con una UPS para respaldo eléctrico, estas tienen una duración de uso muy corta, especialmente si el evento fue durante el fin de semana.

Sobre lo anterior, las Normas técnicas para la gestión y el control de las Tecnologías de Información de la CGR, establece lo siguiente:

"1.4.3 Seguridad física y ambiental.
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:
…
f. La continuidad, seguridad y control del suministro de energía eléctrica, del

cableado de datos y de las comunicaciones inalámbricas.
…"

Esta condición podría ser causada por atrasos administrativos de la gestión de compra debido a que se ha presupuestado y aprobado el dinero para realizar la compra de una planta eléctrica pero aún no se concreta.

Esta situación provocaría que se interrumpan los servicios digitales prestados a los habitantes de la República y también las aplicaciones de uso institucional, debido a la interrupción de los servicios eléctricos y el agotamiento de la energía de las UPS. También, tendería a subir el nivel de riesgo de pérdida de la información y especialmente el daño de los equipos de comunicaciones y servidores por el apagón repentino.

2.6 Temperatura ambiental de los Equipos de TI.

El Cuarto de Comunicaciones y Servidores no cuenta con un adecuado sistema de control de la temperatura debido a que solo hay un aire acondicionado, tipo minisplit, para uso de oficina. Este aparato de aire acondicionado no es adecuado para la cantidad de equipos de comunicaciones y servidores que se encuentran instalados en ese sitio.

Sobre lo anterior, las Normas técnicas para la gestión y el control de las Tecnologías de Información de la CGR, establece lo siguiente:

"1.4.3 Seguridad física y ambiental.
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:
…
h. Los riesgos asociados con el ambiente.
…"

Esta condición podría ser causada por atrasos administrativos de la gestión de compra debido a que se ha presupuestado y aprobado el dinero para realizar la compra de un sistema de aire acondicionado más adecuado a esas necesidades, pero aún no se concreta.

Esta situación provocaría que en caso de que se interrumpa el control de temperatura del aire instalado llevará a que aumente la temperatura interna del Cuarto de Comunicaciones y Servidores y podría dañar todos los equipos electrónicos allí instalados. También, subiría el nivel de riesgo de pérdida de la información y especialmente el daño de los equipos de comunicaciones y servidores por las altas temperaturas.

III CONCLUSIÓN

La Imprenta Nacional, principalmente en su Data Center, y en menor medida en el Cuarto de Comunicaciones y Servidores cuenta con excelentes equipos de comunicación y servidores y las medidas de seguridad física informática adecuadas para atender las necesidades tecnológicas. Sin embargo, carece de adecuadas técnicas de administración tecnológica y de un bajo sistema de control de interno para su administración.

IV RECOMENDACIONES

Como resultado del estudio anterior, se generan las siguientes recomendaciones:

4.1. A la Junta Administrativa de la Imprenta Nacional

4.1.1 Girar las directrices necesarias a las instancias competentes, para que se cumplan las recomendaciones planteadas en este Informe.

4.1.4 Informar a la Auditoría Interna de los resultados obtenidos en el acatamiento de las recomendaciones emitidas en este Informe.

4.2. Al Director General de la Imprenta Nacional

4.2.1. Girar las instrucciones respectivas a quien (es) corresponde, para que se cumplan las recomendaciones planteadas en este Informe.

4.2.4. Informar a la Auditoría Interna de los resultados obtenidos en el acatamiento de las recomendaciones emitidas en este Informe.

4.3. Al Jefe de Informática.

4.3.1. Incorporar los respectivos nombres, firmas, fechas y horas de las personas con la potestad para realizar, revisar y autorizar la documentación de los manuales y procedimientos de los equipos de comunicación y los servidores. **(Ver hallazgo 2.1)**

4.3.2. Realizar una valoración de riesgos de las áreas del Data Center y del Cuarto de Comunicaciones y Servidores para establecer las amenazas y vulnerabilidades, con el fin de implementar las medidas correctivas para disminuir los niveles de riesgos inherentes. **(Ver hallazgo 2.2)**

4.3.3. Implementar un sistema de control interno adecuado a las necesidades proyectadas de la valoración de riesgos de la seguridad de la información de las áreas del Data Center y del Cuarto de Comunicaciones y Servidores. **(Ver hallazgo 2.3)**

4.3.4. Realizar la documentación y bitácoras de los mantenimientos técnicos realizados a los equipos de comunicaciones y servidores ubicados en las áreas del Data Center y del Cuarto de Comunicaciones y Servidores. **(Ver hallazgo 2.4)**

4.3.5. Realizar las gestiones y estudios necesarios para incorporar un respaldo alterno de energía eléctrica complementario a las UPS ya instaladas. **(Ver hallazgo 2.5)**

4.3.6. Realizar las gestiones y estudios necesarios para instalar un sistema de control de la temperatura ambiental que satisfaga las necesidades del Cuarto de Comunicaciones y Servidores. **(Ver hallazgo 2.6)**

4.3.4. Informar a la Auditoría Interna de los resultados obtenidos en el acatamiento de las recomendaciones emitidas en este Informe.