INFORME EJECUTIVO
INFORME DE AUDITORIA INTERNA Nº 007/2019
TI - Gestión de Incidentes y Continuidad
Proyecto N° 7
Mendoza, 28 de Agosto de 2019

SEÑOR PRESIDENTE:

OBJETIVO:

Evaluar el cumplimiento del marco normativo y reglamentario vigente, evaluando el sistema de control interno y la gestión con relación a los aspectos enunciados dentro de la "Política de Seguridad de la Información Modelo" (Decisión Administrativa 669/2004) bajo las clausulas: "GESTIÓN DE INCIDENTES DE SEGURIDAD" y "GESTIÓN DE LA CONTINUIDAD".
El presente trabajo está incorporado en la Planificación Anual de la Unidad de Auditoria Interna para el corriente año como Proyecto N° 7.

ALCANCE DE LA TAREA:

Las tareas se desarrollaron de acuerdo con las Normas de Auditoria Interna Gubernamental establecidas por Resolución N° 152/2002 de la SINDICATURA GENERAL DE LA NACION, ajustando su alcance a la aplicación de procedimientos de control de cumplimiento y sustantivos. Las mismas se extendieron desde el 22/5/2019 hasta el 26/08/2019.

Las tareas se ajustaron a la evaluación de los siguientes objetivos de control:

- Gestión de Incidentes de Seguridad
- Reporte de los eventos de la seguridad de información
- Reporte de las debilidades de la seguridad
- Comunicación de Anomalías del Software
- Responsabilidades y procedimientos
- Aprendiendo a partir de los incidentes de la seguridad de la información
- Procesos Disciplinarios
- Gestión de Continuidad
- Proceso de Administración de la continuidad del Organismo
- Continuidad de las Actividades y Análisis de los impactos
- Elaboración e implementación de los planes de continuidad de las Actividades del Organismo
- Marco para la Planificación de la continuidad de las Actividades del Organismo
- Ensayo, Mantenimiento y Reevaluación de los Planes de continuidad del Organismo

Las tareas de campo se desarrollaron en Sede Central y en Sede de la UAI, lo cual incluyó las tareas previas, el relevamiento y tareas posteriores vinculadas a la preparación y análisis de los datos recabados.

En forma sintética se detallan a continuación las tareas realizadas de mayor significatividad:

- Mediante nota NO-2019-50248970-APN-UAI#INV - "Requerimientos Iniciales" con fecha 29/05/2019 se solicitó al Responsable de Seguridad de la Información y Jefe del Departamento de Informática y Comunicaciones, la información y documentación de respaldo asociada a la "Gestión de Incidentes y Continuidad" de acuerdo al siguiente detalle:
  - Listado de incidentes asociados a seguridad acontecidos durante los últimos 12 meses.
  - Documentación relacionada con el procedimiento de comunicación y respuesta a incidentes.
  - Documentación relacionada con el procedimiento de gestión de las debilidades de la seguridad por parte de usuarios finales.
  - Documentación relacionada con el procedimiento de gestión de incidentes.
  - Designación del equipo para el manejo de incidentes.
  - Detalle metodología de análisis de impacto de los incidentes.
  - Documentación relacionada con el Plan de Continuidad de las Actividades del Organismo.
  - Documentación relacionada a la definición de amenazas y el Análisis de Riesgos del organismo.

- Descripción detallada de los controles preventivos aplicados al centro de procesamiento de datos basados en las amenazas identificadas.
- Detalle de los planes de Contingencia del organismo.
- Documentación relacionada con el cronograma de pruebas de los planes de contingencia y su realización.

- El día 01/07/2019 se recibió mediante nota NO-2019-58403238-APN-DIYC#INV, la documentación solicitada en los Requerimientos Iniciales, y se comenzó a analizar la misma.
- Mediante correo electrónico ?Ampliación de Requerimientos auditoría Gestión Incidentes y Continuidad? con fecha 14/08/2019 se solicitó al Jefe del Departamento de Informática y Comunicaciones, información y documentación de respaldo asociada a "RESTAURACIÓN de SISTEMAS CRITICOS".
- El día 15/08/2019 se recibió la documentación solicitada en la Ampliación de Requerimientos, y se comenzó a analizar la misma.
- Se entrevistaron a los siguientes funcionarios:
  - Jefe del Departamento de Informática y Comunicaciones
- A partir del día 15/08/2019 se comenzaron a notificar las observaciones.

OBSERVACIONES MAS SIGNIFICATIVAS:

OBSERVACIÓN Nº 1	***NORMATIVA GESTION DE INCIDENTES DE SEGURIDAD DESACTUALIZADA***

La política de Seguridad de la Información del Organismo se encuentra desactualizada.- NO está definido un capítulo de Gestión de Incidentes de Seguridad en el cual se cumplan los lineamientos señalados en la “Política de Seguridad de la Información Modelo” aprobada por la ONTI.

RECOMENDACIÓN

Finalizar y Reglamentar el capítulo de la política de Seguridad de la Información asociado a la Gestión de Indicentes de Seguridad en los plazos acordados con SIGEN.

ESTADO: En Trámite

OBSERVACIÓN Nº 2	***INEXISTENCIA PROCEDIMIENTO REPORTE INCIDENTES***

Se observa que no se dispone de un procedimiento formalmente definido para la comunicación y respuesta ante incidentes en el organismo.

RECOMENDACIÓN

Se recomienda generar un procedimiento de comunicación y respuesta ante incidentes, adecuado a la normativa vigente que contemple una correcta temporalidad en la comunicación del evento y un marco general para las acciones de respuesta ante el mismo.

ESTADO: En Trámite

OBSERVACIÓN Nº 3	***INCIDENTES DE SEGURIDAD NO TRATADOS EN CoTySIC:***

Se observa que no se ha informado al CoTySIC los incidentes de seguridad de la información ocurridos durante el año 2018 y el primer semestre de 2019, incumpliendo lo expresado en la política de SI punto 3.2.1.3 "Asignación de Responsabilidades - Comité de Tecnología y Seguridad de la Información y Comunicaciones (CoTySIC)."

RECOMENDACIÓN

Se recomienda que se incluya en el temario de las reuniones del CoTySIC los incidentes de seguridad que revistan mayor significatividad para la toma de conocimiento y monitoreo por parte del mismo de acuerdo a lo indicado en la política de SI.

ESTADO: En Trámite

OBSERVACIÓN Nº 6	***INEXISTENCIA PROCEDIMIENTO MANEJO INCIDENTES***

Se observa que no se dispone de una normativa formalmente definida que contemple el establecimiento de funciones y procedimientos de manejo de incidentes garantizando una tratamiento sistemático a los incidentes relativos a seguridad.

RECOMENDACIÓN

Se recomienda generar normativa que establezca las funciones y procedimientos de respuesta ante incidentes de

seguridad, adecuado a la normativa vigente que contemple la articulación con los planes de contingencia correspondientes.

ESTADO: En Trámite

OBSERVACIÓN Nº 8	***NORMATIVA GESTION CONTINUIDAD DESACTUALIZADA***

La política de Seguridad de la Información del Organismo se encuentra desactualizada.- NO está definido un capítulo de Gestión de la Continuidad en el cual se cumplan los lineamientos señalados en la “Política de Seguridad de la Información Modelo” aprobada por la ONTI.

RECOMENDACIÓN

Finalizar y Reglamentar el capítulo de la política de Seguridad de la Información asociado a la Gestión de la Continuidad.

ESTADO: En Trámite

OBSERVACIÓN Nº 10	***PLAN DE CONTINUIDAD INCOMPLETO Y DESACTUALIZADO***

El organismo posee un plan de contingencia (CIRC GF 28/2013) que no contempla ninguno de los puntos solicitados en la normativa; funciones y procedimientos de emergencia, acciones correctiva, capacitación y pruebas del plan. Además el mismo no ha sido revisado desde su fecha de creación (año 2013) y no contempla ninguna acción asociada a un Plan de Recuperación ante Desastres o restablecimiento de servicios a los usuarios.

RECOMENDACIÓN

Se recomienda confeccionar un plan integral de Continuidad de las Operaciones adecuado a la normativa vigente, una vez que se haya realizado la actualización del Análisis de Riesgo para el organismo.

ESTADO: En Trámite

OBSERVACIÓN Nº 11	***CENTRO DE PROCESAMIENTO ALTERNATIVO INEXISTENTE***

Se observa la no existencia de un centro de procesamiento de datos alternativo o la realización de un convenio de procesamiento en contingencia con otro organismo.

RECOMENDACIÓN

Se recomienda la realización de convenios de procesamiento en contingencia con algún ente ubicado en la provincia que posea una arquitectura compatible con la implementada por el organismo; y capacidad suficiente para albergar el servicio, hasta tanto se concrete la creación de un Centro de Procesamiento Alternativo propio.

ESTADO: En Trámite

CONCLUSIONES:

Considerando la extensa evolución tecnológica que ha sufrido el organismo en los últimos 10 años la cual ha generado un muy alto grado de informatización en las funciones sustantivas y de apoyo, y en base al alcance y tareas desarrolladas se considera que se presentan falencias en los aspectos de Gestión de continuidad del organismo. Para los demás aspectos analizados en el presente informe, puede señalarse que las medidas adoptadas por el organismo resultan aceptables, debiendo solucionar los aspectos observados en el punto "Observaciones" de acuerdo a los compromisos asumidos.

GALINDO
Fernando
Antonio

Firmado digitalmente por
GALINDO Fernando Antonio
Fecha: 2019.08.29 09:57:28 -03'00'