Bogotá D.C., 17 de Octubre del 2025 INT-HCC-040-25

Doctor
GUILLERMO MAYORGA
Representante Legal
UT HOSPITAL CARDIOVASCULAR DE CUNDINAMARCA
Ciudad

ASUNTO: PRESENTACIÓN OPORTUNIDADES DE MEJORA PLATAFORMA GEOVICTORIA Y PROCESO DE SOPORTE TÉCNICO.

Respetado Doctor,

En cumplimiento de nuestras obligaciones contractuales derivadas de la ejecución del contrato de interventoría No. SS-CM-INV-825-2025 cuyo objeto es *"REALIZAR, DESARROLLAR Y EJECUTAR LA INTERVENTORÍA TÉCNICA, JURÍDICA, ADMINISTRATIVA, FINANCIERA Y CONTABLE, EN REPRESENTACIÓN DE LA SECRETARÍA DE SALUD DEL DEPARTAMENTO DE CUNDINAMARCA COMO ENTIDAD CONTRATANTE DEL "CONTRATO DE CONCESIÓN NO. 002 DE 2003" CELEBRADO ENTRE LA SECRETARÍA DE SALUD Y LA UNIÓN TEMPORAL HOSPITAL CARDIOVASCULAR DEL NIÑO DE CUNDINAMARCA*", En cumplimiento de las obligaciones de supervisión y seguimiento establecidas.

Esta interventoría se permite presentar las oportunidades de mejora identificadas sobre la plataforma de GeoVictoria y el proceso de Soporte Técnico del Hospital Cardiovascular de Cundinamarca, actividad realizada en el mes de septiembre 2025.

PLATAFORMA GEOVICTORIA

1. Contrato de servicio y SLA vigentes: El documento firmado constituye el contrato de prestación de servicios de software.
   Contiene cláusulas sobre disponibilidad, continuidad del servicio y condiciones de soporte (funcionan como SLA). Se establecen responsabilidades de ambas partes:

   Proveedor (Geovictoria): garantizar la disponibilidad de la plataforma y actualizaciones.
   Cliente (Hospital): asegurar el acceso a internet y la correcta operación en sus equipos.

2. Soporte ofrecido por el proveedor y responsable interno asignado: en el contrato se estipula que presta soporte técnico remoto, actualizaciones y acompañamiento en caso de fallas.
   Responsable interno: Responsable TI del hospital Coordinador de Informática. El contrato indica que la institución debe nombrar un interlocutor válido para la operación y soporte.

EJEMPLO DE TICKET VISITA TÉCNICA GEOVICTORIA



Observación:
De acuerdo con la información suministrada por el hospital, durante el último semestre no se han registrado solicitudes de soporte asociadas a los servicios de TI.

Nota de seguimiento: Se recomienda mantener un registro formal y trazable de las solicitudes de soporte que puedan presentarse en el futuro, con el fin de garantizar evidencia objetiva y continuidad en la gestión del servicio.

- **Disponibilidad del servicio**

  Durante la revisión de la documentación de Arquitectura y Seguridad de GeoVictoria, se constató que el proveedor asegura la disponibilidad de los servicios en un 99.9% del tiempo, respaldado en la infraestructura de Microsoft Azure, la cual ofrece redundancia a nivel global con múltiples centros de datos y replicación de datos.

Adicionalmente, se evidenció que la solución GeoVictoria Box garantiza la continuidad operativa en escenarios de desconexión a internet, permitiendo la marcación de asistencia de manera local y la sincronización automática de los datos una vez restablecida la conectividad.
SLA definido con uptime del 99.9%.
Publicación de los servicios en Azure con redundancia y replicación entre centros de datos.
Existencia de instancias principales y réplicas para asegurar continuidad ante fallas.
GeoVictoria Box permite la marcación independiente de la conectividad y sincronización posterior.

La definición de un SLA cuantitativo (99.9%) fortalece la medición objetiva de la disponibilidad del servicio. Así mismo, los mecanismos de redundancia en Azure y las funcionalidades offline de GeoVictoria Box refuerzan la resiliencia y continuidad del negocio. No obstante, la documentación revisada no especifica valores de RTO (Recovery Time Objective) y RPO (Recovery Point Objective), lo que limita la capacidad de evaluar tiempos de recuperación en escenarios críticos.

Recomendación
Mantener documentado y comunicado el compromiso de uptime del 99.9% en los acuerdos contractuales.
Complementar el SLA con definiciones claras de RTO y RPO, aplicables a cada servicio crítico.
Documentar y presentar evidencias de las pruebas periódicas de restauración y de continuidad de la solución GeoVictoria Box, para validar su efectividad en escenarios de desconexión.

A nivel institucional, el Hospital cuenta con un documento formal de Plan de Contingencia frente a Caída del Sistema (PT03 DA V3), con vigencia hasta 2027 y control de cambios documentado. Este protocolo define responsables, recursos y flujograma de actuación, así como formatos físicos para dar continuidad a la atención en caso de indisponibilidad prolongada del sistema.
No obstante, el plan presenta vacíos que lo hacen incompleto:

- No se evidencian pruebas o simulacros que validen su efectividad (requisito de la Resolución 3100 de 2019).
- No se definen tiempos de recuperación claros más allá del umbral de dos horas para iniciar registros manuales
    - RTO (Recovery Time Objective): tiempo máximo aceptable que puede estar inactivo el sistema antes de restablecerse.
    - RPO (Recovery Point Objective): cantidad máxima de información que se podría perder (en minutos u horas) sin afectar de manera crítica la operación.
- No contempla un protocolo de comunicación interna y externa para informar oportunamente a usuarios, proveedores, entes de control y pacientes.
- No incluye una matriz de riesgos tecnológicos vinculada al plan.
- No establece un proceso de seguimiento post-incidente que permita documentar, analizar y mejorar tras la recuperación del servicio.

Recomendación

Se recomienda evolucionar el actual Plan de Contingencia PT03 DA V3 hacia un Plan de Continuidad del Negocio (PCN) integral, que contemple no solo la indisponibilidad del sistema, sino también la continuidad de procesos críticos hospitalarios y de soporte.

Este PCN debe incorporar como componente específico el Plan de Recuperación ante Desastres (DRP), con definición clara de RTO y RPO, protocolos de comunicación, matriz de riesgos tecnológicos y pruebas periódicas de validación.

- **Integridad y trazabilidad**

  Se verificó en la plataforma GeoVictoria la existencia de mecanismos de trazabilidad que incluyen: log de accesos (usuarios, fecha y hora), historial de solicitudes y permisos (ejm vacaciones), registro de creación/modificación de turnos y reportes de auditoría. Estas evidencias respaldan la capacidad de la solución para garantizar integridad y trazabilidad en la gestión de asistencia y permisos

  Log de accesos (usuario, fecha, hora, ubicación, dispositivo usado). Registro de creación, modificación o eliminación de turnos Auditoría de cambios en datos de asistencia y permisos.

  Monitoreo continuo (Application Insights – Azure): registra logs de actividad, errores, tiempos de respuesta y telemetría, permitiendo análisis forense en caso de incidentes

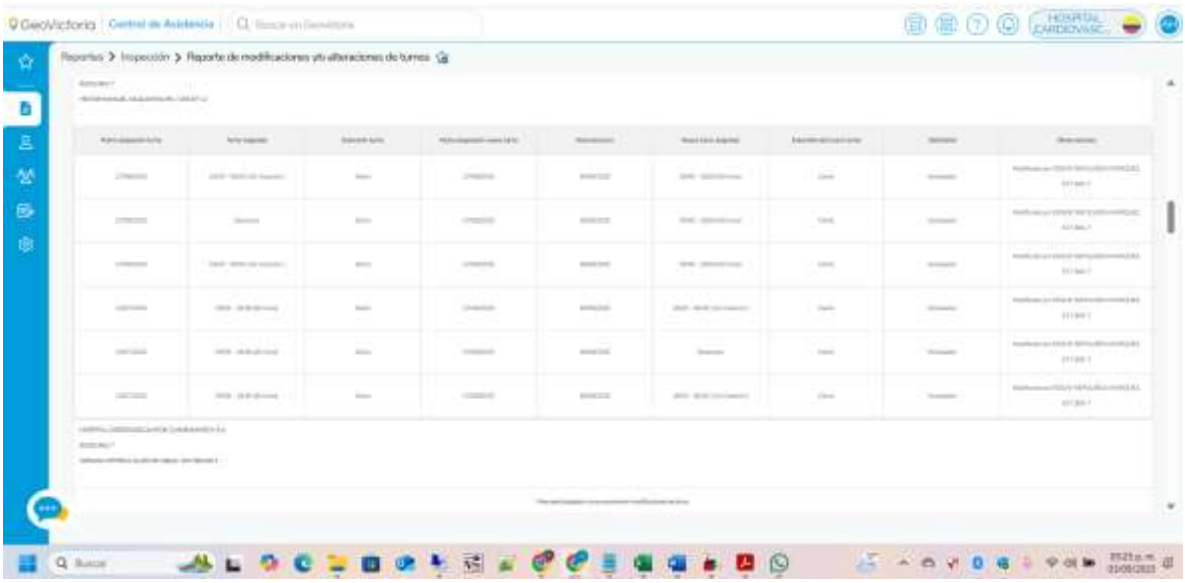
  Logs propios de la solución: cada servicio genera registros internos de operaciones y accesos, fortaleciendo la trazabilidad.

  Gestión de accesos con Azure Active Directory: se aplica el principio de privilegio mínimo, con revisiones trimestrales de privilegios y roles

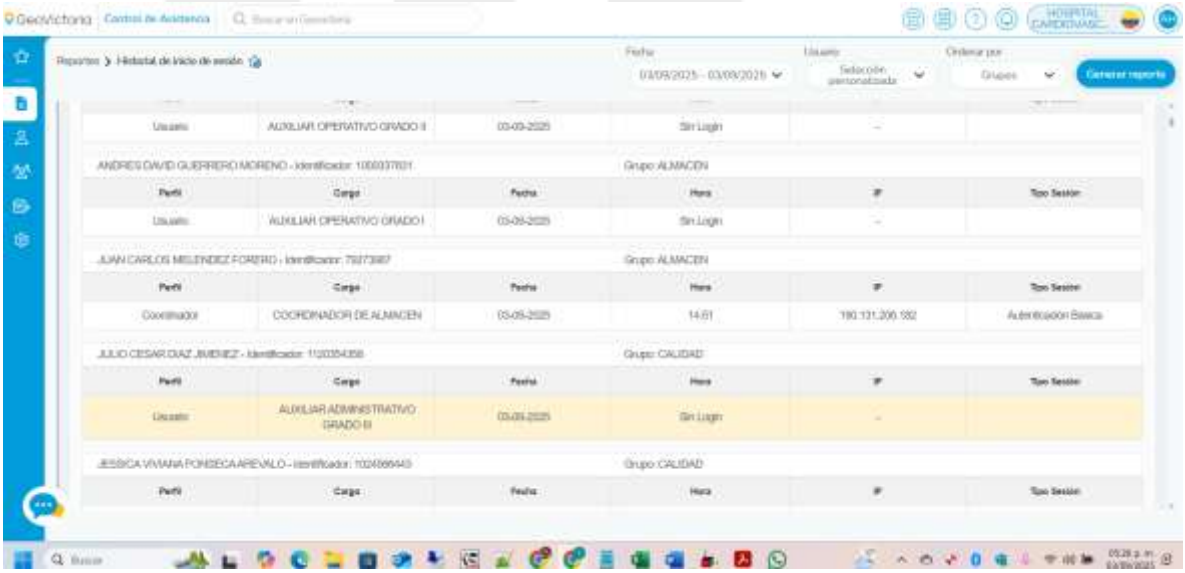
  Evaluación

  Los mecanismos de trazabilidad e integridad son consistentes con buenas prácticas de seguridad y permiten identificar operaciones, accesos y cambios relevantes en la plataforma. No obstante, no se evidencian métricas cuantitativas (ejm número de logs revisados, tiempos promedio de cierre de incidentes, auditorías de accesos), lo que dificulta medir la efectividad de estos controles.

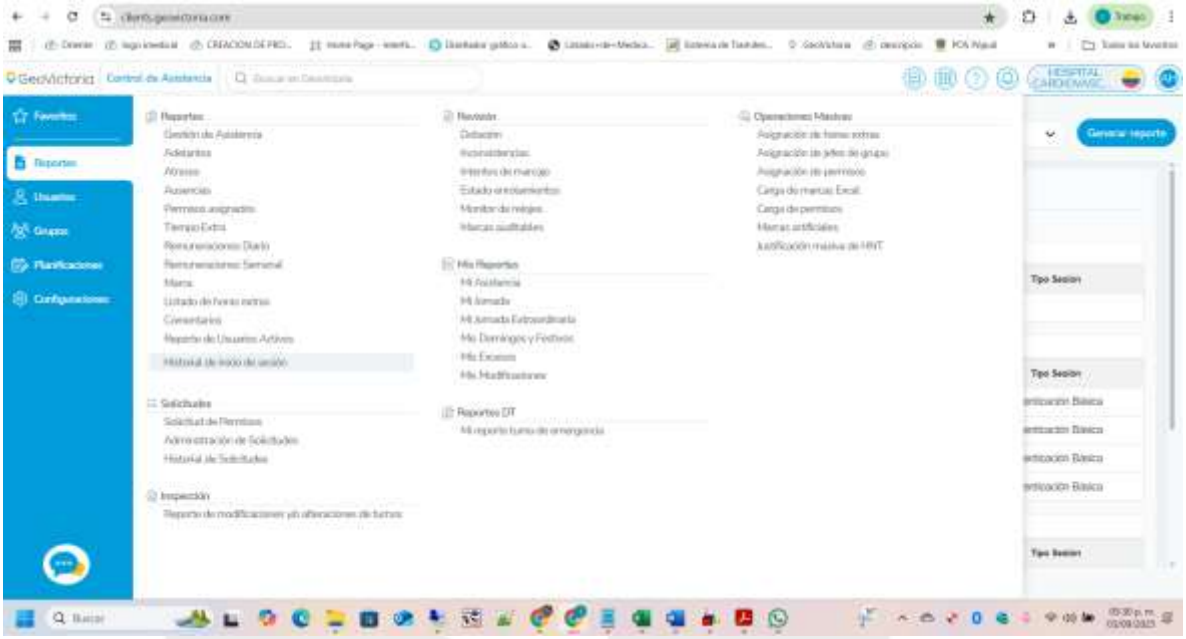
REVISIÓN Y MODIFICACIÓN DE TURNOS GOEVICOTORIA



VERIFICACIÓN DE INICIO DE SESIÓN GEOVICTORIA



REPORTES DE GEOVICTORIA TRAZABILIDAD



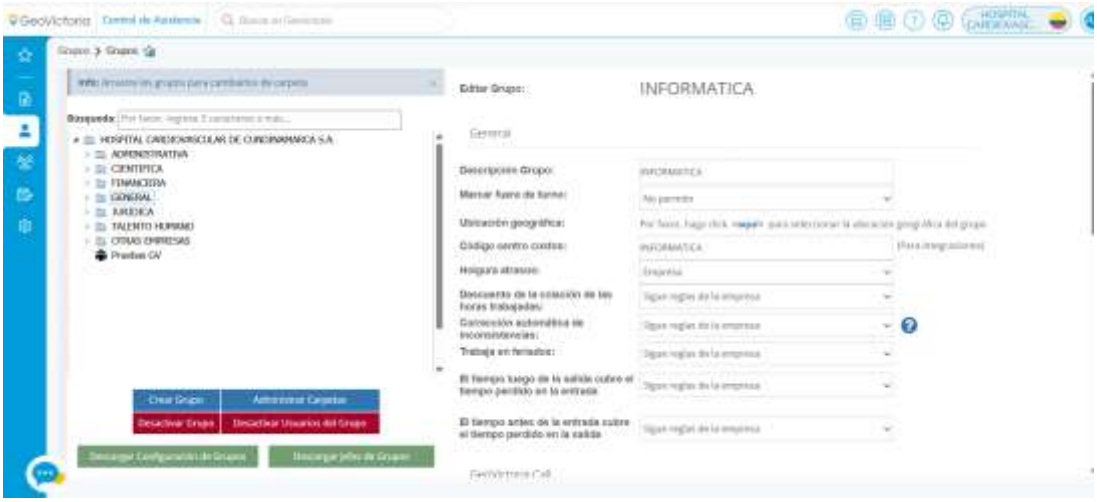
Recomendación
Definir indicadores de desempeño (KPIs) para medir la efectividad de los controles de trazabilidad, tales como:

- Porcentaje de logs revisados dentro de los plazos definidos.
- Número de accesos indebidos detectados y gestionados.
- Tiempos promedio de resolución y cierre de incidentes.
- Mantener evidencia documentada de las auditorías de accesos y revisiones de privilegios, de modo que se garantice trazabilidad verificable ante auditorías externas.

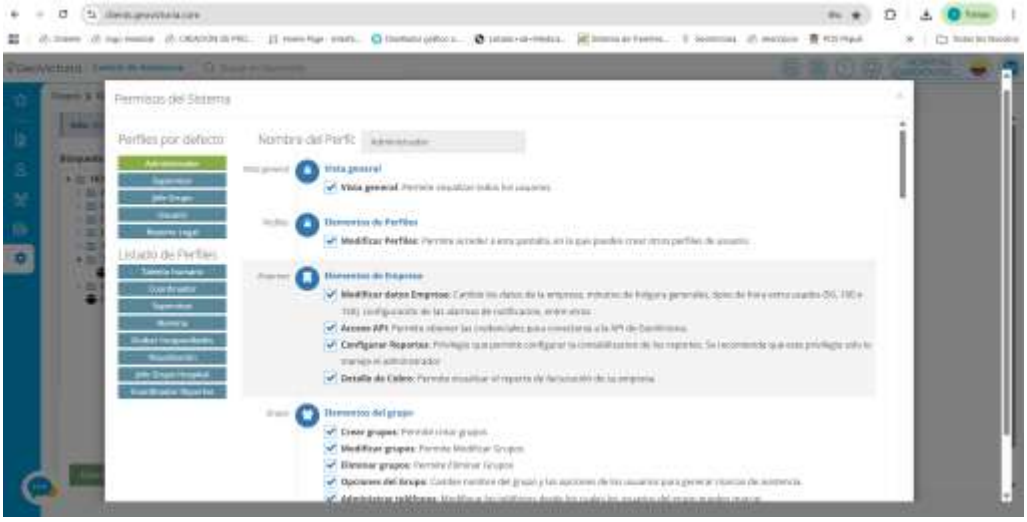
- **Seguridad de la información**

En el entorno hospitalario, la gestión de accesos al aplicativo GeoVictoria es administrada por el área de TI/Coordinación de Informática, quien tienen la facultad de crear usuarios, asignar roles (administrador, supervisor, usuario) y controlar los permisos asociados.
Se evidenció que la administración se realiza directamente en la plataforma, observándose la creación de grupos, perfiles de usuario y la verificación de inicios de sesión. Adicionalmente, se cuenta con un archivo independiente que documenta los roles, perfiles y permisos asociados, lo que garantiza la trazabilidad y facilita la consulta en procesos de auditoría o en caso de contingencia.

GRUPOS GEOVICTORIA

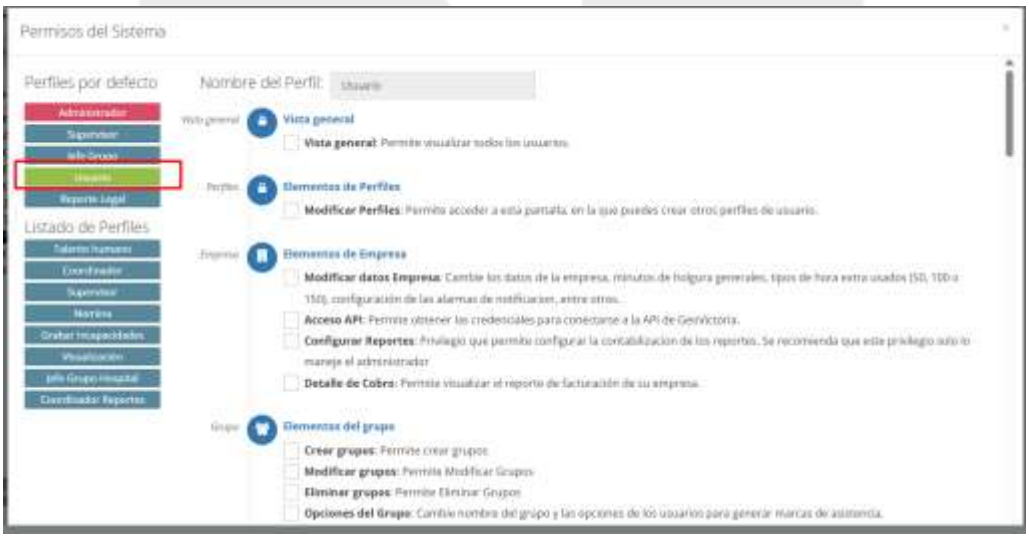


MODULO PERMISOS DEL SISTEMA GEOVICTORIA





PERFIL DE USUARIO GEOVICTORIA



Recomendación

La interventoría considera este control como favorable, resaltando la importancia de mantener dicho documento actualizado, versionado y formalizado como parte de las políticas de seguridad de la información, asegurando su vigencia y aplicabilidad:

- Formalizar una Política de Gestión de Accesos que defina los procesos de creación, modificación y eliminación de usuarios en GeoVictoria, estableciendo responsables, flujos de aprobación y periodicidad de revisión.
- Mantener y versionar la Matriz de Roles y Perfiles en documento independiente (Word o Excel), asegurando que los permisos de cada tipo de usuario estén actualizados y cuenten

con aprobación formal de la Coordinación de Informática.

- Implementar un procedimiento de respaldo documental periódico (exportación de usuarios y roles desde la plataforma), de manera que se cuente con soporte independiente y actualizado en caso de contingencias.

Encriptación de datos: Se evidenció que la plataforma GeoVictoria implementa medidas de seguridad para garantizar la encriptación de datos en tránsito, mediante el uso de HTTPS y cifrado TLS v1.2 en todas las comunicaciones hacia y desde la infraestructura en Azure. Así mismo, se hace uso de Azure Key Vault para la gestión segura de llaves y credenciales.
Sin embargo, no se identificó en la política interna del hospital una referencia explícita a este mecanismo de seguridad, lo que puede generar un vacío en la documentación local de seguridad de la información.

Documentación de Arquitectura y Seguridad: descripción del uso de TLS v1.2 en comunicaciones.
Uso de Azure Key Vault para almacenamiento seguro de llaves y secretos.
Ausencia de referencia en la política interna del hospital sobre cifrado de datos en tránsito.

Recomendación
Incluir en los seguimientos al proveedor (ej. en los comités de servicio o revisiones contractuales) la solicitud de evidencias actualizadas sobre el uso de protocolos de cifrados seguros (TLS/SSL) y la vigencia de las configuraciones aplicadas.
Establecer como requerimiento que el proveedor notifique de manera formal cualquier cambio en los protocolos de cifrado o en los mecanismos de protección de llaves.
Documentar estas revisiones en los reportes de seguimiento al contrato, para garantizar trazabilidad y respaldo en caso de auditorías externas.

GeoVictoria (sobre infraestructura Azure) aplica cifrado robusto tanto en tránsito como en reposo, con doble cifrado para datos sensibles y uso de TLS/SSL con PFS Perfect Forward Secrecy (PFS), que genera claves únicas por sesión, fortaleciendo la seguridad de las conexiones y las conexiones usan claves RSA 2048 bits. Esto asegura un alto nivel de confidencialidad, integridad y protección de datos.

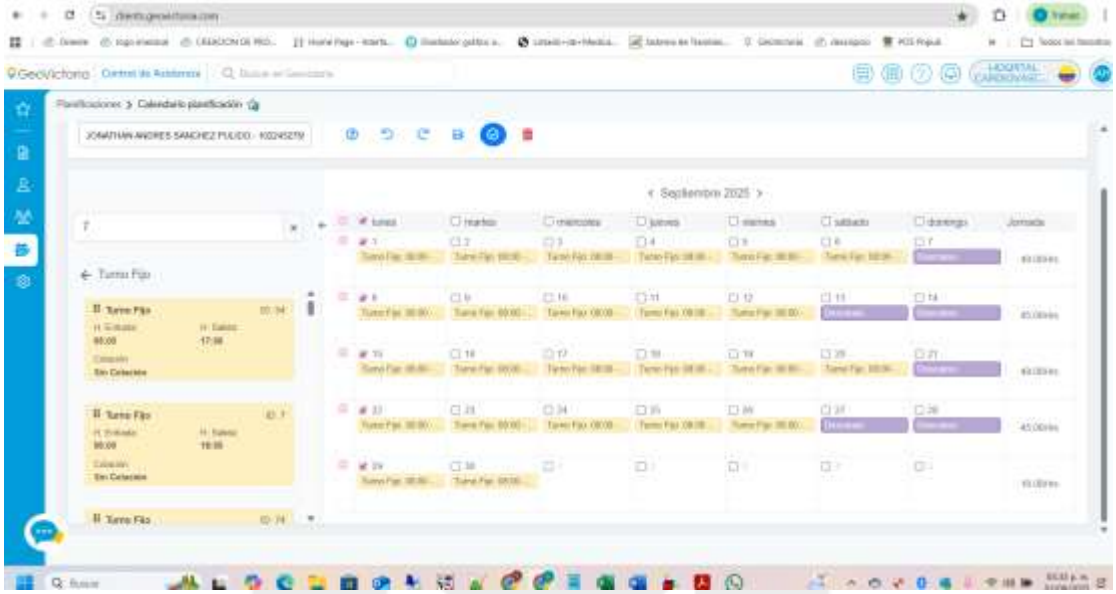
- **Gestión de personal y turnos**
  Correcta configuración de horarios, turnos y descansos. Evidencia de reportes de asistencia confiable. Validación de horas extras, ausencias e incidencias. Procedimientos de ajuste manual y su trazabilidad.
  Se constató que la plataforma GeoVictoria utilizada en el hospital permite la correcta configuración de horarios, turnos y descansos, así como la generación de reportes de asistencia confiables. También se identificó que el sistema admite la validación de horas extras, ausencias e incidencias, y que los ajustes manuales cuentan con trazabilidad interna.

  No obstante, no se evidenció la existencia de una política institucional formal que establezca lineamientos claros sobre la asignación de turnos, aprobación de horas extras, registro de ausencias e incidencias, ni sobre los procedimientos para realizar ajustes manuales. Esto

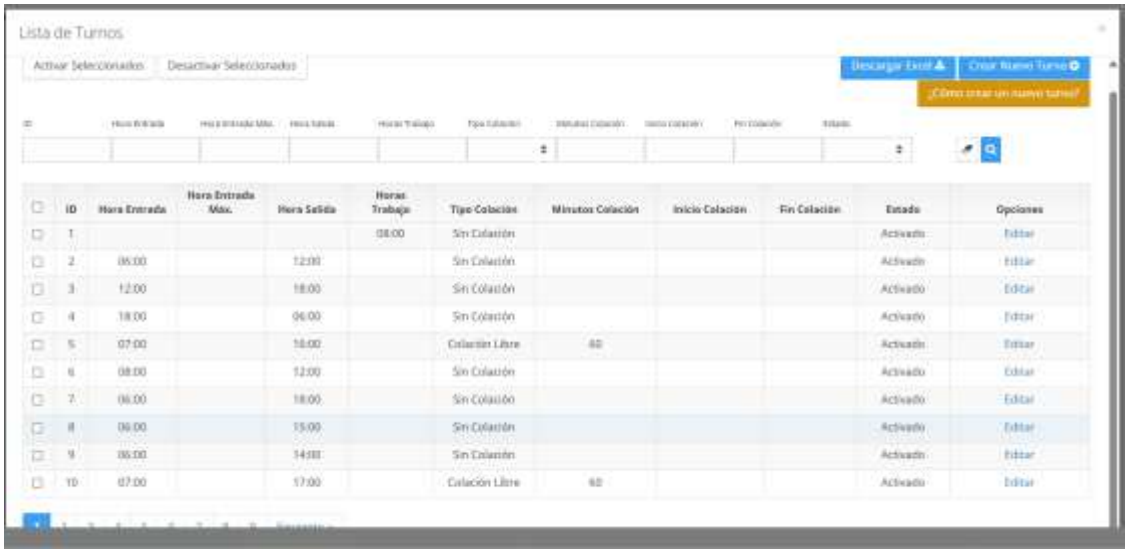
genera dependencia del aplicativo como único respaldo y limita la estandarización de los criterios aplicados.

La plataforma ofrece herramientas sólidas para gestionar horarios y turnos, y garantiza trazabilidad en modificaciones, permisos y reportes de asistencia. Sin embargo, la falta de una política formal documentada genera un riesgo de criterios dispares en la aplicación, dependencia exclusiva del sistema y ausencia de un respaldo normativo que garantice continuidad en caso de fallas técnicas.

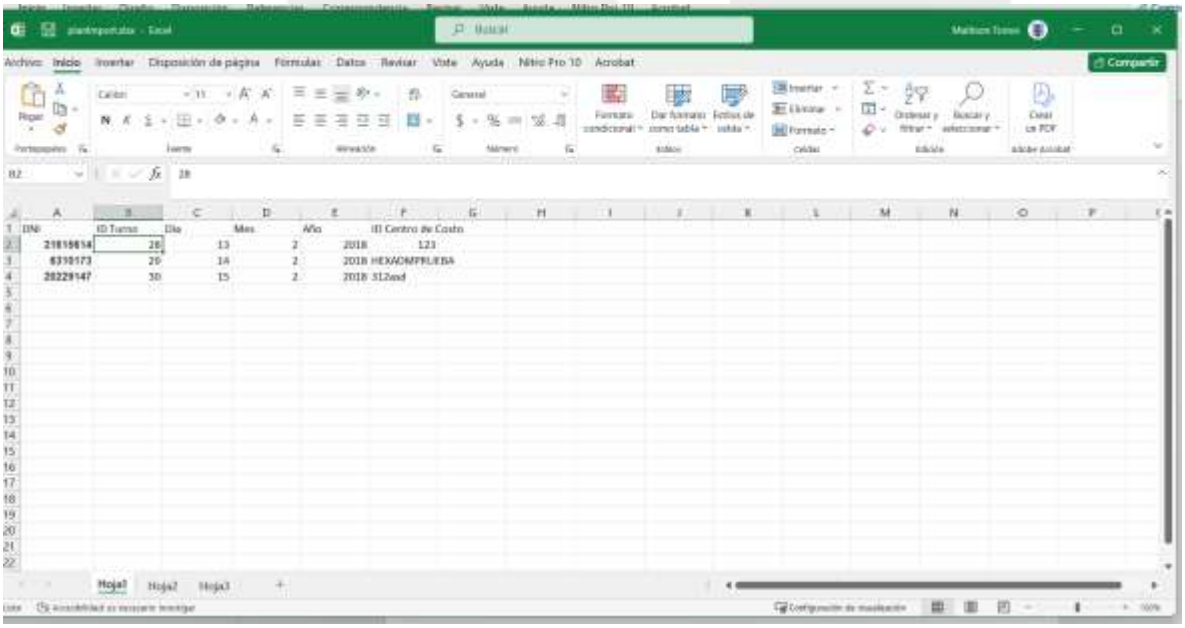
CONFIGURACIÓN DE HORARIOS Y TURNOS CARGUE DE TURNOS Y MODIFICACIONES



PANTALLA DE CONFIGURACIÓN DE TURNOS



PLANTILLA PARA CARGUE MASIVO DE TURNOS



El Hospital cuenta con un protocolo formal para la gestión de permisos en la plataforma Geovictoria, el cual establece de manera clara los objetivos, alcance, tipos de permisos, plazos de solicitud, tiempos de respuesta, responsables (colaborador, jefe inmediato, Talento Humano) y medidas por incumplimiento.

Este instrumento permite asegurar la trazabilidad de las solicitudes, la presentación de soportes obligatorios, y la validación o rechazo dentro de los tiempos definidos, fortaleciendo la transparencia y el control en la gestión de permisos.

Recomendaciones:

- Ampliar el alcance a una política integral: Complementar el protocolo con una Política de Gestión de Turnos y Asistencia, que abarque asignación de turnos, descansos, validación de horas extras y ausencias, para garantizar criterios unificados en toda la gestión de tiempo laboral.
- Alinear la matriz de roles y permisos: Documentar en un archivo independiente (Excel/Word) los tipos de usuario y permisos asignados en GeoVictoria, con el fin de contar con evidencia ágil para procesos de auditoría o contingencias.
- Generar respaldos documentales periódicos: Establecer la práctica de emitir reportes consolidados de asistencia y permisos desde GeoVictoria, validados mensualmente por Talento Humano, como soporte independiente frente a posibles fallas técnicas de la plataforma.
- Fortalecer la capacitación: Realizar sesiones de socialización periódicas con colaboradores y jefes inmediatos sobre el uso del protocolo, soportes válidos y tiempos de gestión, con el fin de mejorar el cumplimiento y reducir reprocesos.

- **Interoperabilidad**

Se evidenció que la plataforma GeoVictoria no cuenta con interoperabilidad con otros sistemas. Actualmente, las novedades de personal son recibidas hasta el día 20 de cada mes y revisadas por el área de Talento Humano a través de soportes físicos y registros en Excel. Posteriormente, la información debe ser cargada manualmente en el sistema SIIGO, lo que genera dependencia de procesos manuales y riesgo de errores en la consolidación de datos.

Recomendación

Se sugiere evaluar mecanismos de interoperabilidad o integración automatizada entre GeoVictoria y el sistema SIIGO, con el fin de reducir la dependencia de procesos manuales y minimizar el riesgo de inconsistencias en la información. Mientras tanto, es importante documentar y formalizar el control de conciliación periódica entre los soportes físicos, los archivos en Excel y la información cargada en SIIGO, asegurando la trazabilidad y exactitud de los datos.

Se recomienda diseñar un diagrama de arquitectura de procesos que represente la relación entre el aplicativo GeoVictoria y el sistema SIIGO, identificando los flujos de información, puntos de control y actividades críticas en la gestión de novedades de personal. Este diagrama debe incluir:

- Los procesos actuales (recepción de novedades, validación por Talento Humano, consolidación en Excel, carga manual en SIIGO).
- Los responsables en cada etapa del flujo.
- Los controles establecidos para garantizar integridad, exactitud y trazabilidad de la información.
- Las oportunidades de mejora orientadas a una futura interoperabilidad o integración parcial/total entre plataformas.

Este diseño permitirá contar con una visión integral y documentada del proceso, facilitando la gestión de riesgos asociados, el control interno y la definición de un plan de mejora tecnológica a mediano plazo.

- **Canales de atención**:
  El proceso de soporte técnico dispone de los siguientes canales de atención: a través de WhatsApp al número 310 217 9101 y mediante la línea telefónica (601) 592 2979, extensiones 402 y 703, con disponibilidad permanente 7x24.

- **Registro de solicitudes:**
  Se evidenció que las incidencias y requerimientos actualmente se registran en una bitácora en Excel, donde se consigna información básica como fecha, usuario, departamento, tipo de incidente, técnico asignado, estado y observaciones. No obstante, este mecanismo no constituye un sistema formal de gestión de tickets, lo que limita la trazabilidad, el seguimiento y la generación de reportes.

  Por otra parte, se observó que el Hospital Cardiovascular de Cundinamarca dispone de un documento "*Gestión de servicios TIC HCC*" donde se pudo evidenciar:

  Fortalezas identificadas
  - Definición de canales claros: WhatsApp corporativo y línea telefónica interna, ambos con disponibilidad 24/7.
  - Orientación al usuario: Se enfatiza en garantizar una comunicación rápida y efectiva, incluso con la posibilidad de enviar fotos o capturas para agilizar el diagnóstico.
  - Priorización según criticidad: Se contempla un esquema de atención diferenciada para incidentes de baja, media y alta prioridad, lo cual es positivo en un entorno hospitalario.
  - Cobertura permanente: Se garantiza continuidad en los servicios hospitalarios gracias a la disponibilidad ininterrumpida.

Debilidades
  - Ausencia de un sistema formal de tickets: Aunque se mencionan los canales, no se evidencia un sistema automatizado para el registro, seguimiento y cierre de casos. Esto limita la trazabilidad.
  - Flujo de gestión poco detallado: El documento enuncia pasos generales de atención (recepción, asignación, atención remota/presencial), pero no especifica tiempos de respuesta (SLA) ni responsables de escalamiento.
  - Falta de métricas o indicadores: No se definen indicadores de desempeño como tiempo promedio de atención, tasa de resolución en primer contacto, o satisfacción del usuario.
  - Políticas generales: Aunque se definen horarios y disponibilidad, no se detallan protocolos de escalamiento ni niveles de servicio documentados.

  Hallazgo:
  El documento constituye una guía básica de atención de casos en el área de Sistemas del Hospital Cardiovascular de Cundinamarca, enfocada en la comunicación ágil con los usuarios y en la disponibilidad 24/7. Sin embargo, presenta debilidades en cuanto a formalización de procesos, trazabilidad y control, lo que se traduce en un hallazgo relevante desde el punto de vista de auditoría y gestión de calidad.

Riesgos asociados

- Baja trazabilidad: Al no existir un sistema de tickets, los registros dependen de controles manuales (Excel, bitácoras), lo que puede generar pérdida de información.
- Falta de control y auditoría: Sin métricas ni reportes, es difícil medir el cumplimiento y eficacia del soporte.
- Dependencia de canales informales: WhatsApp es ágil, pero no garantiza confidencialidad ni formalidad en la gestión de incidencias.

Documento: Bitacora de Soportes - Sistemas HCC.xls
Gestion de servicios TIC HCC.docx.pdf

- **Priorización de incidentes y Tiempos de atención y resolución (SLA):**
  Aunque en el documento de gestión de servicios TIC del Hospital Cardiovascular de Cundinamarca se contempla la clasificación de incidentes por niveles de criticidad (alta, media y baja)

  En el documento de Gestión de servicios TIC HCC.docx.pdf en la práctica no se evidenció su aplicación en los registros ni en la atención de los casos. Adicionalmente, dichos niveles no cuentan con tiempos de respuesta y solución definidos.

  En la revisión de la bitácora de soporte y de los mecanismos de atención, se constató que no se documenta la categoría de criticidad en los incidentes reportados ni se relacionan tiempos de respuesta asociados a cada nivel.

  Riesgo:
  La falta de aplicación y de tiempos definidos por nivel de criticidad limita la efectividad de la priorización de incidentes, lo que puede generar demoras en la atención de casos críticos y afectar la continuidad de los servicios hospitalarios.

- **Escalamiento de incidentes**:
  No se evidenció la existencia de un procedimiento formal de escalamiento para los incidentes que no pueden ser resueltos en la primera línea de soporte técnico.

  En la documentación revisada sobre la gestión de servicios TIC y en la práctica de atención de casos, no se encontraron lineamientos, responsables ni tiempos definidos para el escalamiento de incidentes hacia niveles superiores de soporte.

  La ausencia de un procedimiento de escalamiento puede ocasionar retrasos en la solución de incidentes complejos o críticos, dependencia de la discrecionalidad del personal de soporte y afectaciones a la continuidad operativa del hospital.

- **Evidencias de resolución y cierre de casos:**
  No se evidencian procedimientos ni registros que documenten las evidencias de resolución y el cierre formal de los casos atendidos por el área de soporte técnico.

En la revisión de la bitácora de soportes y en la documentación de gestión de servicios TIC, no se encontraron mecanismos que respalden de manera verificable la resolución ni el cierre de las incidencias registradas.

Riesgo:
La falta de evidencias de resolución y de un cierre formal de los casos limita la trazabilidad y transparencia del proceso, dificulta la validación de la efectividad de las soluciones aplicadas y puede derivar en reincidencia de incidentes o en reclamos por parte de los usuarios sin soporte documental.

- **Reportes periódicos**
  No se generan reportes periódicos de la gestión de soporte técnico, bajo el argumento de que todos los casos son atendidos el mismo día.
  En la revisión de la bitácora de soportes, correspondiente al periodo 26 de junio de 2025 a 25 de septiembre de 2025 (240 registros), se observó lo siguiente:
  - De los casos con fechas de solicitud y solución válidas (136 registros), 133 (98%) se reportan como resueltos el mismo día.
  - Existen 3 registros (2%) con diferencias en las fechas, incluyendo inconsistencias como solución anterior a la solicitud.
  - 104 registros (43% del total) no consignan fecha de solución, lo que impide confirmar la atención real de los incidentes.
  - No se identificaron reportes de consolidación o análisis periódico que permitan verificar tendencias, tiempos de atención promedio o reincidencias.

  Riesgo:
  La ausencia de reportes periódicos y la existencia de registros incompletos/inconsistentes limitan la capacidad de verificar de manera objetiva la oportunidad en la atención, afectan la trazabilidad del proceso y dificultan la implementación de acciones de mejora basadas en datos confiables.

- **Evaluar el control de acceso al WhatsApp corporativo y confidencialidad en la atención.**
  No se evidenció la existencia de controles de acceso, políticas de uso ni lineamientos formales que regulen la confidencialidad de la información gestionada a través del canal de WhatsApp corporativo para la atención de incidentes y requerimientos.

  En la revisión documental y de la práctica operativa, no se encontraron procedimientos que definan:
  - Usuarios autorizados para administrar el canal de WhatsApp corporativo.
  - Políticas de confidencialidad y protección de la información tratada en este medio.
  - Reglas de seguridad relacionadas con conservación, respaldo o auditoría de la información transmitida.

  Riesgo:
  La ausencia de controles de acceso y políticas de confidencialidad en el canal de WhatsApp

corporativo puede derivar en riesgos de exposición de información sensible, manipulación no autorizada, pérdida de trazabilidad y vulneración de principios de seguridad de la información (confidencialidad, integridad y disponibilidad).

- **Retroalimentación y mejora**

  No se evidenció la existencia de actividades de capacitación, espacios de retroalimentación ni aplicación de encuestas de satisfacción a los usuarios sobre el servicio de soporte técnico.

  En la revisión de la documentación de gestión de servicios TIC y de los registros de soporte, no se encontraron planes de capacitación a usuarios, mecanismos de retroalimentación formal ni reportes de encuestas de satisfacción que midan la percepción del servicio.

  Riesgo:
  La falta de capacitación y retroalimentación limita la capacidad de los usuarios para prevenir incidentes recurrentes, impide identificar oportunidades de mejora en el servicio y debilita la medición de la satisfacción del usuario, lo que puede afectar la calidad percibida y la eficiencia del soporte técnico.

- **Indicador GeoVictoria y Soporte Técnico**

Conclusión

- Fórmula definida, pero sin soporte en tickets o soportes.
- Hospital reporta “sin incidentes”, pero no hay trazabilidad ni respaldo documental.
- Interpretación: el indicador no es medible ni confiable en la práctica.

$$Disponibilidad = \frac{Tiempo\ que\ el\ sistema\ estuvo\ disponible}{Tiempo\ total\ esperado} \times 100$$

Recomendación: implementar un sistema de tickets para registrar interrupciones, impactos y acciones de recuperación, permitiendo calcular la disponibilidad de manera objetiva y verificable.

De la misma forma, se informa que a partir del mes de octubre se implementara el siguiente indicador de seguimiento:

Indicador de seguimiento a oportunidades de mejora de la interventoría

Nombre del indicador: Cumplimiento en la atención de oportunidades de mejora formuladas por la interventoría

Objetivo:
Medir el grado de avance y cumplimiento en la implementación de las acciones correctivas o preventivas derivadas de las oportunidades de mejora identificadas por la interventoría en sus informes periódicos.

Fórmula:

$$Porcentaje\ de\ cumplimiento = (\frac{Oportunidades\ de\ mejora\ atendidas}{Oportunidades\ de\ mejora\ formuladas}) \times 100$$

Variables:

- Oportunidades de mejora formuladas: Total de observaciones u oportunidades registradas por la interventoría durante el periodo evaluado.
- Oportunidades de mejora atendidas: Aquellas que cuentan con evidencia de acción implementada, validada y cerrada.

Unidad de medida:
Porcentaje (%)

Frecuencia de medición:
Mensual / Trimestral (según periodicidad de los informes de interventoría)

Meta sugerida:
≥ 90% de oportunidades de mejora atendidas en el periodo

Fuente de información:

- Informes de interventoría
- Plan de acción y seguimiento del área responsable
- Actas de cierre o evidencias documentales de cumplimiento

Responsable:
Coordinador de Sistemas y Coordinador de Informática.

Interpretación:

- **≥ 90 %:** Cumplimiento alto, gestión efectiva de acciones de mejora.
- **70 % – 89 %:** Cumplimiento medio, requiere seguimiento.
- **< 70 %:** Cumplimiento bajo, riesgo de recurrencia de hallazgos.

La información solicitada deberá remitirse a esta interventoría en un plazo no mayor a diez (10) días hábiles.

Cordialmente,



CARLOS ALBERTO YEPEZ GOMEZ
Representante Legal
RYF CONSULTORIA SAS BIC