



UNIDAD DE AUDITORIA INTERNA

TECNOLOGIA DE LA INFORMACION

AÑO 2016

INFORME AUDITORIA N° 12

DICIEMBRE 2017

INFORME EJECUTIVO DE AUDITORÍA

INFORME N° 12 / Hospital Nacional en Red - UAI /2017

TECNOLOGIA DE LA INFORMACION -Año 2016

El presente informe es realizado de acuerdo a lo previsto en el plan anual 2017 de esta Unidad de Auditoría Interna.

Objeto de la Auditoria consistió en evaluar que las acciones informáticas desarrolladas en la institución resulten adecuadas desde la perspectiva tecnológica y operativa y también se encuadren dentro de la legislación y normativa vigente para tal fin.

El objeto del proceso es brindar servicios referidos a la tecnología de la información, bajo la supervisión y coordinación de los profesionales a cargo del Centro de Cómputos.

El alcance del presente informe comprendió:

Comprobar a través de reuniones con los responsables del área informática de la institución (Centro de Cómputos) y de la aplicación de cuestionarios específicos (elaborados a partir de instructivos surgidos desde organismos ejecutivos y de control, como por ejemplo SIGEN) el adecuado nivel de la tecnología de la información instrumentada en el organismo.

Verificar el grado de cumplimiento de las sugerencias aportadas por la SIGEN mediante la Resolución SGN N° 48/05 sobre la Organización Informática, Plan Estratégico Informático, Políticas y Procedimientos Informáticos y Seguridad Informática.

Las tareas de auditoría se llevaron a cabo entre el 8 de noviembre y el 22 de diciembre de 2017.

El examen se realizó de acuerdo con las Normas de Auditoría Interna Gubernamental, aprobadas por Resolución N° 152/02 Sindicatura General de la Nación.

El período auditado corresponde al estado de situación del sector al mes de noviembre 2017.

No se tuvo indicios de que la organización cuente con un Plan Informático Estratégico.

De acuerdo a lo relevado, hasta el presente no tuvimos evidencias concretas de la existencia de una política de seguridad de la información.

En virtud de la tarea realizada según el alcance descripto en el punto 3, los comentarios desarrollados en el punto 6; las observaciones expuestas en el punto 7 y el seguimiento de las observaciones del punto 8; las acciones informáticas desarrolladas en la institución resultan razonablemente adecuadas.

Con relación al sitio web y al dominio web del Hospital no hay observaciones que formular.

Ciudad Autónoma de Buenos Aires, 26 de diciembre de 2017

INFORME DE AUDITORÍA

INFORME Nº 12 / Hospital Nacional en Red - UAI /2017

TECNOLOGIA DE LA INFORMACION -Año 2016

De: Auditor Interno
Dr. Hugo Gimigliano

Al: Sr. Interventor del Hospital Nacional en Red Lic. Laura Bonaparte
Dr. Leandro Mera

Al: Sr. Interventor del Departamento Administrativo Financiero y Servicios Generales.
Dr. Pablo M. Cuadros Panunzio.

1. INTRODUCCIÓN

El presente informe denominado “Tecnología de la información”, se realiza de acuerdo a lo previsto en el Plan Anual 2017 de esta Unidad de Auditoría Interna.

2. OBJETO

El objeto de la Auditoria consistió en evaluar que las acciones informáticas desarrolladas en la institución resulten adecuadas desde la perspectiva tecnológica y operativa y también se encuadren dentro de la legislación y normativa vigente para tal fin.

El objeto del proceso es brindar servicios referidos a la tecnología de la información, bajo la supervisión y coordinación de los profesionales a cargo del Centro de Cómputos.

3. ALCANCE

El alcance del presente informe comprendió:

- Comprobar a través de reuniones con los responsables del área informática de la institución (Centro de Cómputos) y de la aplicación de cuestionarios específicos (elaborados a partir de instructivos surgidos desde organismos ejecutivos y de control,

como por ejemplo SIGEN) el adecuado nivel de la tecnología de la información instrumentada en el organismo.

- Verificar el grado de cumplimiento de las sugerencias aportadas por la SIGEN mediante la Resolución SGN N° 48/05 sobre la Organización Informática, Plan Estratégico Informático, Políticas y Procedimientos Informáticos y Seguridad Informática.

Para esto se realizaron los siguientes procedimientos:

- Se elaboró un cuestionario en concordancia con la Resolución SGN N° 48/05 aprobatoria de las Normas de Control Interno para la tecnología de la información para el sector Público Nacional con las adaptaciones a las particularidades del sistema informático del organismo.
- Se verificó en la Dirección Nacional del Registro de Dominios de Internet los datos de los dominios de internet que posee el Hospital.
- Se realizaron pruebas de verificación tendientes al seguimiento de las observaciones pendientes de regularización.

Las tareas de auditoría se llevaron a cabo entre el 8 de noviembre y el 22 de diciembre de 2017.

El examen se realizó de acuerdo con las Normas de Auditoría Interna Gubernamental, aprobadas por Resolución N° 152/02 Sindicatura General de la Nación.

El período auditado corresponde al estado de situación del sector al mes de noviembre 2017.

4. LIMITACION AL ALCANCE

No se pudo mantener entrevista con el responsable del sector Tecnología de la Información a pesar de que la misma fue solicitada por nota.

5. MARCO DE REFERENCIA

- Resolución SGN N° 48/05 aprobatoria de las Normas de Control Interno para la tecnología de la información para el sector Público Nacional.

6. TAREAS REALIZADAS

Ante la negativa de conceder una entrevista se elaboró un cuestionario a efectos de verificar lo dispuesto en la Resolución SIGEN Nº 48/05 aprobatoria de las Normas de Control Interno para la Tecnología de la Información para el sector Público Nacional con las adaptaciones a las particularidades del sistema informático del organismo.

El día 8 de noviembre se solicita una entrevista con el responsable del área de TI adjuntando el cuestionario para que se tome conocimiento de los temas a tratar en la entrevista. Mediante nota Nº NO-2017-27378716-APN-D#HNRESMYA.

El Jefe 1 del Depto. Administrativo Contable y Servicios, por nota Nº NO-2017-27523179-APN-DACYS#HNRESMYA, responde que no corresponde tener reuniones porque no es el mecanismo para dar respuesta a los requerimientos de la SIGEN y que oportunamente se nos enviara la documentación necesaria para dar respuesta a los cuestionarios.

Por nota Nº NO-2017-28617044-APN-DACYS#HNRESMYA el día 16 /11/2017, se responde el cuestionario solicitado.

Por nota del 28/11/2017 Nº NO-2017-30231312-APN-D#HNRESMYA, se solicita documentación de respaldo a lo volcado en el cuestionario.

El día 13/12/2017 a través de nota Nº NO-2017-32691845-APN-DACYS#HNRESMYA, se responde que la documentación del respaldo solicitada se encuentra en el expediente 062/2017. El cual fue solicitado mediante nota Nº NO-2017-33170851-APN-D#HNRESMYA. Luego se analizó el expediente a efectos de recabar del mismo las respuestas al cuestionario.

6.1 Cuestionario Resolución Nº 48 Sigen

A continuación, se expone el cuestionario y las respuestas al mismo, vertidas por el sector las cuales se detallan en letra cursiva:

1. ORGANIZACION INFORMATICA

1.1. Responsable de la unidad de Tecnología de la Información (TI).

"Por resolución 50/2016 de fecha 5 de mayo de 2016, el Interventor General lo delega al Departamento Administrativo Financiero y Servicios Generales".

La dependencia funcional del área de informática recae en el Interventor del Departamento Administrativo Financiero y Servicios Generales, Cr. Pablo M. Cuadros Panunzio.

1.2. ¿Dentro de la estructura orgánica está garantizada la independencia de la unidad de TI respecto de las áreas usuarias, asegurando la atención de todos los sectores de la organización.

“Parcialmente”

1.3. ¿Existe una descripción documentada y aprobada de los puestos de trabajo que conforman la unidad de TI, la cual debe contemplar tanto la autoridad como la responsabilidad?

“No”

2. PLAN ESTRATEGICO DE TI

2.1. ¿Existe un plan informático estratégico?

“Se encuentra en el Exp 062/2017 de Servicio de Mantenimiento de Software y Hardware – KHEM LABS SRL-OC 10/2017. Ver Fojas 20 (dorso); artículo 2º del Pliego de Bases y condiciones del Clausulas Especiales.

A criterio de esta UAI, lo citado en el mencionado expediente dentro de las cláusulas especiales en su artículo 2º “Descripción de las tareas”, no representa un plan informático estratégico.

2.2 ¿El plan informático estratégico está alineado con el plan estratégico y el presupuesto de la organización?

“Se encuentra en el Exp 062/2017 de Servicio de Mantenimiento de Software y Hardware – KHEM LABS SRL-OC 10/2017. Ver Fojas 8, autorización de la solicitud de gastos de afectación preventiva y ver foja 315 Orden de compra”.

A criterio de esta UAI, esta respuesta no corresponde a lo solicitado.

2.3. ¿El plan informático está aprobado por la dirección de la organización?

“Por Resolucion Nº 50/2016 de fecha 5 de mayo de 2016, el Interventor General lo delega al Departamento Administrativo Financiero y Servicios Generales. Esta aprobado el procedimiento y el pliego a través de la Disposición Nº 61/2017 de fecha 01 de marzo de 2017.”

El pliego de acuerdo a lo vertido por esta UAI en el punto 2.1 no constituye per se un plan informático estratégico. Asimismo, el pliego no está aprobado por la Intervención General, sino por una disposición del Interventor Administrativo Financiero y Servicios

Generales que a la postre es responsable del área de informática, no existiendo un control por oposición en esta operación.

2.4. ¿Cuál es la periodicidad de actualización del plan?

“Anual”

2.5. ¿Existe un presupuesto elaborado por la unidad de TI asociado a la ejecución del plan informático y el desarrollo de sus actividades, está evaluado y aprobado por la dirección?

“Se encuentra en el Exp 062/2017 de Servicio de Mantenimiento de Software y Hardware –KHEM LABS SRL – OC 10/2017”

La respuesta del auditado hace referencia a una orden de compra, lo cual no responde a lo solicitado.

3. ARQUITECTURA DE LA INFORMACION

3.1. ¿Está definido por la unidad de TI el modelo de arquitectura de la información de la organización, orientado a asegurar que los datos se encuentren organizados eficientemente y de manera homogénea, garantizando que estarán disponibles para su utilización, en concordancia con las necesidades operativas de las diferentes áreas usuarias en cuanto a oportunidad, integridad, exactitud o formato, entre otras?

“Sí, aunque todavía se está trabajando en mejorar la redundancia en los datos”

4. POLITICAS Y PROCEDIMIENTOS

4.1. ¿La unidad de TI ha desarrollado, documentado y comunicado políticas y procedimientos respecto de las actividades relacionadas con la TI?

“Parcialmente, existen documentos en la Intranet que detallan los procedimientos de las actividades de TI, sin embargo, aún se están redefiniendo políticas de la Unidad”

5. CUMPLIMIENTO DE REGULACIONES EXTERNAS

5.1. ¿La unidad de TI garantiza el cumplimiento de las regulaciones relativas a privacidad de la información, propiedad intelectual del software, seguridad de la información, así como de las demás normas que resulten aplicables?

“Sí”

5.2. ¿La unidad de TI ha establecido convenios o contratos formales con aquellos terceros con los que existan intercambios de información o prestación de servicios relacionados con la TI?

“Sí”

5.3 Especificar convenio y contratos, proveedor, periodo.

“Licencias de Windows – Proveedor: Soft Line Internacional – OC Nº 50/2016 del 18/10/2016”

“Compra de Computadoras - Proveedor: Servicio Globales de Informática S.A.- OC Nº 23/2016 del 6/07/2016”

“Compra de Computadoras – Proveedor: CORADIR – OC Nº 63/2016 del 22/12/2016”

“Proveedor de Internet: Telmex – Desde el 2008 a la fecha”

“Proveedor de Almacenamiento de Datos: AMX – Desde 05/2016 a la fecha”

“Proveedor de Internet: FIBERCORP-Desde fines 2015 a la fecha.”

“Servicio de Mantenimiento/Actualización de Software – OC 10/2017 del 10/04/2017 – Periodo 01/04/2017 al 31/03/2018”

6. ADMINISTRACION DE PROYECTOS

6.1. ¿La unidad de TI dispone de una metodología de administración de proyectos?

“Sí”

6.2. Describa brevemente:

“Se utiliza la metodología SCRUM para el seguimiento de los proyectos de Desarrollo (aplicaciones internas, sitios web, etc.) y se realizan reuniones mensuales con el equipo de TI para revisar el avance y prioridades de las tareas del área.”

7. DESARROLLO, MANTENIMIENTO O ADQUISICION DE SOFTWARE DE APLICACIÓN.

7.1. ¿La unidad de TI dispone de un procedimiento o metodología para las actividades de desarrollo, mantenimiento o adquisición de sistemas, que debe estar documentado y aprobado, y debe aplicarse en forma complementaria a las normas relativas a administración de proyectos?

“Parcialmente, existen el procedimiento y metodología, pero el mismo no esta documentado.”

La unidad de TI no dispone de un procedimiento o metodología documentado.

7.2. ¿Está justificada por escrito y autorizada por el responsable de la unidad de TI La contratación de servicios externos de desarrollo de sistemas?

“Sí”

7.3 ¿En los contratos de servicios externos de desarrollo de sistemas está asegurada la propiedad intelectual del software para el organismo?

“Si, los desarrollos se hacen bajo licencias open source y el código siempre es entregado al organismo.”

8. ADQUISICION Y MANTENIMIENTO DE LA INFRAESTRUCTURA TECNOLOGICA

8.1. ¿Existe un plan de mantenimiento preventivo periódico del hardware, a fin de reducir la frecuencia y el impacto de las fallas en su desempeño?

“Se encuentra en el Exp .062/2017 de Servicio de Mantenimiento de Software y Hardware – KHEM LABS SRL-OC 10/2017. A fojas 21 artículo 2º inciso 2 y 3 hace referencia a la infraestructura y microinformática”.

8.2. ¿Existen procedimientos documentados para la gestión de licencias de software a fin de asegurar que en la organización solamente se utilicen productos adquiridos por vías oficiales?

“Se adquirieron mediante licitación, según expedientes que se detallan a continuación:

1-2002-4134000139/16 Adquisición Licencias Windows.

1-2002-4134000645/16 Adquisición Computadoras

9. SEGURIDAD

9.1. ¿Existe una política de seguridad de la información?

“Se encuentra en el Exp. 062/2017 de Servicio de Mantenimiento de Software y Hardware – KHEM LABS SRL – OC 10/2017- ”

Hasta el presente no existe una política de seguridad de la información, en el expediente está previsto que, de acuerdo a los requerimientos de infraestructura de TI, el proveedor sugiera implemente y administre las políticas de seguridad del organismo intra y extra muros.

10. SERVICIOS DE PROCESAMIENTO Y/O SOPORTE PRESTADOS POR TERCEROS

10.1. ¿En caso de contrataciones de servicios externos en los que el proveedor realice el procesamiento de la información de la organización mediante sistemas que pertenecen al tercero, careciendo la organización de los programas fuente, existen previsiones necesarias para asegurar la disponibilidad de los mismos por parte de la organización en caso de alguna contingencia o salida del mercado del proveedor —por ejemplo, dejando una copia de los fuentes bajo custodia de escribano para el caso de una eventual quiebra del proveedor ?

“Los datos y los programas (con su correspondiente código fuente) se encuentran resguardados en los servidores de la organización”

11. SERVICIOS DE INTERNET/EXTRANET/ INTRANET

11.1. ¿El contenido y la estructura del sitio web de la organización está aprobado por las autoridades, se encuentran documentados los siguientes aspectos: contenido y estructura del sitio web, fuentes de ingreso de datos, frecuencia de las actualizaciones, necesidades de disponibilidad del sitio, recursos afectados, ¿responsable de los contenidos y todo otro dato atinente al contenido y funcionamiento del sitio?

“Si, el contenido del sitio web de la intranet / extranet / intranet es administrado por la unidad de Comunicación y aprobado por la dirección”.

11.2. ¿Existe un acuerdo de nivel mínimo de servicios con los proveedores de los servicios de comunicaciones, a fin de asegurar que la prestación de los mismos se corresponda con los requerimientos de la organización?

“Si”

12. MONITOREO DE LOS PROCESOS

12.1. ¿Existen indicadores de desempeño para monitorear la gestión y las excepciones de las actividades de TI?

“Se adjuntan a continuación los mails donde surgen los grados de avance de las tareas desarrolladas.”

Esta UAI no tuvo evidencias de indicadores de desempeño de monitoreo de la gestión.

6.2 Dominio de Internet

Se constató que el sitio web del Hospital estuviera disponible en la web.

Se verificó en la Dirección Nacional del Registro de Dominios de Internet, dependiente de la Subsecretaría Técnica de la Secretaría Legal y Técnica de la Presidencia de la Nación los datos del dominio “cenareso.gob.ar” a nombre del Hospital Nacional en Red especializado en Salud Mental y Adicciones Lic. Laura Bonaparte, con fecha de alta el 11 de marzo de 2003, y cuya fecha de vencimiento opera el 13 de abril de 2018.

Y el dominio “hospitalbonaparte.gob.ar” que posee el Hospital, el cual está a nombre del Hospital Nacional en Red especializado en Salud Mental y Adicciones Lic. Laura Bonaparte, con fecha de alta el 7 de agosto de 2017, y cuya fecha de vencimiento opera el 7 de agosto de 2018.

7. OBSERVACIONES

7.1. Observación al punto 6.1 (2.1 del cuestionario)

No se tuvo indicios de que la organización cuente con un Plan Informático Estratégico.

Impacto: Medio.

Causa: Falta de estructura orgánica de TI.

Efecto: Ausencia de un esquema de actualización orientado a evaluar la conveniencia de incorporar nuevas tecnologías y evitar la obsolescencia tecnológica.

Opinión del Sector Auditado: *"Al no encontrarse dentro de la estructura orgánica la Unidad de TI, que es quien debe elaborar e implementar un plan estratégico, es que no poseemos el mismo, tal como lo expresa art. 2; 1.2 y 2.1. Resolución SGN 48/05".*

Comentario de la UAI: Se mantiene la observación.

Recomendación: Se recomienda arbitrar los medios necesarios para la formulación de un plan estratégico de informática.

7.2. Observación al punto 6.1 (9.1 del cuestionario)

De acuerdo a lo relevado, hasta el presente no tuvimos evidencias concretas de la existencia de una política de seguridad de la información.

Impacto: Medio.

Causa: Falta de estructura orgánica de TI.

Efecto: La falta de política de seguridad atenta contra con el resguardo de la información del hospital.

Opinión del Sector Auditado: *"Se adjunta en archivo embebido el informe producido al efecto por la empresa prestataria del servicio de mantenimiento de software y hardware...".*

Comentario de la UAI: Habiendo solicitado un detalle de la política de seguridad de la información del hospital, nos fue dado un informe de los trabajos realizados en el área de sistemas. Lo cual no constituye una descripción de la política de seguridad del organismo. De acuerdo a lo expuesto se mantiene la observación.

Recomendación: Se recomienda arbitrar los medios necesarios para la delinear una política de seguridad.

8. SEGUIMIENTO DE LAS OBSERVACIONES

Informe 13 Fecha 28/12/2016 Impacto: Medio **Estado:** En Trámite

Texto del Hallazgo Nº 1:

En base a la respuesta aportada por el sector auditado en el cuestionario establecido por la Resolución 48/2005 SIEGEN, con relación a la Organización Informática se observa que no está garantizada la independencia de la unidad de TI respecto de las áreas usuarias, asegurando la atención de todos los sectores de la organización.

Comentario UAI:

Desde el 3 de enero de 2018 por resolución 10 del Interventor General el área de informática pasa a depender en forma directa de la Intervención General para su jerarquización como surge de los fundamentos de dicho acto administrativo. Por lo expuesto se regulariza la observación.

Informe 13 Fecha 28/12/2016 Impacto: Medio **Estado:** En Trámite

Texto del Hallazgo Nº 2:

El organismo no dispone de un procedimiento o metodología para las actividades de desarrollo, mantenimiento o adquisición de sistemas.

Comentario UAI:

De acuerdo a la manifestación vertida, no surge un procedimiento documentado y aprobado para las actividades de desarrollo, mantenimiento o adquisición de sistemas. Se mantiene la observación hasta la próxima revisión.

9. CONCLUSION

En virtud de la tarea realizada según el alcance descripto en el punto 3, los comentarios desarrollados en el punto 6; las observaciones expuestas en el punto 7 y el seguimiento de las observaciones del punto 8; las acciones informáticas desarrolladas en la institución resultan razonablemente adecuadas.

Con relación al sitio web y al dominio web del Hospital no hay observaciones que formular.

Ciudad Autónoma de Buenos Aires, 26 de diciembre de 2017