INFORME AI-INF-ATI-19-32

Resumen Ejecutivo

Informe sobre incidente Cibernético del 19 de abril del 2019

Este estudio es parte de los trabajos especiales realizados en esta auditoría, donde se investigó el incidente informático ocurrido el 19 de abril del 2019. Producto del incidente mencionado, se dio una pérdida de información, lo anterior a pesar de contar con un sitio alterno que debió de prever este tipo de incidentes. Los resultados encontrados se enlistan a continuación:

- ✓ **2.1 Perdida de información con el ataque del 19 de abril 2019.**
- ✓

Se determinaron las siguientes pérdidas:

- **En la Dirección General de Educación Vial**:
  - Lo correspondiente a notas de las pruebas teóricas y prácticas en distintas sedes
- **En la Dirección General de Policía de Tránsito**:
  - Boletas de Citación (Partes) a personas
  - Partes oficiales de colisiones
  - Mapas/Croquis de los accidentes
- **En la Consejo de Seguridad Vial**:
  - Transacciones bancarias de pagos recibidos
  - Impugnaciones
  - Listados de información digitada (se necesitó volver a digitar la misma)

- ✓ **2.2 Comunicación del incidente.**
  La comunicación del incidente fue deficiente con las diferentes direcciones del MOPT.

- ✓ **2.3 Falla de procedimientos de respaldos en la Dirección General de Educación Vial y la Dirección General de Policía de Tránsito**

- ✓ **2.4 El Contrato 2016LN-000007-0058700001 para el fortalecimiento de los recursos de TI.**

  Respecto al contrato se evidencio un incumplimiento del mismo propiamente lo relacionado al punto 4.1 sobre los tiempos de atención de averías.

- ✓ **2.5 Preparación de la institución ante nuevos ataques cibernéticos.**

Por lo tanto, se recomienda a la Junta Directiva que:

INFORME AI-INF-ATI-19-32

A- Instar al Viceministro de Transportes que se giren instrucciones a la Dirección General de Educación Vial y la Policía de Tránsito, con el propósito de que:

A.1-. Elabore los procedimientos necesarios para el control y seguimientos en caso de ataques cibernéticos, que considere los aspectos preventivos tanto de los servidores, equipos y dispositivos que se utilizan en el proceso de manejo de la información y sea comunicado a todas las Direcciones y departamentos funcionales.

B- Instar a la Dirección Ejecutiva para que:

B.1-. Evaluar de forma detallada el contrato actual que se tiene con el consorcio con el fin de que se determine los grados de responsabilidad, así como las sanciones correspondientes según correspondan.

B.2-. Valorar de forma detallada el contrato actual con el Consorcio Control Electrónico S.A. y ADN Solutions S.R.L. la necesidad de una adenda en caso de continuación o renovación del mismo para afrontar futuros casos de este tipo de ataque cibernéticos.

A la Dirección Ejecutiva:

C- Girar instrucciones a la Asesoría de Tecnologías de Información para que:

C.1-. Verifiquen y garanticen a la institución que el objeto del contrato para el sitio alterno sea suficiente para garantizar la continuidad de las operaciones y el salvaguardo de la información en todos sus aspectos y que cuente con la documentación respectiva.

C.2-. Que valore la posibilidad de monitorear continuamente 24/7/365 los sistemas, con el fin de que exista un control continuo de los diferentes sistemas críticos, para que se obtenga una respuesta oportuna en caso de una futura eventualidad.

C.3-. Determine si las funciones como fiscalizadores (del contrato del sitio alterno) que desempeñaron los funcionarios encargados del área de Base de Datos y de Seguridad de la información, están acordes con el objeto de la contratación y las necesidades institucionales.