Estudio No. 04-2017: Aspectos de Seguridad de Tecnologías de Información

Alcance

Evaluar el cumplimiento de □Plan de mejoramiento de la Seguridad- Institucional□ a cargo del Departamento de Informática, correspondiente al periodo establecido del 01 de enero al 30 de setiembre de 2016.

Objetivos específicos

Entre los objetivos definidos para esta revisión, están los siguientes:

1. Revisión de controles de seguridad existentes en apego de las políticas de Seguridad de la Información Institucional y el □Plan de mejoramiento de la Seguridad Informática Institucional□.
2. Verificar el cumplimiento de la normativa vigente, en los aspectos, relacionados con el tema bajo estudio, para el periodo bajo revisión.

Resultados obtenidos

Entre los hallazgos observados, se encuentran:

1. En la visita realizada al área donde se ubica la planta eléctrica, se observó que había un pozo de agua en el piso, que ingresaba por la parte superior del lugar; situación que debe ser atendida lo antes posible, para prevenir riesgos en el funcionamiento del equipo especializado ubicado en el sitio.
2. Se verificó el proceso de ingreso, control al sitio y aprobación de los accesos por terceros al lugar; determinándose que existen deficiencias de control para el acceso al sitio alterno, de acuerdo con lo descrito en los documentos aportados por la Administración.
3. De conformidad con la consulta realizada a los procedimientos disponibles en la intranet institucional, se determinó por ejemplo:
 - Existen dos documentos denominados de igual manera, pero con diferente ubicación en la intranet institucional.
 - Se indican una serie de puestos que no están incluidos en el Manual de Clasificación y Valoración de Puestos vigente.
 - Se establecen nombres de departamentos que no corresponden según la estructura organizacional vigente.
 - Algunos apartados presentan la misma numeración.
 - Se incluye numeración de un apartado, pero no presenta actividades.
4. Al revisar el cumplimiento del procedimiento INF-01-18-48 □Perfiles de Dominio□ con lo obtenido en el reporte denominado Grupos de Dominio, se verificó que la documentación se encontraba desactualizada, debido a la existencia de grupos que no se estaban debidamente incluidos en el procedimiento indicado.
5. Se revisó el documento INF-SI-24-2016 que tiene como actividad principal el inventario de software Institucional, realizado por el ingeniero en seguridad informática, donde se detalla el software instalado y que no está autorizado de conformidad con lo establecido en el □Procedimiento de inventario de software autorizado□ y hoy □Guía Directrices Software

Autorizado □

P17-GI-ACC-23.

Lo cual implica una violación al punto No. 6 de las políticas de seguridad de la información institucional. A la fecha estas situaciones fueron corregidas.

6. Al revisar el informe INF-SI-39-2016, cuyo objetivo es revisar, actualizar y mejorar el programa de continuidad de la Junta de Pensiones, llamó a nuestra atención lo siguiente:
 1. Para el simulacro de continuidad Institucional, no se reportaron todos los encargados de procesos críticos de la Junta.
 2. De la fecha del simulacro efectuado el 29/04/2016 al 07/10/2016, se muestra que en algunos casos, el personal designado por algunos departamentos para atender los procesos en caso de poner en marcha el plan de continuidad, está desactualizado.

Revelando aspectos de riesgo para llevar a cabo la continuidad de procesos críticos para la institución, al no demostrar interés o participación activa de algunos encargados de procesos ya que al 07/10/2016 no habían reportado las causas de su ausencia.

El estudio fue aprobado por la Junta Directiva, en la Sesión Ordinaria No. 16-2017 del 13 de febrero de 2017.