INFORME FINAL
Auditoría de Gestión – Controles Generales de TI
Sistema de Información de Victimas SIVIC

PERIODO DE EJECUCION

Entre el 27 de marzo y 16 de mayo 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 Victimas SIVIC.

OBJETIVO GENERAL

Establecer la existencia, aplicabilidad y efectividad de los controles generales de Tecnología para el Sistema de Información SIVIC, que permitan asegurar la confidencialidad, integridad y disponibilidad de la información.

ALCANCE

Se evaluaron los controles generales de tecnología en el Sistema de Información SIVIC, 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

Jorge Eliecer Gómez Quintero - Jefe Oficina de Control Interno (1 al 8 de Abril 2025)
María Jazmin Gómez Olivar – Jefe (E) Oficina de Control Interno (a partir del 9 de abril 2025)
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 para la adquisición de infraestructura tecnológica, el desarrollo o adquisición de nuevas soluciones tecnológicas (PR-106 V16)
   - ✓ Gestión de Cambios de TI (GS-111 v1)
   - ✓ 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

   12.3 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
   A12.3 Copias de Respaldo
   A12.6 Gestión de la Vulnerabilidad Técnica

CONCLUSION

Como resultado de la auditoría practicada a los Controles Generales de TI para el Sistema de Información SIVIC, correspondiente al periodo objeto de evaluación comprendido entre el 1 de octubre de 2024 y el 31 de marzo 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 grado de efectividad, resaltando los siguientes aspectos:

- 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.

- La OCDPVR cuenta con controles para la gestión y depuración de los usuarios con acceso al Sistema de Información SIVIC. Asimismo, se cuenta con una matriz de equivalencia de perfiles de acceso del Sistema de Información con relación a los perfiles misionales existentes para la operación del proceso de Victimas, Paz y Reconciliación.

- Se implementaron funcionalidades en el Sistema de Información, que permiten realizar cambios de información en la base de datos, a través de una interfaz gráfica y dejando trazabilidad de la acción realizada, para las modificaciones de “desmonte de medidas de ayuda”.

- La base de datos SIVIC hace parte de los procesos de copia de respaldo que se realizan periódicamente y automáticamente desde la OTIC, a través de la herramienta DataProtector.

- Se realizó en el año 2024, análisis de vulnerabilidades para el Servicio del Sistema de Información SIVIC y se implementaron medidas correctivas para una vulnerabilidad clasificada con criticidad Alta.

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

- 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.

- El Sistema de Información SIVIC, cuenta con dos manuales para su operación que son: el manual de usuario del Sistema y el manual técnico de Instalación, Configuración y Despliegue del aplicativo en producción.

Se identificaron 4 observaciones, 3 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 SIVIC como soporte tecnológico del proceso de Paz, Victimas y Reconciliación:

Observaciones:

1. Debilidades en la aplicación de los controles para la depuración e inactivación de usuarios y perfiles de acceso al sistema de información.

2. Usuarios creados en el Sistema de Información SIVIC sin la documentación soporte de solicitud y aprobación según lineamientos y políticas existentes en la Entidad.

3. Inoportunidad en la atención de los casos de soporte registrados en la herramienta GLPI por la Mesa de Servicio.

4. Realización de cambios de información directamente sobre la Base de datos y no a través de una interfaz gráfica del aplicativo, sin contar con un registro de trazabilidad (log de auditoría) sobre la base de datos del ajuste realizado.

Oportunidades de Mejora:

1. Implementar parámetros de seguridad de contraseña para fortalecer los controles de acceso del Sistema de Información SIVIC.

2. Mejorar la documentación en los casos de soporte, 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.

3. Planificar una prueba de contingencia tecnológica para SIVIC, que permita evaluar la efectividad del Plan de Contingencia de TI para la infraestructura que soporta este sistema de información, con el fin de determinar los tiempos de recuperación ante los diferentes eventos que se pudiesen presentar de inoperatividad, así como confirmar que el Manual de Instalación, Configuración y Despliegue para el aplicativo SIVIC aplica en caso de requerirse la instalación total del aplicativo.

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 OCDPVR como Gestor Funcional del aplicativo.

2. Alinear la atención de los casos de soporte GLPI del Sistema de Información SIVIC, con los controles establecidos en el procedimiento PR-101 Gestión de incidentes, requerimientos y problemas tecnológicos y de la guía GS-044 Sistema de Gestión de Servicios.

3. 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 a la población víctima.

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

5. Evaluar en detalle los riesgos que potencialmente pueden materializarse para las vulnerabilidades categorizadas en criticidad “media” como resultado del análisis de vulnerabilidades del servicio SIVIC, con el fin de definir si alguna requiere plan de remediación. Asi como definir formalmente el criterio para priorizar y atender las vulnerabilidades identificadas cuando se realiza el análisis de vulnerabilidades a los Sistemas de Información.

6. Evaluar la infraestructura de contingencia con que se cuenta actualmente en la entidad, con un análisis de costo/beneficio y estudiar las diferentes opciones para asegurar los tiempos de restablecimiento de la plataforma tecnológica y asegurar la continuidad de la operación del proceso de Victimas, Paz y Reconciliación, en caso de la ocurrencia de un evento o la materialización de un riesgo de TI que afecte el funcionamiento correcto del Sistema SIVIC, categorizado como crítico en el documento actual de Plan de Contingencia.

7. Planificar una prueba de contingencia tecnológica que permita evaluar la efectividad del Plan de Contingencia de TI para la infraestructura que soporta SIVIC, determinar los tiempos de recuperación ante los diferentes eventos que se pudiesen presentar de inoperatividad, así como confirmar que el Manual de Instalación, Configuración y Despliegue para el aplicativo SIVIC aplica en caso de requerirse la instalación total del aplicativo.

8. 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 e incluir la revisión de lo normado en la Circular 049 de 2007 de la SGAMB, sobre el uso adecuado de internet y del correo electrónico en la entidad, que incluye lineamientos sobre la desactivación de cuentas con acceso a la red de la Entidad.

9. Realizar la revisión y actualización de los manuales de usuario y de instalación de SIVIC, así como en coordinación con el área de planeación, identificar si fuese necesario su publicación según los lineamientos establecidos por dicha dependencia. Al igual que, realizar sesiones de sensibilizaciones al interior de la OCDPVR, en especial a los funcionarios que interactúan constantemente con el Sistema de Información en su labor diaria.

Adicionalmente, tomando en consideración lo informado por la OTIC en memorando No. 3-2025-13288 del 29/05/2025 (respuesta al informe preliminar de esta auditoría), se resalta la importancia de fortalecer los controles para el sistema de información SIVIC, como parte de las actividades que se realizarán desde la Dirección de Reparación Integral, a través del proceso de contratación que actualmente se adelanta orientado a la *"evaluación integral del Sistema de Información de Víctimas de Bogotá (SIVIC) para la Oficina Consejería Distrital de Paz, Víctimas y Reconciliación (OCDPVR), con el fin de mejorar la gestión en la atención de las víctimas, la coordinación y articulación de las entidades del orden nacional y territorial que conforman el Sistema Nacional de Atención y Reparación Integral a las Víctimas".*

OBSERVACIONES, OPORTUNIDADES DE MEJORA Y RECOMENDACIONES PRODUCTO DE LAS PRUEBAS PRACTICADAS

Para el desarrollo de la auditoría de gestión a los controles generales tecnológicos para el Sistema de Información de Victimas SIVIC, se realizaron pruebas en línea y análisis de los soportes recibidos de la aplicación de controles para el sistema de información SIVIC: 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.

A continuación, se describen los principales aspectos evaluados, las observaciones y oportunidades de mejora identificadas y las recomendaciones formuladas como resultado de las pruebas practicadas:

1. Actualización y publicación de Normatividad Asociada a Controles Generales de TI

Se identificaron los siguientes documentos donde se definen los controles generales de Tecnología para los Sistemas de Información, observando que los documentos se encuentran vigentes y debidamente publicados en la herramienta Daruma con actualizaciones entre julio 2022 y enero 2025.

Se recomienda para los cuatro (4) documentos con fecha de publicación entre agosto 2022 y mayo 2023, realizar revisión con el fin de garantizar que continúan vigentes y acorde con los controles que se encuentran operativos actualmente en la dinámica de la operación del proceso Gestión de Servicios Administrativos y Tecnológicos, específicamente en lo referente a Tecnología. Los cuatro documentos son: Guía Gestión de Usuarios (GS-038), Guía Metodológica para el desarrollo y mantenimiento de soluciones de software (GS-108), Guía de Arquitectura de Software para Soluciones Tecnológicas (GS-006) y Plan de contingencia TI – DRP (PL-020).

2. Administración de usuarios del Sistema de Información de Victimas SIVIC

Una vez analizado el listado de usuarios existentes en el aplicativo SIVIC, se tiene un total de 909 usuarios en el Sistema de Información (172 en estado activo y 737 inactivos). Una vez realizado el análisis de los 172 usuarios en estado “activo” con relación a los funcionarios y/o contratistas activos en la entidad, retirados y vigentes en el Directorio Activo, se identificó que la OCDPVR, como área funcional del Sistema de Información, administra los usuarios para el acceso, observando lo siguiente:

- 104 usuarios activos en el Sistema de información con acceso vigente tanto en SIVIC como en el Directorio Activo.

- 2 usuarios genéricos activos en SIVIC e inexistentes en DA, asignados a usuarios externos, que realizan entregas de ayudas a las víctimas del conflicto armado.

Para los usuarios restantes, las siguientes son las situaciones de auditoría evidenciadas con respecto a la gestión de usuarios y configuración de parámetros de seguridad para contraseña de acceso:

Observación No. 1 – Debilidades en la aplicación de los controles para la gestión de usuarios con acceso al Sistema de Información SIVIC

1. Existen 63 usuarios en estado activo en SIVIC pero que en el Directorio Activo se encuentran inactivos (estado = false), lo que significa que no son colaboradores activos en la entidad. Si bien el no contar con acceso al Directorio activo, mitiga el riesgo de accesos no autorizados, potencialmente se podría materializar considerando que el control de acceso del sistema de información no está integrado con el Directorio Activo, además esto evidencia falta de integridad entre ambos sistemas (DA y SIVIC).

2. Treinta (30) de 172 usuarios activos en el aplicativo SIVIC (17%), corresponden a colaboradores que ya no tienen una relación laboral o contractual vigente con la entidad, de manera que no fueron inactivados de forma oportuna

3. Un (1) usuario identificado en SIVIC con el número de cédula diferente al número registrado en el Directorio Activo, evidenciando falta de integridad entre la información de usuarios registrada en SIVIC y la registrada en el Directorio Activo.

4. Un (1) usuario sin relación contractual vigente con la entidad, que si bien cuenta con el formato FT-1000 y la pantalla SECOP del contrato firmado en el mes de enero 2025, el mismo fue cedido, de manera que es un usuario que debería estar inactivo en SIVIC.

5. Seis (6) usuarios (5 de ellos en estado activo y 1 en estado inactivo en SIVIC), que presentaron ingreso al Directorio Activo en fecha posterior a su retiro de la entidad, y no es posible evidenciar acceso al Sistema de Información SIVIC debido a que no se cuenta con este registro en la base de datos.

6. De una muestra de 24 usuarios, se identificaron dos (2) que no pertenece a la OCDPVR sino a las dependencias: Dirección del Sistema de Servicio a la Ciudadanía y a la Subdirección Técnica de Desarrollo Institucional, por lo que se debe revisar si existen más usuarios bajo estas condiciones y que todos los accesos con usuario activo en el sistema de información SIVIC, lo requieran y los perfiles de acceso estén acorde con las tareas que realiza el colaborador.

7. No se evidenciaron soportes que dieran cuenta de la aplicación del control de depuración de usuarios que se venía desarrollando periódicamente como parte del proceso de administración de usuarios que se realiza desde la dependencia OCDPVR, con rol de administrador funcional del sistema de información.

Lo anterior en cumplimiento a lo establecido en:

- Manual de Políticas y controles de seguridad y privacidad de la información y políticas-de-TI (MA-031) en sus numerales:

  12.3.3 Terminación y/o cambio de empleo, en el tercer párrafo, que establece: "*Los retiros de los permisos del personal vinculado de manera directa por la entidad o los contratistas o proveedores son informados a la Oficina de Tecnologías de la Información y las Comunicaciones – OTIC a través del documento de Paz y Salvo emitido en el momento de la finalización de la relación contractual para con la Entidad."*

  12.5.1 Política para control de acceso que dice: "*La Secretaría General llevará a cabo una revisión sobre el control de acceso a través de la validación y verificación de solicitudes sobre las novedades relacionadas con usuarios que sean informadas por la Dirección de Talento Humano y/o la Dirección de Contratación acorde con la vinculación o desvinculación del personal a la Entidad, para tal efecto, se aplicará lo indicado en los documentos: 2211200-PR-156 Contratación Directa y 2211300-PR-221 Gestión Organizacional.*"

  En el mismo numeral se relacionan las *Responsabilidades de la Administración,* entre otras, se mencionan las siguientes:
  "…
  - *Es responsabilidad de los propietarios de los activos realizar revisiones periódicas y depuraciones de los accesos asignados a las cuentas de usuarios a intervalos regulares.*

- *Para las dependencias que cuentan con sistemas de información y su administración, es responsabilidad de cada una de ellas mantener y garantizar el control de acceso de usuarios sobre estos sistemas y sus respectivas bases de datos.*
- *En caso de que existan identificadores de usuarios genéricos en cualquier sistema operacional, base de datos, o aplicación, deben estar debidamente individualizados los responsables de estos*

"

En el mismo numeral 12.5.1 - Política para control de acceso, en la sección titulada "*Respecto al acceso a sistemas y aplicaciones*", se establece que: "*La creación de usuarios de ciertos aplicativos se encuentra a cargo de los líderes funcionales o la dependencia que administre o tenga el control correspondiente del aplicativo*."

- Guía GS-038 - Guía Gestión de Usuarios, que en su numeral 11. RECOMENDACIONES PARA LA GESTIÓN DE USUARIOS EN PORTALES Y SISTEMAS DE INFORMACIÓN, menciona las siguientes recomendaciones:

  - *"Realizar la revisión periódica (mínimo cada 3 meses) del estado o vigencia de los usuarios para determinar cuales se deben bloquear o eliminar. En esta validación se debe tener en cuenta el tipo de permisos de acuerdo con los roles y responsabilidades de los usuarios*
  - *Validar los últimos inicios de sesión y los usuarios que no hayan accedido al sistema de información, sitio o página o portales web, en los últimos 90 días sean bloqueados."*

- ISO 27001:2013 control A.9.2 Gestión de acceso de usuarios, A.9.2.1 Registro y cancelación de registro de usuarios, A.9.2.5 Revisión de los Derechos de acceso de usuarios: "*Los propietarios de los activos deben revisar los derechos de acceso de los usuarios, a intervalos regulares"* y A.9.2.6 Retiro o ajuste de los derechos de acceso.

Dadas las situaciones anteriormente planteadas, se recomienda:

- Revisar los accesos de dichos usuarios posteriormente a la fecha de retiro o desvinculación de la entidad con el fin de asegurar que no se hayan realizado operaciones no autorizadas en el sistema con dichos usuarios.
- Realizar una revisión y actualización de información de los usuarios, tanto en el sistema de información SIVIC como en el Directorio Activo.

- Evaluar la posibilidad de implementar control de acceso del aplicativo SIVIC integrado con el Directorio Activo.
- Aplicar de inmediato el control de revisión y depuración de usuarios en el Sistema SIVIC, asegurando que todos los usuarios activos tengan una relación laboral o contractual con la entidad, y que su perfil de acceso esté alineado con sus responsabilidades dentro del proceso.

Recomendación No. 1

Respecto de las cuentas que se encontraron con ingreso al Directorio Activo luego de la desvinculación del colaborador pero que estaban dentro del periodo de gracia de ocho (8) días posteriores a la desvinculación con la entidad, según lo normado en la circular 049 de 2007 que dice: *"Las cuentas de correo y acceso a la red serán desactivadas después de un periodo de 8 días a partir de la fecha en la cual la persona termine oficialmente su vinculación con la entidad o cuando la dependencia o el proyecto dejen de existir o por solicitud del Jefe de Área o Dependencia correspondiente(...)*", se recomienda revisar esta normatividad integralmente con el Manual de Políticas y Controles de Seguridad y Privacidad de la Información y Políticas de TI (4204000-MA-031), con el fin de actualizar y detallar la política del uso de usuarios posterior a su desvinculación con la entidad.

Observación No. 2 – Usuarios creados en SIVIC sin el soporte requerido

Para una muestra de veintiuno (21) usuarios creados durante el período evaluado, diez (10)(48%) registran soporte de solicitud y aprobación para la creación del usuario, nueve (9) (43%) no cuentan con un soporte de solicitud y aprobación para la creación del usuario (caso de soporte GLPI en mesa de ayuda y/o formato FT-1000) y dos (2) aunque tienen formato de solicitud, en la misma no se específica que se requiere acceso a SIVIC, lo cual, no está alineado a lo establecido en la guía GS-038 Guía Gestión de Usuarios.

De otra parte, es observaron dos (2) usuarios activos en SIVIC que no existen en el Directorio Activo y no se observa que tengan relación laboral o contractual vigente con la entidad, que de acuerdo con lo informado por la OCDPVR son usuarios creados bajo los casos de soporte GLPI 274986 y 353785 y están asignados a operadores externos, razón por la cual no requieren tener usuarios en el Directorio Activo porque son empresas que dan el servicio a la consejería de víctimas, pero registran información en el sistema SIVIC.

Con relación a estos dos (2) usuarios externos, se observó que no cuentan con un soporte de aprobación para la creación del usuario, y solo uno (1) de ellos cuenta con un archivo Excel (control de la ODCPVR) como soporte de la creación del perfil en el aplicativo SIVIC. Por lo tanto, se recomienda que, para la creación de usuarios externos, se aplique el control del formato FT-1000 o soporte similar y se adjunte el soporte de la relación vigente del operador externo con la entidad (contrato / convenio).

Lo anterior incumple los siguientes criterios:

- Manual de Políticas y controles de seguridad y privacidad de la información y políticas-de-TI (MA-031) en sus numerales:

  12.5.1 Política para Control de Acceso, en el título "Respecto al Registro y Cancelación de Usuarios", que dice: "*Para las novedades relacionadas con registro y cancelación de usuarios se debe solicitar autorización al jefe inmediato o supervisor del contrato realizando el diligenciamiento del formato **4204000-FT-1000 Solicitud de Servicios TIC"***

  En la sección con título "*Respecto al acceso a sistemas y aplicaciones*" del mismo numeral 12.5.1 Política para control de acceso, que dice: *"La creación de usuarios de ciertos aplicativos se encuentra a cargo de los líderes funcionales o la dependencia que administre o tenga el control correspondiente del aplicativo".*

- Guía GS-038 Guía Gestión de Usuarios, que en su numeral 6. Gestión de Usuarios Sistemas De Información, Aplicaciones Y Portales No Administrados por la Oficina TIC, dice: "*En caso de solicitar usuarios en otros sistemas de información, portales o aplicaciones, el usuario deberá escalar la solicitud a través de una comunicación formal y debidamente diligenciado el formato de solicitud de servicios TIC Secretaría General 4204000-FT- 1000 Solicitud de servicios TIC Secretaría General indicando los servicios requeridos para que el usuario desarrolle sus funciones, firma de solicitante y jefe de dependencia; lo anterior dirigido a la dependencia funcional que corresponda de acuerdo con la tabla (Anexo 01)".*

  En el anexo 01 de la guía se relaciona a la Oficina Alta Consejería de Paz, Víctimas y Reconciliación como Gestor Funcional de Sistema de información de víctimas del Distrito Capital-SIVIC.

Por las situaciones antes expuestas, es necesario que, la OCDPVR como gestor funcional del Sistema de Información, en coordinación con la OTIC, se realicen los ajustes correspondientes y se fortalezcan

los controles y se dé cumplimiento a los lineamientos establecidos en los diferentes documentos asociados al control de acceso como son el Manual de Políticas y controles de seguridad y privacidad de la información y políticas de TI (MA-031) y Guía Gestión de Usuarios (GS-038).

Recomendación No. 2

Código User ID de identificación de usuario en SIVIC diferente al del Directorio Activo

De los 168 usuarios activos en SIVIC que cuentan con usuario en el Directorio Activo, se identificaron 22 (13%) que tienen el mismo nombre de usuario (user id) en ambos sistemas y 146 (87%) que la identificación de usuario registrada en SIVIC difiere con la del Directorio Activo.

Si bien no es requerido que el nombre de identificación de los usuarios en el Sistema de Información sea igual al del Directorio Activo, por integridad de información, estándar, trazabilidad y como mejor práctica de seguridad, se recomienda alinear estos nombres entre ambos sistemas de información y fortalecer el control de depuración de usuarios que actualmente se aplica desde la OCDPVR como área que administra funcionalmente el Sistema de Información.

Se recomienda evaluar si es factible integrar las credenciales de acceso del Sistema de Información SIVIC con el Directorio Activo, tomando en consideración el impacto que esto pudiese tener en la oportuna atención a los ciudadanos (población víctima), en caso de presentarse fallas con el DA.

Oportunidad de Mejora No. 1 – Falta de configuración de parámetros de seguridad para la contraseña de acceso al sistema de información

En prueba realizada en línea, ingresando al link https://sivic.alcaldiabogota.gov.co/Sivic, se evidenció que el sistema de información no cuenta con parámetros de contraseña para dar seguridad en el acceso al sistema; es decir, que no exige la configuración mínima de contraseña como es: mínimo un tamaño de 8 caracteres y combinación de una mayúscula, una minúscula, un número y un carácter especial, y tampoco bloquea al usuario luego de intentar varias veces seguidas el ingreso con contraseña errada.

Aunque estos parámetros de seguridad no se encuentran establecidos como exigencia para ser configurados en los Sistemas de Información, la política de acceso en su sección de “Responsabilidades de los Usuarios” (Manual MA-031 numeral 12.5.1 – Política para control de acceso) relaciona los lineamientos para la construcción de contraseñas seguras.

Por lo tanto, se recomienda implementar la configuración de contraseña, según mejores prácticas de seguridad, para que el sistema de información controle automáticamente aspectos como: - cambio de contraseña al primer ingreso del usuario, exigencia de cambio de contraseña en intervalos de tiempo regulares y la construcción de contraseñas seguras que incluyan como mínimo: 1 carácter especial, 1 carácter en Mayúscula, 1 carácter numérico, longitud mínima de 8 Caracteres, así como, bloqueo por no utilización del usuario en un tiempo establecido y bloqueo del usuario por cantidad de intentos fallidos de acceso al aplicativo. Aspectos que al ser controlados automáticamente por el Sistema de Información fortelecen los controles de acceso y minimizan los potenciales riesgos de accesos no autorizados.

Lo anterior de acuerdo con lo establecido en:

- Manual de Políticas y controles de seguridad y privacidad de la información y políticas-de-TI (MA-031), numeral 12.5.1 - Política para Control de Acceso, que en su título "responsabilidades de los usuarios", dice: "…A continuación, se detallan los siguientes lineamientos a tener en cuenta: …- Cambiar la contraseña en intervalos de tiempo regulares, Construir contraseñas seguras que incluyan como mínimo: 1 carácter especial, 1 carácter en Mayúscula, 1 carácter numérico, Debe contener una longitud mínima de 8 Caracteres…"

- Manual de Usuario SIVIC, que en su página 15, dice: **"…***Se diligencian los datos de la matriz de creación de usuario que viene en el caso de GLPI, el "Loguin" se asigna con la primera letra del primer y segundo nombre, el primer apellido y la primera letra del segundo apellido, la* ***clave*** *inicial se puede asignar por un gestor de contraseñas o cumpliendo las* ***políticas de seguridad:*** *Longitud de 8* ***caracteres****, una* ***minúscula****, una* ***mayúscula*** *y un* ***carácter especial*** *(Ejemplo: Nrojas*4756)…"*

- ISO 27001, el control A.9.4.3 – Sistema de Gestión de Contraseñas *"Los sistemas de gestión de contraseñas deben ser interactivos y deben asegurar la calidad de las contraseñas".*

3. Casos de Soporte GLPI registrados en la Mesa de Servicio para el Sistema de Información SIVIC

Revisados los casos de soporte para SIVIC registrados en la herramienta GLPI de la Mesa de Servicio, entre el 1/10/2024 al 31/03/2025, se evidenciaron seis (6) categorías para el Sistema de Información SIVIC con sus correspondientes ANS definidos.

A continuación, las situaciones de auditoría observadas:

Observación No. 3 - Inoportunidad en la atención de los casos según los ANS establecidos

En relación con el cumplimiento de los ANS establecidos para las categorías del sistema de gestión de servicios GLPI, para una población de 334 casos de soporte SIVIC, registrados durante el periodo evaluado, se observó que 243 (73%) de los casos registrados, cumplieron los ANS establecidos.

No obstante, se identificaron las siguientes situaciones:

- En 76 (23%) de los casos de soporte registrados se incumplieron los ANS establecidos.

- Tres (3) casos cerrados sin estar solucionados y se reabren en uno nuevo, con el riesgo de perder la trazabilidad para la atención o seguimiento del cumplimiento de los ANS puesto que en ocasiones no se deja la trazabilidad de esta situación. Por ejm: 344716, 350824 y 364037.

- Veintitrés (23) casos mal categorizados (7%), de los cuales 17 (5%) se categorizaron como "SISTEMAS DE INFORMACIÓN > Sistema de Información SIVIC" sin una asociación a alguna de las subcategorías existentes como son: Fallas SIVIC, Nuevos Desarrollos, Modificación de Servicios, Gestión de Usuarios, y los seis (6) restantes, es decir el 1.8%, se clasificaron en "modificación de servicios", "nuevos desarrollos (actualizaciones)" o "gestión de usuarios" correspondiendo a una subcategoría diferente

Lo anterior, incumpliendo lo establecido en:

- Guía Sistema de Gestión de Servicios (GS-044), numeral 3.1 Objetivos específicos "*Cumplir con los niveles de servicio (ANS) acordados.*"

- Procedimiento PR-101 – Gestión de incidentes, requerimientos y problemas tecnológicos, actividad 10 - Elaborar y presentar informe del Sistema de Gestión de servicios, que dice: … *Realiza seguimiento a los servicios de forma semanal con fin de dar cumplimiento a los ANS establecidos*."

Dado lo anterior, es necesario alinear las actividades de atención de los casos de soporte GLPI del Sistema de Información SIVIC, a las actividades y controles establecidos en el procedimiento PR-101 Gestión de incidentes, requerimientos y problemas tecnológicos y de la guía GS-044 Sistema de Gestión de Servicios.

Oportunidad de Mejora No. 2 – Documentación incompleta o inadecuada para el cierre de los casos de soporte GLPI

Para una muestra de 22 casos GLPI, se revisó la documentación y solución dada para el cierre del caso de soporte, evidenciando siete (7) casos (32%) con documentación y trazabilidad completa de la solución y soportes que dan cuenta de las acciones realizadas para la gestión respectiva y, 15 casos (68%) que no cuentan con la documentación completa que permita tener trazabilidad de las acciones realizadas, como por ejm: soporte de los VoBo para la modificación de datos, pantallas de evidencia de las modificaciones realizadas en la Base de datos, entre otros.

Al respecto y de acuerdo con la actividad 7- Verificar la documentación de la solución, del procedimiento PR-101 Gestión de incidentes, requerimientos y problemas tecnológicos, se identificó que la OTIC realiza esta actividad para el 5% de los servicios que se atienden por dicha dependencia y debido a que los casos de soporte para SIVIC son atendidos por la OCDPVR, los mismos no están siendo objeto de la actividad de monitoreo que se realiza por la OTIC.

Las situaciones mencionadas de acuerdo con lo establecido en:

- Procedimiento Gestión de incidentes, requerimientos y problemas tecnológicos (PR101), actividad 7 - Verificar la documentación de la solución, que dice: "*El profesional de la Oficina TIC selecciona una muestra del 5% de los servicios en estado Resuelto y Cerrado donde se verifica si lo registrado en las pestañas (seguimientos, solución y documentos), son coherentes con la solicitud del usuario, el procedimiento y los protocolos respectivos. 1.En todos los casos de la muestra seleccionada, debe verificarse la conformidad de la documentación de la solución registrada en el sistema de gestión de servicios."*

- *Actividad 6 - Solucion y documentación de la solicitud,* que dice*: "…Registra en la sección correspondiente a "Solución", una explicación clara de cómo se realizó el proceso."*

Dado lo anterior, se recomienda que en el OCDPVR, dependencia que atiende los casos de soporte para SIVIC en el nivel 2 de atención, se implemente la actividad de seguimiento para verificar la documentación de la solución acogiéndose a la actividad 7- Verificar la documentación de la solución establecida en el procedimiento PR-101 Gestión de incidentes, requerimientos y problemas tecnológicos.

Observación No. 4 – Ajustes directos realizados en producción a la base de datos

Se observaron algunos casos de cambios realizados por la OCDPVR que no se realizan a través de una interfaz gráfica por el aplicativo, sino que se realizan directamente sobre la base de datos, para los que se cuenta con trazabilidad a través del GLPI; no obstante, no existe soporte de trazabilidad (log de auditoría) en la Base de Datos. Asimismo, se identificó que siendo un cambio directo sobre la base de datos no hacen parte de los cambios gestionados a través del Comité de Cambios implementado desde la OTIC (guía GS-111 – Gestión de Cambios), situación que genera riesgos de cambios no autorizados sobre la base de datos y dificultad para realizar seguimiento a los mismos, debido a que la base de datos no tiene políticas configuradas para conservación y administración de registros de logs de auditoría dificultando identificar todos los cambios a datos realizados durante el periodo evaluado.

Al respecto, la OTIC informó que: "*Actualmente, el sistema de víctimas no cuenta con una funcionalidad implementada de trazabilidad a nivel de base de datos que permita registrar de forma automática y detallada las transacciones realizadas mediante comandos como UPDATE, DELETE u otras operaciones que impliquen modificación directa de la información*".

Se identificaron diez (10) cambios en GLPI que se realizaron directamente sobre la Base de Datos, categorizados en la herramienta GLPI como "Modificación de Servicios" pero que no se realizan a través del aplicativo, uno de ellos puntual y que actualmente no se realiza relacionado con la división del nucelo familiar.

Se recomienda fortalecer el proceso de cambios directo a datos que se realiza actualmente, 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 incluir 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 a la población víctima.
Evaluar la posibilidad de implementar el log de auditoría sobre la base de datos, específicamente para los cambios directos a datos realizados e implementar monitoreo periódico sobre las acciones realizadas de cambios directamente sobre la base de datos y que no se hacen a través de la interfaz gráfica del aplicativo.

4. Plan de contingencia y copias de respaldo

Se observó la publicación en Daruma del documento denominado “Plan de Contingencia TI – DRP V7 (PL-020)” con fecha de publicación 19/01/2023, el cual contiene: roles y responsabilidades, estado actual de la infraestructura de la SGAMB, Sistemas de Información Críticos que soportan la operación de la Entidad, Fase reducción de riesgos, Monitoreo, estrategia plan de contingencia, plan de continuidad de operaciones, entre otros. Documento que en la sección 7. Sistemas de Información Críticos se relaciona el Sistema de Información SIVIC, y que de acuerdo con lo informado por la OTIC, este documento se encuentra en proceso de actualización.

Con respecto a las copias de respaldo, se realizaron pruebas para verificar la configuración para la toma periódica del backup de la base de datos, evidenciando que en la herramienta Data Protector se encuentra debidamente configurado para toma de copias de respaldo diaria, semanal y mensualmente de la Base de Datos SIVIC. Asimismo, se realizó prueba de restauración de la copia de respaldo de la base de datos al corte diciembre 2024, observando que el proceso terminó satisfactoriamente.

Oportunidad de Mejora No. 3 – Sistema de información SIVIC sin pruebas de efectividad del Plan de Contingencia ni plan de restauración de copias de respaldo

Referente al Plan de Contingencia para la recuperación de la infraestructura ante cualquier falla o evento inesperado tecnológico, aún no se cuenta con este plan de contingencia debidamente implementado, generando debilidad de control para la entidad, en el sentido que permita dar continuidad a la operación en caso de materialización riesgos por daños en la infraestructura tecnológica que soporta el Sistema de Información SIVIC, fallas en la aplicación o daño de la base de datos.

Al respecto, la OTIC informó que tecnológicamente se garantiza que se puede recuperar la operatividad del Sistema de Información en aproximadamente un (1) día. Sin embargo, no se obtuvo evidencia que dé cuenta de la realización de pruebas que permitan asegurar que tecnológicamente se podrá recuperar el sistema en el tiempo indicado y contar con mediciones de los tiempos reales en que se tendrá operativo el Sistema de Información ante la presencia de alguna falla o evento inesperado que ponga no operativa la infraestructura que soporta el Sistema de Información SIVIC.

Asimismo, no se evidencian soportes que den cuenta de una prueba de recuperación y restauración de la infraestructura que soporta el Sistema de Información SIVIC, de manera que se pueda asegurar la

recuperación total del aplicativo y la base de datos a partir de los backups existentes, y de acuerdo con las tareas y actividades definidas en el Plan de Contingencia de la entidad.

Referente a las copias de respaldo, no se evidenció la ejecución de pruebas de restauración de las copias de respaldo para el sistema de información SIVIC, y no se evidenció un plan de restauración para la vigencia 2025 donde se pudiera verificar que se tiene planeado un proceso de restauración para este sistema de información, con lo cual se verifica que la información almacenada en las copias de respaldo esté funcional.

Dado lo anterior, se recomienda evaluar la infraestructura de contingencia con que cuenta actualmente en la entidad, de llevar a cabo un estudio de costo/beneficio, evaluar las diferentes opciones para la implementación y puesta en marcha del funcionamiento de un plan de contingencia para soportar la operación del proceso de Victimas, objeto de esta auditoría.

Asimismo, planificar una prueba de contingencia tecnológica que permita evaluar la efectividad del Plan de Contingencia de TI para la infraestructura que soporta SIVIC, determinar los tiempos de recuperación antes los diferentes eventos que se pudiesen presentar de inoperatividad, así como confirmar que el Manual de Instalación, Configuración Y Despliegue para el aplicativo SIVIC aplica en caso de requerirse la instalación total del aplicativo.

5. Análisis de Vulnerabilidades

Se evidenció que el 20 de julio de 2024, se realizó el análisis de vulnerabilidades para el Servicio de SIVIC, cuyo resultado generó una (1) vulnerabilidad tipificada como alta, ninguna tipificada como “crítica-Critical”, 5 tipificadas en “medio-medium” y 12 “bajas-low”.

Para la vulnerabilidad categorizada como Alta, se evidenció que se atendió la vulnerabilidad de categoría alta, encontrada en el proceso de ejecución del análisis de vulnerabilidades y se implementó el plan de remediación correspondiente.

Se observó que en el documento “GS-042- Gestión de incidentes de seguridad y privacidad de la información y gestión de vulnerabilidades”, en la sección 8-Análisis de Vulnerabilidades no se tiene formalmente establecido a cuáles de las vulnerabilidades según criticidad se les debe definir y ejecutar un plan de remediación.

Recomendación No. 3

Para las vulnerabilidades categorizadas en criticidad “media”, se recomienda evaluar en detalle y en conjunto con la OCDVPR, los riesgos que potencialmente pueden materializarse con el fin de definir si alguna requiere plan de remediación.

Adicionalmente, definir formalmente el criterio para priorizar y atender las vulnerabilidades identificadas cuando se ejecuta el análisis de vulnerabilidades a los Sistemas de Información. Asimismo, comunicar todas las vulnerabilidades (criticas, altas, medias y bajas) a la OCDPVR, para que, como área administradora funcional del Sistema de Información, concluya respecto a la necesidad de implementar los planes de remediación o asumir los riesgos según corresponda.

6. Activos de Información

Una vez analizada la matriz de activos de información (FT-367) con los Activos identificados para la dependencia OCDPVR, se evidenciaron los siguientes Activos de Información correspondientes al Sistema de Información SIVIC: El aplicativo SIVIC (OACPVR-003), la base de datos URCUNINA BD (OACPVR-004) y la página Web de Víctimas (OACPVR-012).

Se observó que cada activo de información tiene identificados los riesgos asociados a Seguridad de la Información, valorados y definidos sus respectivos controles.

Para los Activos de Información “SIVIC” y “URCUNINA BD”, se observa que el campo (columna el responsable propietario No. 2 (columna R del formato FT-367_AI_OACPVR_2024_FINAL.xls) y el custodio del activo de información No. 2 (columna V del mismo formato FT-367) corresponde a un “contratista”, por lo que se recomienda que adicionalmente al contratista se incluya como responsable y custodio del Activo de Información a un funcionario de planta o provisional (Profesional Universitario y/o profesional especializado), con el fin de dar continuidad a la operación mitigando el riesgo potencial de interrupciones en las labores debido a la dependencia en los procesos de contratación en la entidad.

7. Cambios a Programas

Se observó que durante el periodo evaluado, se registraron siete (7) nuevos desarrollos y un (1) cambio en la herramienta GLPI, que al ser analizados se concluye que:

1. Los siete (7) nuevos desarrollos no implicaron despliegues en producción, por las siguientes razones:

   - Dos (2) estaban por fuera de los tiempos de atención por lo que se cerraron sin solución y se abrieron nuevos casos que se encuentran en proceso de ser atendidos en estado “en espera”. Casos GLPI: 346710 y 350824
   - Un (1) caso cerrado que indica “se implementara una solución en una versión reciente de SIVIC". Caso GLPI 346773.
   - Cuatro (4) casos que aun se encuentran abiertos en estado “en espera”. Casos GLPI: 360480, 360493, 360505 y 360516

2. El cambio para el cual se realizó despliegue en producción, fue registrado bajo el GLPI No. 348769 - Control de Cambios - SISTEMA MIR SIVIC, tipificado en la categoría “Despliegue Aplicaciones > Cambios TI”, para el cual se evidenciaron los soportes adecuados: el formato FT1121 - Solicitud de Cambios FRC y Análisis de impacto y soporte del Comité de Cambios donde fue aprobado su paso a producción.

Se concluye que el procedimiento aplicado para la gestión de cambios de SIVIC se está efectuando bajo los criterios establecidos en la guía GS-111 Gestión de Cambios.

8. Manuales de Usuario y Técnico del Sistema de Información

Recomendación No. 4

Se observó que el Sistema de Información SIVIC cuenta con Manual de usuario y Manual de Instalación, configuración y despliegue, los cuales no han sido actualizados o no se tiene evidencia de su revisión desde el año 2021, que permita asegurar su aplicabilidad.

Se recomienda realizar la revisión y actualización de los manuales, así como en coordinación con el área de planeación identificar si fuese necesario su publicación según los lineamientos establecidos por dicha dependencia. Al igual que, realizar sesiones de sensibilizaciones al interior de la OCDPVR, en especial a los funcionarios que interactúan constantemente con el Sistema de Información en su labor diaria.

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: María Jazmín Gómez Olivar – Jefe (E) Oficina de Control Interno