INFORME EJECUTIVO
Auditoría de Gestión – Controles Generales de TI
Sistema de Información de Personal y Nómina PERNO

PERIODO DE EJECUCION

Entre el 23 de mayo y 1 de julio de 2025, en cumplimiento del Plan Anual de Auditoría aprobado para el 2025, se realizó auditoría de gestión sobre los controles generales de tecnología para el Sistema de Información de Personal y Nómina PERNO.

OBJETIVO GENERAL

Establecer la existencia, aplicabilidad y efectividad de los controles generales de Tecnología para el Sistema de Información PERNO, que permitan asegurar la confidencialidad, integridad y disponibilidad de la información. Así como al seguimiento de las acciones de mejora implementadas como resultado de la auditoría anterior.

ALCANCE

Se evaluaron los controles generales de tecnología en el Sistema de Información PERNO, correspondientes a: administración de usuarios (creación, eliminación y modificación de cuentas de usuario y sus perfiles de acceso), configuración parámetros de contraseña, cambios a programas (ajustes normales y/o de emergencia), nuevos desarrollos de funcionalidad puestos en producción durante el período evaluado, gestión de casos de soporte, modificaciones directas a la base de datos, copias de respaldo y plan de contingencia.

EQUIPO AUDITOR

Mónica María Granados Cadavid – Jefe Ad-Hoc Oficina de Control Interno
Constanza Cárdenas Aguirre – Auditora de Sistemas.

METODOLOGIA APLICADA

Para el desarrollo de las pruebas, se aplicaron las técnicas de auditoría internacionalmente aceptadas tales como indagación, observación, inspección, revisión de registros y comprobación selectiva a través de muestreo, entre otros.

De acuerdo con la población, para cada prueba de auditoría a practicar se genera la muestra aleatoria objeto de evaluación con el Papel de Trabajo en Excel respectivo para el periodo objeto de evaluación definido.

MARCO NORMATIVO:

1. Procedimientos y Guías SIG:
   - ✓ Gestión de Servicios Administrativos y Tecnológicos (4233100-CR-033 v10 y v11)
   - ✓ Procedimiento Gestión de Incidentes, Requerimientos y Problemas Tecnológicos (PR-101 v14 y v15)
   - ✓ Guía Sistema de Gestión de Servicios (GS-044 v8, v9 y v10)
   - ✓ Guía Gestión de Usuarios (GS-038 v7)
   - ✓ Guía de gestión y administración de copias de respaldo (GS-036 V7 y v8)
   - ✓ Gestión de Cambios de TI (GS-111 v1)
   - ✓ Guía Metodológica para el desarrollo y mantenimiento de soluciones de software (GS-108 V1)
   - ✓ Guía de Arquitectura de Software para Soluciones Tecnológicas (GS006 V6)
   - ✓ Plan de Contingencia TI - DRP (PL-020 v7)
   - ✓ Circular 049 de 2007 - Uso adecuado de Internet y del correo electrónico en la Entidad
2. Manual de Políticas y Controles de Seguridad y Privacidad de la Información y Políticas de TI (4204000-MA-031) V7

   12.2 Organización de Seguridad de la Información
   12.3 Seguridad de los recursos Humanos
   12.4 Gestión de Activos
   12.5 Control de Acceso
   12.10 Adquisición, desarrollo y mantenimiento de Sistemas
   12.13 Aspectos de Seguridad de la Información de la Gestión de la Continuidad de Negocio
   10.4.8.6 Respaldo de la Información.
3. ISO 27001:2013 – Anexo de controles:

   A7 - Seguridad de los Recursos Humanos
   A8.3 Manejo de Medios
   A 8.1.1 Gestión por los Activos
   A9 - Control de Acceso
   A.12.1 Procedimientos operacionales y responsabilidades
   A.12.4 Registro y seguimiento
   A12.3 Copias de Respaldo
   A12.6 Gestión de la Vulnerabilidad Técnica

CONCLUSIÓN

Como resultado de la auditoría practicada a los Controles Generales de TI para el Sistema de Información PERNO, correspondiente al periodo objeto de evaluación comprendido entre el 1 de diciembre de 2024 y el 31 de mayo de 2025, se estableció que en términos generales de acuerdo con la práctica de pruebas seleccionadas al Sistema de Información se aplicó adecuadamente los controles definidos que mitigan la materialización de riesgos y soportan adecuadamente la gestión de acceso de usuarios al sistema de información, la gestión de cambios (despliegues en producción), las copias de respaldo a la base de datos y la gestión de los casos de soporte atendidos a través de la herramienta GLPI.

Se encontró que, los controles aplicados brindan un adecuado grado de efectividad, resaltando los siguientes aspectos:

1. Se cuenta con la normatividad vigente y actualizada con relación a los procedimientos y guías que establecen los controles generales de tecnología para los Sistemas de Información.

2. Para la creación de usuarios y asignación de roles para acceso al Sistema de Información PERNO, se requiere el diligenciamiento del formato FT-1000 con la aprobación del jefe de la dependencia a la que pertenece el colaborador y solo se realiza con una solicitud a través de la Mesa de Servicio OTIC (herramienta GLPI)

3. La OTIC cuenta con un control periódico para el bloqueo de usuarios que no han ingresado al Sistema de Información por más de 30 días. Así como, actividades de control definidas en la guía GS-038 de Gestión de Usuarios para la creación, depuración y asignación de roles a través de la Base de Datos.

4. Existencia de parámetros de seguridad de contraseña, con lo cual se fortalece el control de acceso al Sistema de Información PERNO, a través de los perfiles asignados en la Base de Datos a cada usuario (campo “profile”).

5. La base de datos PERNO hace parte de los procesos de copia de respaldo que se realizan periódica y automáticamente desde la OTIC, a través de la herramienta DataProtector, al igual, que se realizaron restauraciones de la base de datos por solicitud de la dependencia funcional. Al igual que se cuenta con proceso de copia de respaldo para la aplicación que reside en el repositorio GIT.

6. Se realizó en el mes de mayo 2025, el análisis de vulnerabilidades de los servicios donde se encuentran, entre otros, los sistemas de SAT WEB y PERNO; y la Oficial de Seguridad de la Información informó a los responsables de infraestructura y administrador de la base de datos sobre el plan de remediación que se encuentra en proceso de implementación de las medidas correctivas para tratar la vulnerabilidad encontrada y clasificada como criticidad Media – Exploitable.

7. Se tienen identificados los principales Activos de Información que soportan la infraestructura del Sistema de Información PERNO, como son: la base de datos y el aplicativo, asi como los riesgos de seguridad de la información y los controles correspondientes.

8. La OTIC implementó la guía Gestión de Cambios de TI (GS-111), que hace parte del procedimiento “Gestión para la Adquisición de Infraestructura Tecnológica, el desarrollo o adquisición de nuevas soluciones tecnológicas (PR-106)” como parte del fortalecimiento de los controles para los despliegues que se realizan a producción de los desarrollos y cambios a los Sistemas de Información.

9. El Sistema de Información PERNO, cuenta con dos manuales para su operación que son: el manual de usuario denominado “Manual del Usuario Convenio Interadministrativo SHD” y el manual técnico del Sistema de Personal y Nómina PERNO.

Se identificaron 3 observaciones, 2 oportunidades de mejora y se realizan algunas recomendaciones que al ser adoptadas propenderán por fortalecer y mejorar la efectividad de los controles y la dinámica de la operación del sistema de información PERNO como soporte tecnológico del proceso de Gestión de Nómina:

Observaciones:

1. Debilidades en la aplicación de controles para la administración de usuarios, asignación de roles de acceso y trazabilidad en las fechas de creación y bloqueo de usuarios, así:

   - Inoportunidad en la inactivación o bloqueo de usuarios en el aplicativo PERNO, cuando finalizan la relación laboral o contractual con la entidad o cuando ya no se requiere el acceso (rol asignado al usuario) debido a un cambio en las funciones o responsabilidades del colaborador. Si bien la OTIC realiza un bloqueo a los usuarios que no ingresan al aplicativo por más de 30 días, este no minimiza el riesgo de accesos no autorizados durante los 30 días o más en que se encuentra activo el usuario en el sistema de información PERNO.

- Roles asignados y activos para los usuarios PERNO (tanto activos como bloqueados en PERNO pero activos en la entidad) que no son requeridos para el desempeño de las labores de los colaboradores.

- Falta de trazabilidad de la fecha de creación de los usuarios con acceso al sistema de información PERNO, que fueron creados antes del proceso de migración de la BD Oracle que se realizó el 21/11/2025. Todos los usuarios creados antes del proceso de migración quedaron con registro de fecha de creación el 21/11/2025.

- En la política de control de acceso no se tiene definido el tiempo requerido para la desactivación de los usuarios de los Sistemas de Información

- El control de depuración periódica de usuarios por falta de conexión al sistema de información (30 días o más) se ejecutó mensualmente, sin embargo, se identificó que puntualmente para el mes de abril de 2025 no se aplicó el mencionado control de bloqueo de usuarios.

- Registro de novedades de funcionarios con un usuario genérico denominado RH, el cual no tiene un responsable definido y puede ser compartido, sin poder determinar responsabilidades de su uso en caso de requerirse**.**

Al respecto, de acuerdo con la respuesta recibida de la OTIC al informe preliminar, se precisa lo informado por dicha dependencia respecto a que: "*una vez un usuario se retira de la entidad; se eliminan sus accesos (via vpn) a los servicios que se encuentran internos; de esta manera, el usuario no podría ingresar al sistema así estuviera la clave activa por 30 días*".

2. Inoportunidad en la atención de los casos de soporte registrados en la herramienta GLPI por la Mesa de Servicio, incumpliendo los Acuerdos de Nivel de Servicio (ANS) establecidos y/o debilidades en la gestión de los casos para dar atención a los mismos en caso de requerir mayor tiempo para su solución.
3. Realización de cambios de información directamente sobre la Base de datos, sin contar con un registro de trazabilidad (log de auditoría) sobre la base de datos del ajuste realizado; al igual, que cambios de información (novedades de funcionarios) que pueden ser realizadas a través del aplicativo por la dependencia funcional, pero son registrados en la mesa de servicio para ser atendidos por la OTIC.

Oportunidades de Mejora:

1. Actualizar la circular 049 de 2007 de la SGAMB que establece lineamientos sobre bloqueo e inactivación de usuarios con acceso a la red, alineando lo allí definido con las actuales políticas de Seguridad de la Información (Manual de Políticas y Controles de Seguridad y Privacidad de la Información y Políticas de TI (4204000-MA-031)).

2. Mejorar la documentación en los casos de soporte GLPI, con el fin de contar con la trazabilidad completa de las situaciones presentadas durante la atención del caso y el registro de las acciones de seguimiento realizadas hasta su cierre. Se resalta que la OTIC realiza cuatrimestralmente control de verificación de la documentación y procesos continuos de capacitación a los colaboradores que atienden los casos de soporte GLPI.

Recomendaciones:

1. Fortalecer los controles en la administración de usuarios, alineados con las políticas de control de acceso definidas en el Manual de Políticas y controles de seguridad y privacidad de la información y políticas de TI (MA-031) y la Guía GS-038 Guía Gestión de Usuarios donde se define a la DTH como Gestor Funcional del aplicativo, de tal forma que se definan los tiempos para la inactivación o bloqueo de los usuarios en los Sistemas de Información y los tiempos de gracia en caso de requerirse por temas de servicio y cierre de las labores del colaborador retirado o con fin de contrato.

2. Aunque se cuenta con el control de bloqueo periódico de usuarios, realizado desde la OTIC cuando el usuario no ha ingresado al aplicativo por 30 días o más, es necesario dar cumplimiento al proceso de inactivación oportuna de los usuarios en PERNO cuando finalizan la relación laboral o contractual con la entidad, o cuando ya no requieren el acceso debido a cambio en las funciones o responsabilidades dentro del proceso.

3. Fortalecer el control de desactivación de los usuarios en los Sistemas de Información, alineado y paralelamente a la inactivación del usuario que se realiza en el Directorio Activo, cuando se finaliza la relación laboral o contractual con la entidad, dando cumplimiento a lo establecido en la guía GS-038 de Gestión de Usuarios.

3. Fortalecer el control de acceso al sistema de información, con la definición de los roles de acceso en el aplicativo asociándolos y relacionándolos con los cargos/responsabilidades de los funcionarios para

la operación del proceso de Gestión de Nómina y/o contabilización en los procesos financieros de la Entidad.

4. Fortalecer el proceso de cambios directo a datos, y evaluar la posibilidad de que sean gestionados bajo una tipificación de cambios en producción y sean aprobados a través del Comité de Cambios e incluyendo este tipo de cambios en la guía de gestión de cambios (GS-111), con un análisis de tiempos de atención vs la necesidad de contar con la oportunidad de atención de los requerimientos de gestión de nómina. Asimismo, analizar los casos atendidos por la OTIC y que pueden ser gestionados desde la dependencia funcional e identificar si existen falencias en el manejo del aplicativo con el fin de fortalecer los procesos de capacitación y transferencia de conocimiento a quienes deben ingresar novedades de nómina.

5. Evaluar la posibilidad de implementar el log de auditoría sobre la base de datos, específicamente para los cambios realizados directamente sobre la base de datos e implementar monitoreo periódico sobre las acciones que realizan los administradores directamente sobre la base de datos y no a través del aplicativo.

6. Dar continuidad al proyecto de implementación del Plan de contingencia Tecnológico (que de acuerdo con lo informado por la OTIC hace parte del proyecto 8110 – Fortalecimiento de las Tecnologías de la Información y las Comunicaciones), asegurando incluir la infraestructura del Sistema de Información PERNO como parte de las pruebas integrales de contingencia tecnológica que se tengan planeadas según las etapas del proyecto, con el fin de determinar los tiempos de recuperación ante los diferentes eventos que se pudiesen presentar de inoperatividad y asegurar la continuidad de la operación del proceso de gestión de nómina.

7. Evaluar en detalle los riesgos que potencialmente pueden materializarse para las vulnerabilidades categorizadas en criticidad “media” como resultado del análisis de vulnerabilidades de la infraestructura SAT WEB (PERNO), con el fin de definir si alguna requiere plan de remediación. Así como definir formalmente el criterio para priorizar y atender las vulnerabilidades identificadas cuando se realiza el análisis de vulnerabilidades a los Sistemas de Información.

8. Revisar los tiempos que se definen entre la detección y el cierre de las vulnerabilidades en los Sistemas de Información, considerando que para el cierre de la vulnerabilidad detectada para PERNO, se realizará el cierre en el mes de septiembre (cuatro (4) meses después de ser detectada) y, de ser posible dar prioridad a la gestión del plan de remediación ya definido por parte de la OTIC.

9. Revisar la normatividad vigente asociada a controles generales de TI para los Sistemas de información, en especial los documentos con fecha de publicación en Daruma entre agosto 2022 y mayo 2023.

10. Actualizar el manual técnico en los roles de acceso al sistema de información, y asegurar que el manual publicado en Daruma se encuentra actualizado con la versión final de marzo 2025. De otra parte, realizar sesiones de sensibilizaciones al interior de las dependencias que son usuarias del sistema de información PERNO, en especial a los funcionarios de la DTH y de la SF, quienes interactúan constantemente con el Sistema de Información en su labor diaria.

11. Alinear los nombres de las cuentas de usuario entre el sistema de información PERNO y el Directorio Activo y fortalecer el control de depuración de usuarios que actualmente se aplica desde la OTIC como área que administra los usuarios del Sistema de Información. Adicionalmente, evaluar la posibilidad de integrar el control de acceso del Sistema de Información PERNO con el Directorio Activo.

12. Ajustar el perfil por defecto para control de contraseña, de los usuarios que aún no tiene asignado el perfil denominado “TIEMPO_LIMITE”, para que en caso de activar el usuario se mitigue el riesgo de asignación de contraseñas débiles por parte de los usuarios.

Criterios de clasificación de conceptos derivados de la auditoría

Tipo de observación	Descripción
Observación	Incumplimiento de normas o procedimientos internos que pueden materializar un riesgo.
Oportunidad de mejora	Sin implicar un incumplimiento normativo o de procedimientos internos, es susceptible de mejora el proceso.

Elaborado por: Constanza Cárdenas Aguirre – Contratista, Auditora de Sistemas
Revisado y Aprobado por: Mónica María Granados Cadavid – Jefe Ad-Hoc Oficina de Control Interno