Tecnología de la información y comunicación

Se practicaron 3 auditorías de Tecnología de la Información y Comunicación: una dirigida a la evaluación del proceso administrativo y sistemático para el otorgamiento de la solvencia laboral emitida por el Registro Nacional de Entidades de Trabajo (RNET) implementado por la Dirección del Registro Nacional de Entidades de Trabajo del Ministerio del Poder Popular para el Proceso Social del Trabajo (MPPPST) durante el segundo semestre de año 2015 y al tercer trimestre del ejercicio económico financiero año 2016; una dirigida a evaluar el Sistema Integrado de Gestión de Proyectos de los Consejos Comunales (SIGPCCO) utilizado por el Servicio Fondo Nacional del Poder Popular (Safonapp) durante el ejercicio económico financiero año 2016 y desde el 1 hasta el 23 de enero de 2017; y una dirigida a evaluar el sistema automatizado de información de nómina de la Defensa Pública (DP), así como la seguridad tecnológica implementada por la Dirección Nacional de Tecnología de la Información (DNTI) de la DP durante el ejercicio económico financiero año 2015 y primer trimestre del año 2016.

Fallas y deficiencias

Como resultado de las actuaciones realizadas por este Órgano Superior de Control, se detectó una serie de fallas y deficiencias en los órganos y entes sujetos a su ámbito de control, las cuales se mencionan a continuación:

En el Ministerio del Poder Popular para el Proceso Social del Trabajo (MPPPST)

- En la estructura organizativa, no se encuentra incorporada la Dirección del Registro Nacional de Entidades de Trabajo (RNET).
- El Manual del RNET no se encuentra formalmente aprobado por la máxima autoridad.
- Se constató que cuando falla la interconexión del sistema del RNET con los entes encargados de emitir la información correspondiente a los regímenes prestacionales del sistema de seguridad social, una pantalla de alerta impide a los usuarios efectuar el registro para la emisión de la solvencia laboral, durante el tiempo que se mantenga el servicio fuera de línea.
- Se comprobó que el RNET emite el certificado electrónico de

Solvencia Laboral sin la previa verificación de los estatus en los que podrían encontrarse las entidades de trabajo ante el Instituto encargado de emitir la información integral en materia de prevención, salud y seguridad laboral.

- En pruebas realizadas para el momento de la actuación, se observó que el Sistema del Registro Nacional de Entidades de Trabajo (RNET) no bloquea la clave del usuario después de tres intentos fallidos, así como tampoco emite un mensaje de alerta. Por otro lado, dicho sistema permite al usuario copiar el *Logon_ID* en el campo de contraseña, sin que el aplicativo emita un mensaje que indique que dicha acción no es permitida. Adicionalmente, el sistema solo bloquea la sesión al transcurrir una hora desde que se ha dejado desatendido.
- Se constató la inexistencia de un diccionario corporativo de datos formal que contenga las reglas de sintaxis de la data organizacional y el esquema de clasificación del RNET.
- El modelo de entidad-relación de la base de datos del sistema donde se registra la información relacionada con el RNET no se encuentra normado, ni aprobado.

En el Servicio Fondo Nacional del Poder Popular (Safonapp)

- La Oficina de Sistemas y Tecnología de la Información (Osti) no cuenta con documentación asociada a los manuales de normas y procedimientos, planes de recuperación, aseguramiento del centro de datos, ejecución de respaldos, restauración de sistemas, contingencia y de seguridad física y lógica.
- La Oficina de Sistemas y Tecnología de la Información no dispone de un Plan de Continuidad Operativa que garantice el restablecimiento oportuno de las operaciones de la plataforma tecnológica ni la restauración de los servicios en un tiempo razonable.
- En cuanto a los mecanismos de seguridad y control de acceso al Sistema Integrado de Gestión de Proyectos de los Consejos Comunales (SIGPCCO), se evidenciaron las siguientes debilidades: Permite copiar el *Logon_ID* (identidad de acceso) en el campo correspondiente a la contraseña; no obliga a los usuarios cambiar la clave periódicamente; no se bloquea al intentar acceder varias veces con clave errada; solo valida contraseñas que contengan

letras y números; admite el uso de claves utilizadas anteriormente por parte de los usuarios, y no bloquea la sesión al permanecer desatendido por un tiempo prolongado.

- En relación con los procesos para la generación de respaldos, su resguardo y eventual restauración, se evidenciaron las situaciones que se mencionan a continuación: ausencia de manuales e instructivos técnicos para los procedimientos de respaldos y reposición de datos debido a que estos están en proceso de levantamiento de información para su elaboración; la Osti no cuenta con una bóveda para almacenar las copias de respaldo del SIGPCCO, a causa de que el Safonapp no dispone de presupuesto para adquirir los dispositivos para tal fin; no se evidenció el resguardo fuera de las instalaciones de la mencionada oficina de las copias de los respaldos, que solo se almacenan en un disco de respaldo conectado al servidor de pruebas, esto aunado a que no cuentan con un servicio de hospedaje o centro de procesamiento de datos alterno; la Osti no dispone de copias físicas de los respaldos del SIGPCCO, debido a la inexistencia de equipos de almacenaje para ello; y la Osti no cuenta con un centro alterno o servicio de hospedaje fuera de las instalaciones de la sede, debido a que el Safonapp no dispone de recursos presupuestarios para la adquisición de servidores; así como tampoco para la contratación de dicha asistencia tecnológica.

En la Defensa Pública (DP)

- La Dirección Nacional de Tecnología de la Información (DNTI) no cuenta con la documentación asociada a los planes de recuperación, aseguramiento del centro de datos, ejecución de respaldos, restauración de sistemas, contingencia y de seguridad física.
- No se observó la existencia de manuales vinculados a los procesos de la división de telecomunicaciones y redes, la división de proyectos e innovación tecnológica o la gestión de usuarios del Sistema Integrado de Gestión Financiera de Recursos Humanos (Sigefirrhh).
- La DNTI no dispone de un plan de continuidad operativa para el restablecimiento de las operaciones de la plataforma tecnológica y la restauración de los servicios en un tiempo razonable.
- No existe un área de seguridad informática en la estructura or-

ganizativa de la DP; no se realizan simulacros de operatividad en sus sistemas de redundancia, respaldo y recuperación; ni auditorías de seguridad informática; y no se ejecutan planes de divulgación, formación y sensibilización en el área de seguridad informática al personal.

- Falta de capacitación del personal en relación con el SIGEFIRRHH.

Recomendaciones

En virtud de la importancia de las observaciones señaladas, y con la finalidad de que estas sean subsanadas en beneficio de una gestión administrativa eficiente y eficaz, este Máximo Órgano Contralor recomienda lo siguiente:

Al director de la Oficina de Tecnología de la Información y Comunicación del MPPPST

- Adelantar las acciones administrativas a fin de aprobar oficialmente el Manual del RNET.
- Establecer planes técnicos de contingencias formales, debidamente verificados y aprobados, para que cuando los servicios de conexión con los entes involucrados en la comprobación de las solvencias se encuentren fuera de línea, se pueda seguir con las comprobaciones de las solvencias laborales.
- Crear procedimientos formales verificados, probados y aprobados que permitan la interacción entre el RNET y el Instituto encargado de emitir la información integral en materia de prevención, salud y seguridad laboral, a los fines de constatar los estatus reales de las empresas del país por ante el mencionado ente.
- Establecer políticas que permitan la validación de forma sistémica de los usuarios que realizan *logging* en el RNET, así como de los campos creados para la escritura de las contraseñas.
- Implantar un diccionario corporativo de datos en el que se definan las reglas de sintaxis de la organización, a objeto de establecer procedimientos que permitan la interconexión entre las aplicaciones, y que estas no difieran de las establecidas por la organización.
- Establecer procedimientos de monitoreo aprobados que permitan minimizar las vulnerabilidades y otros eventos que involucren

las inconsistencias de la información institucional, tal como el modelo de entidad-relación de las bases de datos del RNET.

Al director de la Oficina de Sistemas y Tecnología de la Información del SAFONAPP:

- Dirigir lo concerniente para dar celeridad al proceso de elaboración de los planes, políticas y manuales de normas y procedimientos requeridos en la OSTI, a los fines de su aprobación por parte de la máxima autoridad.
- Elaborar un plan de continuidad operativa que responda a los procesos de recuperación de la información del SAFONAPP. Dicho documento debe estar aprobado por la máxima autoridad e informado al personal involucrado. Asimismo, debe indicar la asignación de responsabilidades sobre su ejecución y control, tendentes a lograr respuestas oportunas ante las posibles interrupciones del servicio, garantizando su recuperación en el menor tiempo posible.
- Implementar políticas que establezcan las validaciones de forma sistémica de los usuarios que acceden en el SIGPCCO, así como de los campos creados para la escritura de las contraseñas. Asimismo, implantar mecanismos automáticos que cierre la sesión del usuario cuando no haya actividad en dicho aplicativo.
- Realizar las gestiones necesarias para resguardar copias de los respaldos fuera de las instalaciones del SAFONAPP.
- Gestionar lo concerniente a la instalación o contratación del servicio de un centro de procesamiento de datos alterno que permita recuperar los servicios del SAFONAPP en un tiempo razonable, garantizando la continuidad de los servicios de Tecnología de Información.

A la Dirección Nacional de Tecnología de la Información (DNTI) de la Defensa Pública (DP)

- Emprender las gestiones que correspondan para definir, revisar e implementar los planes de recuperación, aseguramiento del centro de datos, ejecución de respaldos, restauración de sistemas, contingencia y de seguridad física; así como de las políticas y manuales vinculados a los procesos de la división de telecomunicaciones y redes, la división de proyectos e innovación tecnológica y la

gestión de usuarios del SIGEFIRRHH, a los fines de su aprobación por parte de la máxima autoridad.

- Establecer un plan de continuidad operativa debidamente documentado, aprobado por la máxima autoridad, el cual debe ser informado al personal involucrado, a los fines de que responda a los procesos de recuperación de la información de la plataforma tecnológica administrada por la DNTI, el cual debe indicar los documentos generados para tal fin la asignación de responsabilidades sobre su ejecución y control, tendentes a lograr respuestas oportunas ante las posibles interrupciones del servicio, garantizando su recuperación en el menor tiempo posible.
- Formalizar la incorporación de un área de seguridad informática como apoyo a la gestión de la DNTI. Esta área deberá participar en los simulacros de operatividad en sus sistemas de redundancia, respaldo y recuperación; auditorías anuales y de la labor formativa y masificadora de información sobre la seguridad informática que deben llevar a cabo en las instituciones.
- Tramitar la realización y consecución de un plan de capacitación dirigido a todos los funcionarios que interactúan con el SIGEFIRRHH, con el objetivo de brindar formación en cuanto a su funcionalidad.