Estudio No. 32-2021:
Compra y funcionamiento de la herramienta NAC-Forescout

I. Alcance

Adquisición y funcionamiento de la herramienta tecnológica denominada NAC.

II. Objetivo

Cumplir el requerimiento del Órgano Colegiado, referente a efectuar un estudio sobre la compra y el funcionamiento de la herramienta llamada "Sistema NAC-FORESCOUT".

III. Resultados Obtenidos

De conformidad con el objetivo propuesto para se concluye:

- ✓ El NAC-Forescout es una herramienta robusta que permite a la Unidad de Seguridad de TI, efectuar validaciones o comprobaciones diarias de los usuarios que se conectan a los equipos tecnológicos que pertenecen a JUPEMA (pc's u otros), con el objetivo de identificar a los usuarios que no cumplen con las políticas definidas en el NAC, proteger los datos de los afiliados e incrementar la seguridad de la información.

- ✓ Se verificó el proceso de contratación efectuado por parte del Departamento Administrativo de la herramienta denominada "Sistema NAC-FORESCOUT" y se estableció:

  - El proceso de contratación al proveedor Soluciones Seguras S.A., cumplió con cada una de las fases establecidas en el Reglamento de Contratación Administrativa y lo establecido en el procedimiento de Contratación de Bienes y Servicios, que se encuentran publicados en la Intranet Institucional.

  - El Departamento de TI justifica la compra del NAC, con base en el estudio técnico efectuado por la empresa SPC Consulting para la evaluación de 3 procesos Cobit, relacionados con la seguridad de la información.

- ✓ El funcionamiento de la herramienta NAC-Forescout se encuentra implementada en la infraestructura tecnológica de JUPEMA, constatando lo siguiente:

  - La responsabilidad del funcionamiento de la herramienta NAC-Forescout, recae en el Ingeniero en Seguridad de Información y el Asistente de Seguridad de la Información, quienes recibieron la capacitación respectiva por parte del proveedor de servicios.

  - Desde el inicio de la contratación hasta el proceso de implementación del NAC-Forescout, el Ingeniero en Seguridad Información era el responsable

de verificar que se cumplieran todas las etapas definidas en un cronograma de trabajo creado por la empresa Soluciones Seguras.

- Los registros incluidos en el Cherwell Software no permiten identificar el tipo de herramienta tecnológica específica (Sistema o equipo) que es afectada cuando se ingresa o clasifica un incidente, por cuanto se identifica es en forma general (por ejemplo Redes y Comunicaciones, Infraestructura de Servidores, Seguridad Centralizado u Oficial de Seguridad Informática).

✓ Se efectuó una comprobación de los registros relacionados con incidentes y solicitudes de servicio entre los periodos del 21/01/2020 al 18/08/2020 y del 19/08/2020 al 11/06/2021, para establecer el comportamiento de estos.

Sin embargo, para esta Auditoría no es posible establecer con certeza, que todas estas situaciones son originadas o son responsabilidad de la Implementación del NAC, debido en primer lugar a la categorización de los incidentes y la existencia de factores exógenos que no son administrados o gestionados por el Departamento de TI de JUPEMA.

Esta revisión fue aprobada en la Sesión Ordinaria No. 115-2021 del 15 de octubre de 2021.