Objeto:
Auditoría de relevamiento y supervisión de las tecnologías de la información en el Ministerio de Gobierno (MG).

Período auditado:
17 de enero al 12 de abril de 2019.

Normativa relevante:
Resoluciones N° 177-ASINF/13, N° 239-ASINF/14, N° 12-ASINF/17 y N° 46-ASINF/17.

Equipo auditor:
Emilse TEYO
Federico SZTYRLE
Matías VIESCA
José GOICOECHEA
Martín ZANITTO
Rodrigo DEPETRIS

Informe Ejecutivo

PROYECTO N° 43/19
Ministerio de Gobierno
Dirección General Técnica, Administrativa y Legal

Alcance:
A fin de relevar la gestión de activos de información realizada en el Ministerio de Gobierno (en adelante MG), en primera instancia se verificó la existencia de documentación que respalde dicha gestión. En el caso de no contar con ella, se procedió a trabajar de manera conjunta con el auditado en una identificación de los activos de información pertenecientes a su dominio, de modo tal que posteriormente les permitiese determinar la criticidad de la misma basándose en la clasificación de acuerdo a sus niveles de Confidencialidad, Integridad y Disponibilidad.
Una vez realizada la identificación y clasificación de los activos, esta información fue registrada por el auditado en un documento desarrollado por esta Sindicatura General, de acuerdo a los lineamientos establecidos por la Agencia de Sistemas de Información. Posteriormente, se procedió a la evaluación y supervisión del mismo.
Las tareas de campo se llevaron a cabo entre los días 17 de enero y 12 de abril de 2019, en las dependencias del Ministerio de Gobierno cuyas locaciones a continuación se detallan:

- Ministerio de Gobierno - Dirección General Técnica, Administrativa y Legal (en adelante DGTALGOB) sita en las calle Uspallata 751.
- Ministerio de Gobierno - sita en la calle Rivadavia 620.
- Subsecretaría de Trabajo, Industria y Comercio (en adelante SSTIYC) sita en la calle Bartolomé Mitre 545.
- Dirección General Registro del Estado Civil y Capacidad de las Personas (en adelante DGRC) sita en la calle Uruguay 751.

Limitaciones al alcance:
No existieron.

Principales hallazgos/observaciones:
a) Descentralización de la supervisión de las áreas de sistemas en las dependencias de la DGRC y de la SSTIYC. La mencionada descentralización, no se encuentra en concordancia con las Misiones y Funciones de la Mesa de Ayuda del Ministerio y suboptimiza la supervisión de las áreas de sistemas mencionadas, pudiendo conllevar al riesgo de ineficiencias en la gestión de TI.

b) No se ha evidenciado la existencia de un Plan Estratégico u Operativo para el año en curso. La ausencia de planes conlleva a riesgos de imprevisión que a su turno generan ineficiencias en la administración de los recursos.

c) Inexistencia de Plan de Contingencia y de Continuidad de las Actividades. Dada la criticidad que poseen los activos de información para dar soporte de las actividades

que se realizan en el Organismo, se pone en riesgo la operatoria y la seguridad de la información del Ministerio.

d) Tanto para las aplicaciones administradas por la DGRC y por la SSTIYC, no ha sido posible verificar durante las tareas de relevamiento, la existencia de políticas y procedimientos para su operación y mantenimiento. Asimismo, y habida cuenta que la mayoría de las aplicaciones pertenecientes a la DGRC y la SSTIYC revisten características de alta criticidad (según la clasificación realizada por el mismo auditado), se evidencia que las mismas no están en concordancia con los requisitos mínimos de seguridad de información que deberían de acuerdo a esta clasificación.
Por otra parte, los recintos donde se alojan estas aplicaciones carecen de las medidas de seguridad física requeridas.
Lo expresado podría constituir posibles riesgos de falta de integridad y disponibilidad de información que tendrían impacto en la administración de las operaciones del organismo auditado.

e) Del relevamiento efectuado a una muestra de ciento diecisiete (117) equipos informáticos, se comprobaron los hechos que a continuación se listan, los cuales indican que la administración del parque informático no se encuentra completamente alineada con lo dispuesto en las Políticas del Grupo 7 del Marco Normativo de TI poniendo en riesgo la seguridad de la información del organismo:

- Cuarenta y cuatro (44) equipos no operan en Dominio, lo que representa un 38% del total de equipos relevados.
- Dos (2) equipos no cuentan con el Antivirus Corporativo implementado, lo que representa un 2% del total de equipos relevados.
- Veintiocho (28) equipos presentan Actualizaciones Pendientes de instalar para su Sistema Operativo las cuales son de carácter importantes o críticas, lo que representa a un 24% del total de equipos relevados.
- Nueve (9) equipos tienen implementado *Software* no Corporativo o de entretenimiento, lo que representa un 8% del total de equipos relevados.
- Cincuenta y cuatro (54) equipos no cuentan con un Bloqueo Automático de la estación de trabajo en períodos de inactividad, lo que representa al 46% del total de equipos relevados. Estos equipos pertenecen a la DGRC.
- Se ha evidenciado una notable heterogeneidad en las versiones instaladas del Sistema Operativo, según el siguiente detalle obtenido de los equipos relevados: noventa y cuatro (94) versión *Windows 7*, siete (7) equipos versión *Windows 8*, cuatro (4) equipos versión *Windows 8.1*, once (11) equipos versión *Windows 10*, y un (1) equipo versión *Windows 7 Ultimate*.

f) Del relevamiento efectuado en los CPD localizados en dependencias que administra el MG, se evidencia que la seguridad física y del entorno de los mismos no se encuentra completamente alineada con lo dispuesto en las Políticas del Grupo 6 del Marco Normativo de TI:

1. CPD de la DGRC - No se ha evidenciado la existencia de: piso técnico, cartelería indicando la prohibición de fumar, comer dentro del recinto, de control de temperatura, de sistema de control de polvo, de programa de mantenimiento periódico del recinto, ni de libro de registro de visitantes.
2. CPD de la SSTIYC – El recinto no cumple con las características técnicas exigibles por la normativa vigente. Se trata de una oficina compartida donde se alojan equipos, servidores y otros elementos de soporte. Se ha notado la existencia de elementos combustibles como cajas, y resmas de papel para impresión. Las puertas no son ignífugas, las puertas de emergencia no son ignífugas, y no se ha evidenciado la existencia de un registro de personas autorizadas para el ingreso al recinto, ni de visitantes.

En ambos casos, no se ha evidenciado la existencia de procedimientos formales para la habilitación de personas a los recintos descriptos.

Lo expuesto evidencia que la descentralización de la gobernanza del Área de Sistemas del Ministerio, podría generar riesgos en la administración de la información crítica alojada en los recintos arriba mencionados, toda vez que el auditado ha informado que la mayoría de las aplicaciones allí alojadas revisten ese carácter.

Respuesta del organismo al Informe de Auditoría:
Emitió opinión.

Conclusiones y principales recomendaciones:
En base a la información remitida por el auditado y al resultado de las tareas de fiscalización efectuadas por este Organismo de Control, se infiere que la principal fortaleza del auditado radica en la administración de su Parque Informático y la clasificación de activos de TI efectuada, clave para implementar de manera eficiente una gestión de la seguridad de la información en base a riesgos tecnológicos.
Su principal debilidad deviene de la gestión descentralizada de TI que impacta en la administración de sus aplicaciones y de las áreas críticas donde ellas se alojan. La debilidad señalada constituye una oportunidad de mejora para el servicio que la DGTALGOB le debe brindar a toda la Jurisdicción y que sea de manera integral a todo el Organismo en base a los lineamientos establecidos por el Marco Normativo de TI de GCABA.
Adicionalmente, se recomienda elaborar: los Planes Estratégico y Operativo -conteniendo el cronograma de los trabajos a desarrollar por el sector, los recursos implicados a dichas tareas y los objetivos fijados para el período en curso-; las políticas y procedimientos para la operación y el mantenimiento de las aplicaciones -principalmente aquellas que revisten características de alta criticidad-; y el Plan de Contingencia y el de Continuidad de las Actividades.
Finalmente, es necesario alinear la seguridad física de los Centros de Procesamiento de Datos con las pautas generales definidas en el Marco Normativo de TI, habida cuenta de la criticidad de las aplicaciones alojadas en dichos recintos.

G O B I E R N O DE LA C I U D A D DE B U E N O S A I R E S
"2019 -Año del 25° Aniversario del reconocimiento de la autonomía de la Ciudad de Buenos Aires"

Hoja Adicional de Firmas
Informe externo Reservado

Número: IF-2019-19009707-GCABA-SGCBA

Buenos Aires, Jueves 13 de Junio de 2019

Referencia: Informe Ejecutivo - Proyecto N° 43/19.-

El documento fue importado por el sistema GEDO con un total de 3 pagina/s.

Digitally signed by Comunicaciones Oficiales
DN: cn=Comunicaciones Oficiales
Date: 2019.06.13 16:21:11 -03'00'

MONICA FREDA
Sindico General
SINDICATURA GENERAL DE LA CDAD. AUTONOMA DE BS.AS.
AREA JEFE DE GOBIERNO

Digitally signed by Comunicaciones Oficiales
DN: cn=Comunicaciones Oficiales
Date: 2019.06.13 16:21:12 -03'00'