RYF S.A.S
Consultoría, Auditoría e Interventoría

ACTA DE REUNIÓN No. 11

RESPONSABLE DE LA REUNIÓN: Carolina Romero

(En caso de ser presencial):

FECHA: 11 de noviembre 2025 VIRTUAL: PRESENCIAL: X LUGAR: Hospital Cardiovascular de Cundinamarca

OBJETIVO DE LA REUNIÓN: Auditoría Plataforma de Siigo

HORA DE INICIO: 9_00 am HORA DE FINALIZACIÓN: __12:00 am

ASISTENTES:

NOMBRE	ENTIDAD o DEPENDENCIA	CARGO	CORREO ELECTRÓNICO	TELÉFONO	FIRMA
Andrés Cruz	Hospital Cardiovascular de Cundinamarca	Coordinador Sistemas	sistemas@hccsa.com.co	3209795384	
Malitson Torres	Hospital Cardiovascular de Cundinamarca	Coordinador Informática	informatica@hccsa.com.co	3212031615	
Sebastián Alvarado	Hospital Cardiovascular de Cundinamarca	Administrador de Siigo			
Lilibeth Escamilla Rubio	Hospital Cardiovascular de Cundinamarca	Directora Administrativa			
Carolina Romero	RYF SAS	Interventor TI	Trabajo.interventoria@gmial.com	3184050702	

1. TEMAS A TRATAR

a) Modelo de despliegue y arquitectura
b) Control de Accesos
c) Gestión de Credenciales y Autenticación
d) Gestión de Cambios
e) Disponibilidad y Continuidad
f) Respaldos y Recuperación
g) Integridad y Trazabilidad
h) Validación Normativa

2. DESARROLLO DE LA REUNION O DESCRIPCION DE ACTIVIDADES REALIZADAS

a) Modelo de despliegue

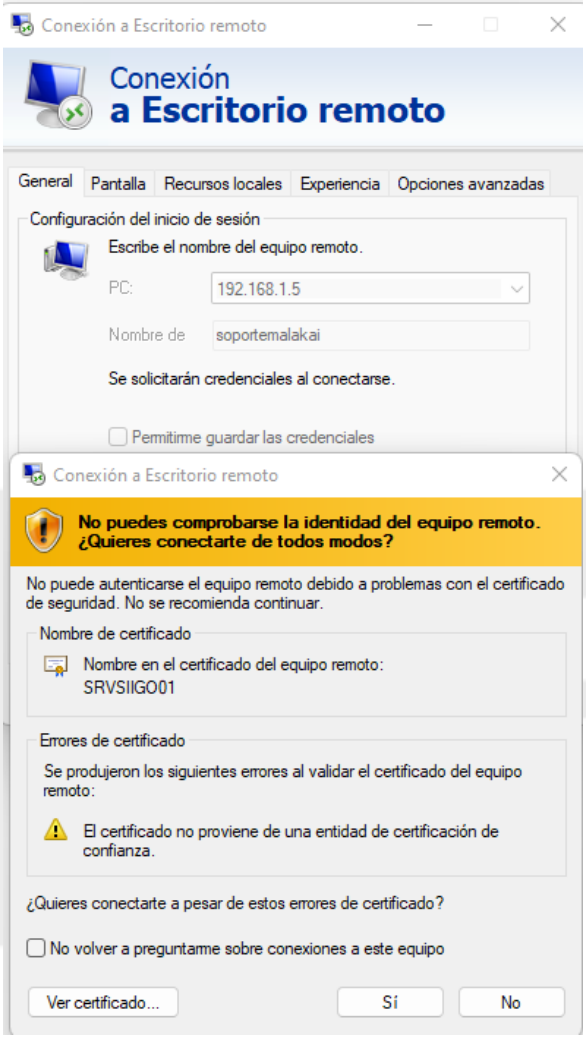
- **Arquitectura**

Servidor de aplicación Windows Server donde se encuentra instalada y ejecutándose la plataforma de Siigo 192.168.1.5 WServer RDP.
El servidor 192.168.1.5 (WServer RDP) es el servidor principal donde está instalada y alojada la plataforma Siigo utilizada por el Hospital Cardiovascular de Cundinamarca.
Los usuarios acceden mediante Escritorio Remoto (RDP), cargando sus perfiles individuales dentro del servidor, donde se ejecutan directamente Siigo, sus módulos y sus bases de datos. El servidor es administrado una parte operativamente por el área de Sistemas del Hospital Cardiovascular Navarra y otra parte por el proveedor que administra el servidor, mientras que Smoothcloud administra la infraestructura, seguridad en pfSense, accesos VPN, disponibilidad y respaldos.

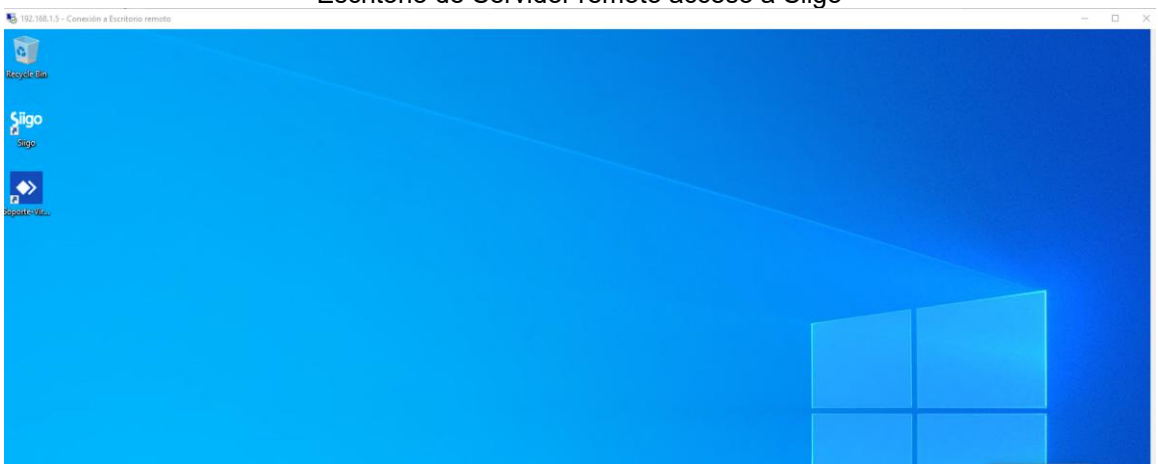
Funciones:
- Servidor RDP (Remote Desktop Protocol)
- Servidor donde reside la base de datos y los archivos de Siigo
- Servidor controlado y protegido por Smoothcloud

Los usuarios se conectan de la siguiente forma:
- El usuario abre Escritorio Remoto
- Ingresa la IP privada del servidor: 192.168.1.5
- Ingresa usuario y contraseña asignados
- Se carga su perfil
- Se abre Siigo desde el servidor
- Trabaja directamente sobre el sistema alojado allí
- No trabaja nada en local, todo sucede dentro del servidor.

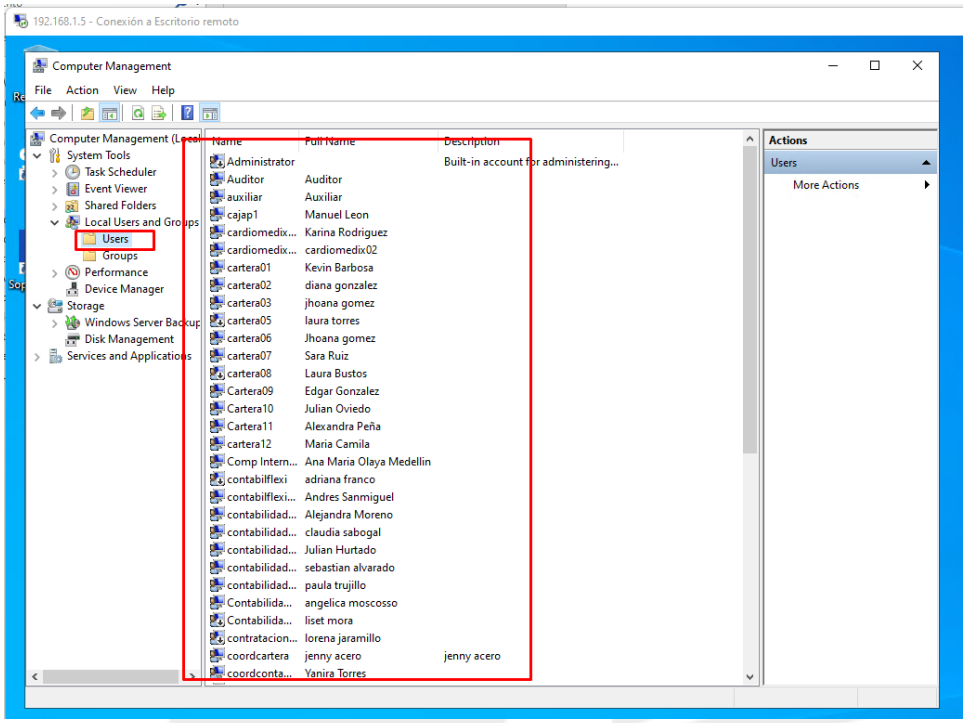
Conexión a escritorio remoto servidor 192.168.1.5 WServer



Escritorio de Servidor remoto acceso a Siigo



Desde el servidor de Windows 192.168.1.5 (WServer RDP) de SIIGO se crean los usuarios para acceso a cada perfil.



Smoothcloud en base a un servidor con pfSense, es el firewall y router avanzado basado en FreeBSD para la protección del servidor donde está alojado Siigo. PfSense solo controla, protege y permite el acceso seguro hacia el servidor donde está instalado Siigo.

Aspecto de Seguridad Información Smoothcloud:

- Hosting de la máquina virtual
- Firewall (pfSense)
- Seguridad de red
- Acceso VPN
- Respaldos
- Monitoreo
- Disponibilidad del servidor
- Administración del entorno cloud

El proveedor no administra Siigo ni los usuarios del hospital, solo lo que tiene que ver con infraestructura.

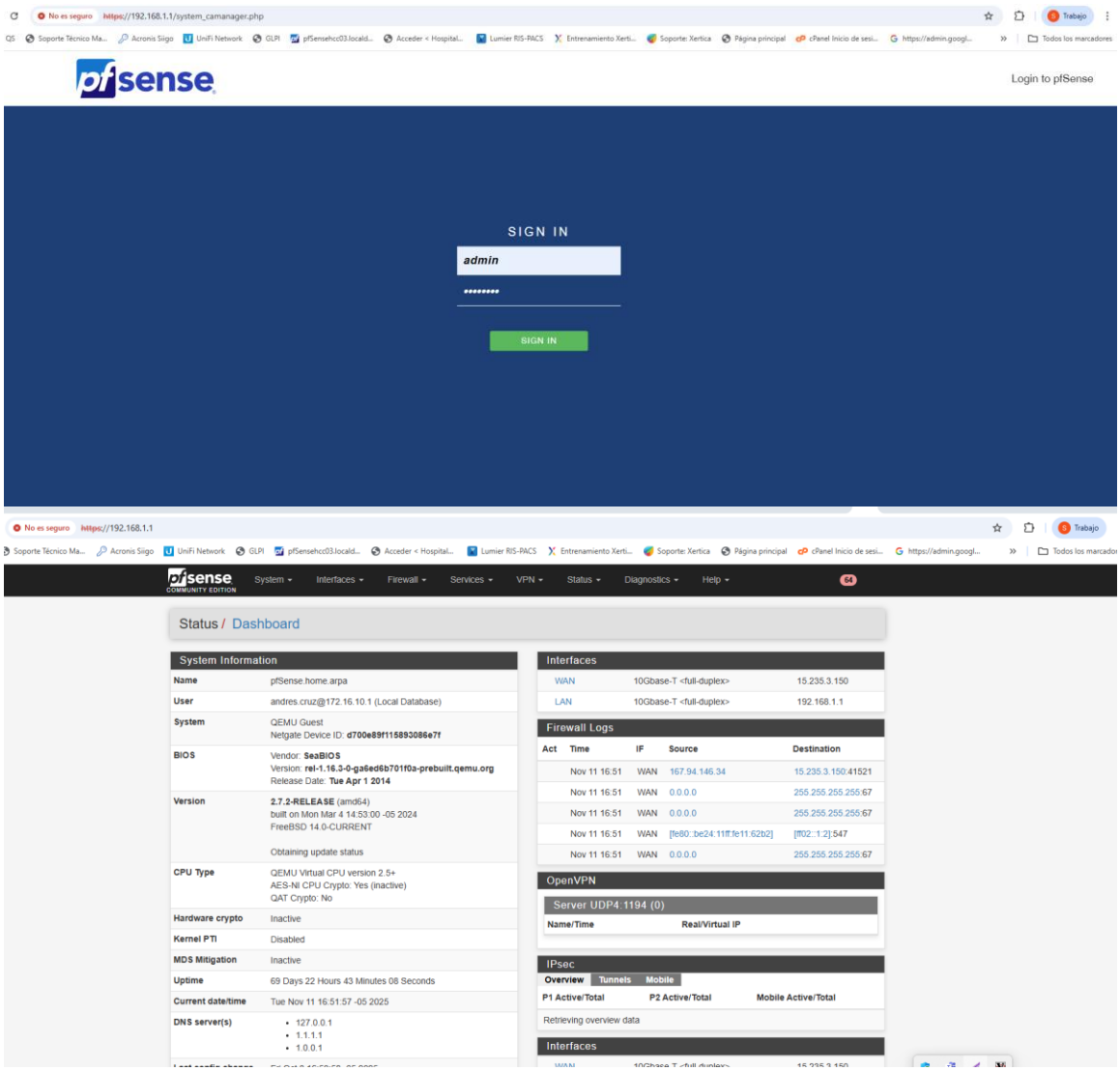
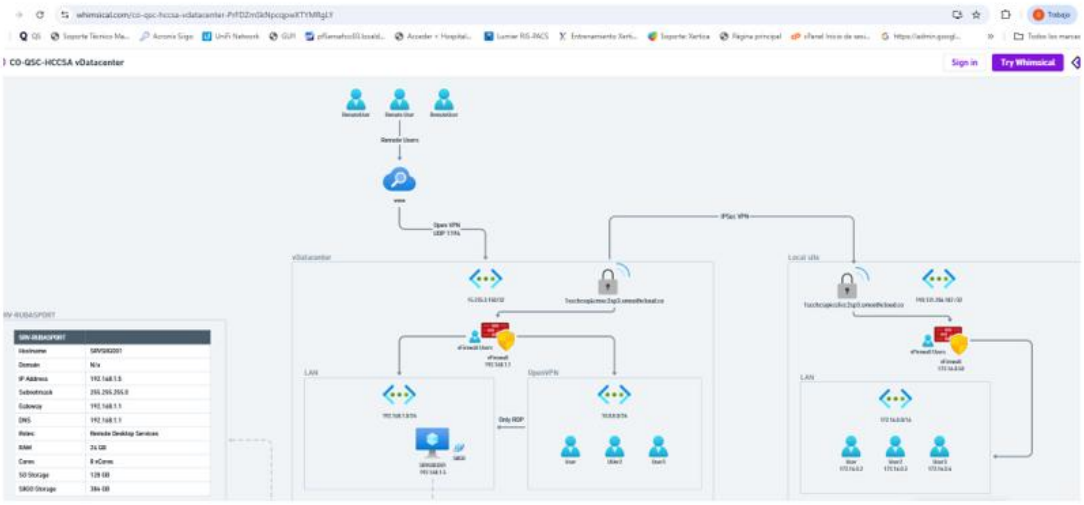


Diagrama de Topología: La topología presentada refleja una arquitectura híbrida cloud–on-premise con control centralizado en un Datacenter Virtual administrado por Smoothcloud, interconectado mediante VPNs (IPSec y OpenVPN) a los sitios locales.



Oportunidad de mejora: Contraseñas de usuarios RDP sin política formalizada

Si los usuarios son administrados por el Hospital Cardiovascular de Cundinamarca, se debe garantizar:

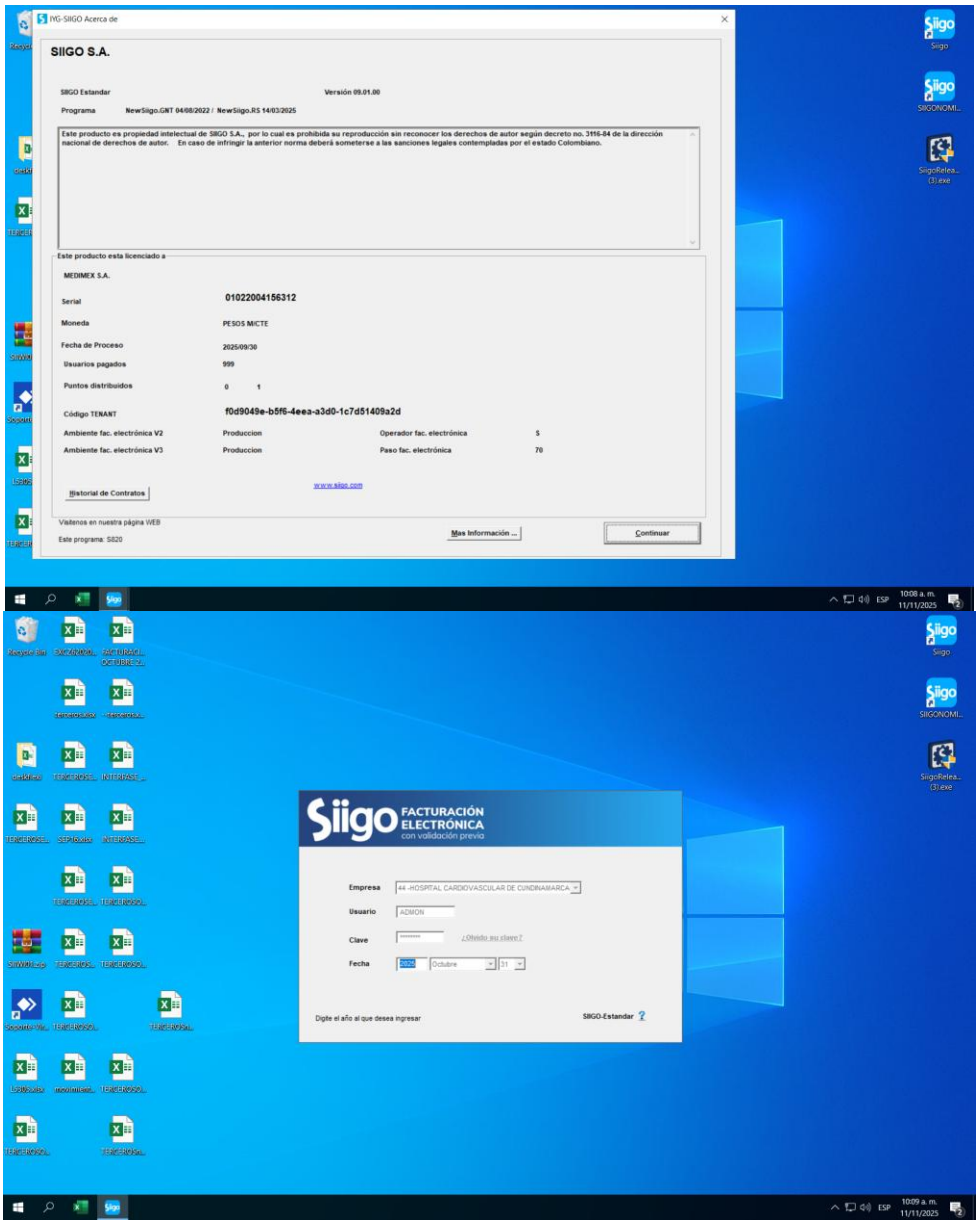
- Longitud mínima
- Expiración
- Historial
- Doble factor si es posible (aunque en RDP suele ser opcional)

Conclusión: La arquitectura presentada corresponde a un modelo de despliegue seguro y funcional para la operación de Siigo en el Hospital Cardiovascular de Cundinamarca, donde el servidor 192.168.1.5 actúa como servidor de aplicaciones RDP y repositorio de los módulos del sistema. Smoothcloud administra exclusivamente la infraestructura cloud, el firewall PfSense, la seguridad de red, la VPN y los respaldos de la VM, mientras que la administración de usuarios RDP corresponde al hospital y la gestión funcional de Siigo. La distribución de responsabilidades es adecuada y acorde al modelo de hosting, aunque se identifican oportunidades de mejora en políticas de contraseñas

- **Situación actual, división y alcance de SIIGO**
  De acuerdo con la verificación realizada, se identifica que SIIGO Pyme en el Hospital Cardiovascular se utiliza únicamente con dos módulos principales:
  - Módulo de Facturación
    - Cuentas por Cobrar (CxC)
    - Cuentas por Pagar (CxP)
    - Tesorería
    - Registros contables

  Este módulo gestiona los movimientos contables derivados de los procesos administrativos y financieros.

  - Módulo de Nómina
    - La nómina se liquida dentro del módulo, mediante formatos preestablecidos (comprobante de pago).
    - No existe integración automática con otros sistemas de talento humano o planta de personal.
    - Los valores o asientos contables se registran de forma manual en el módulo de facturación/contabilidad cuando corresponde.



Oportunidad de mejora: Dado que los módulos de SIIGO Pyme (Facturación y Nómina) operan de manera independiente y no existe integración automática entre ellos, se identifica como oportunidad de mejora la formalización de un procedimiento documentado que describa el flujo manual de información entre ambos módulos. Esto permitiría asegurar consistencia en los registros, reducir errores de digitación y garantizar la trazabilidad de la información que se transfiere manualmente o cargue de archivo planos.

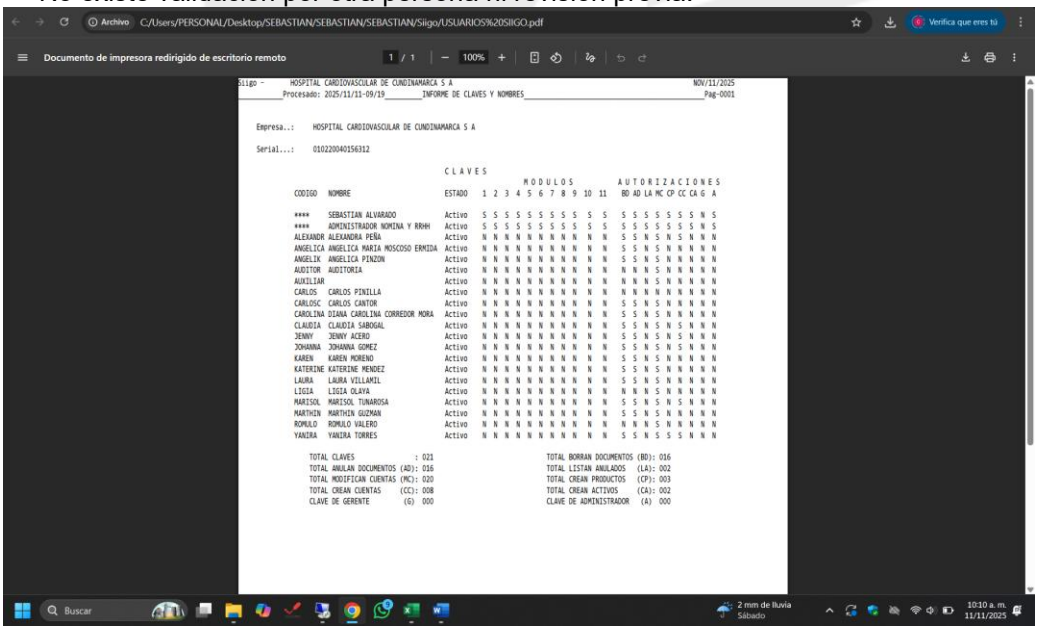
Conclusión: SIIGO Pyme en la entidad se encuentra segmentado únicamente en dos módulos operativos: Facturación y Nómina. El módulo de Facturación integra CxP, CxC, Tesorería y la transmisión de documentos, mientras que el módulo de Nómina realiza la liquidación mediante formatos internos predefinidos, sin integraciones automáticas con sistemas externos. Ambos módulos funcionan de manera independiente y no existe interoperabilidad automatizada entre ellos ni con otras plataformas institucionales.

b) Gestión de Accesos:

- **Procedimiento para la solicitud, aprobación y eliminación de usuarios en SIIGO:**
  A partir de la revisión con el personal del Hospital y la evidencia entregada, se identificó que el proceso de creación, modificación y eliminación de usuarios en SIIGO se realiza de manera informal y sin un procedimiento establecido. El flujo actual funciona así:

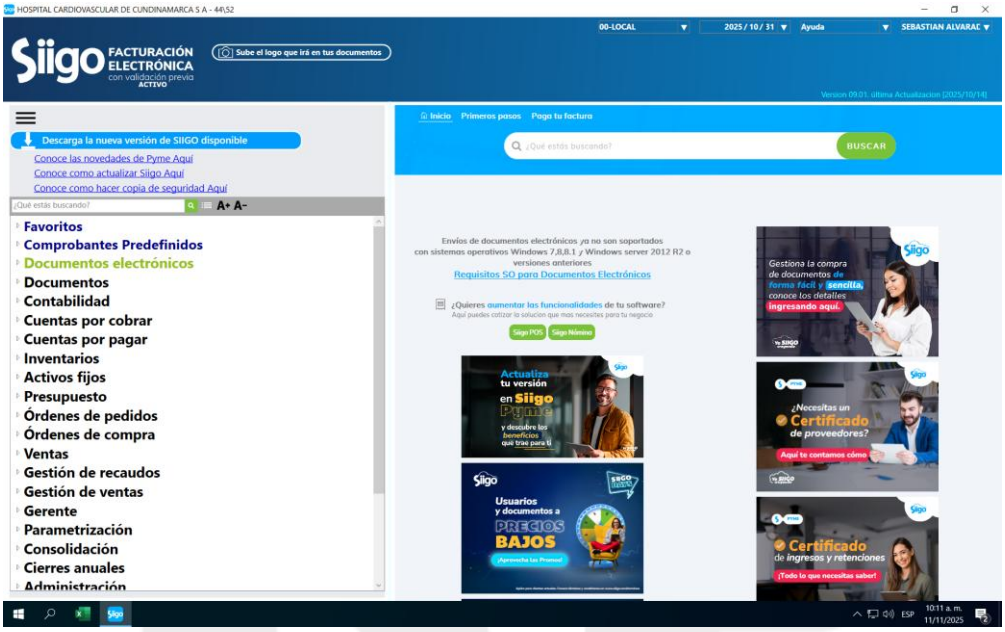
  - Solicitud de creación de usuario
    - Cuando un funcionario nuevo ingresa al área contable, administrativo o financiera, la solicitud se hace verbalmente o por WhatsApp al encargado de SIIGO en contabilidad y encargado de sistemas acceso remoto RDP y VPN.
    - No existe formato, correo formal ni documento que respalde la solicitud.
    - El encargado recibe pantallazos o mensajes informales donde se indica: los datos del funcionario que requiere los permisos.
      - Permisos que "debería tener" (según criterio interno)
    - No existe una trazabilidad sobre la solicitud y creación de usuario.

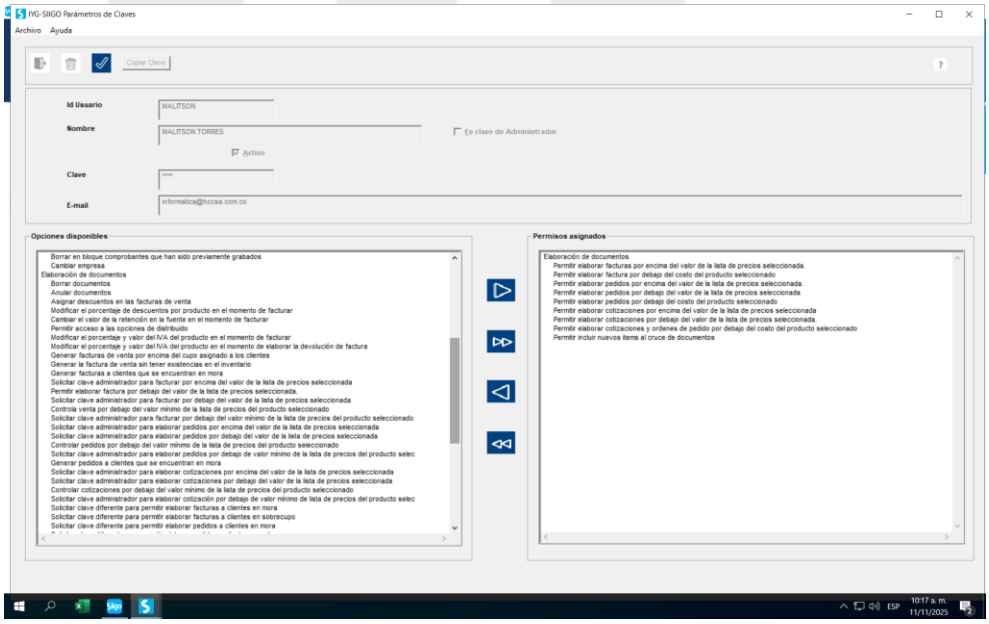
  - Creación del usuario en el sistema
    - El funcionario encargado de SIIGO ingresa al módulo de claves del sistema.
    - Registra manualmente:
      - Código de usuario
      - Nombre
      - Clave temporal
      - Estado del usuario
    - No existe validación por otra persona ni revisión previa.

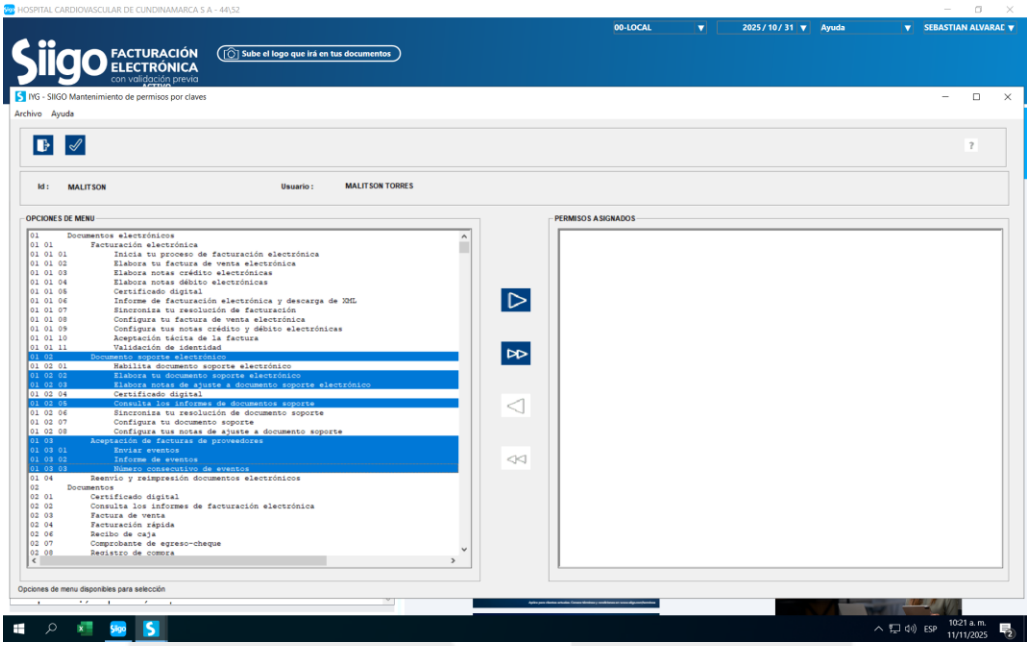


  - Asignación de permisos
    - En SIIGO Pyme no existen roles ni perfiles definidos.
    - El encargado debe entrar opción por opción, seleccionando permisos manuales para cada usuario.
    - Los permisos se asignan según:
      - Experiencia previa
      - Petición verbal
      - Criterio del encargado
    - Los permisos no siguen un estándar ni matriz de responsabilidades.

- No existe evidencia de aprobación de los permisos asignados.







- Modificación de permisos
  - Cuando hay cambios de funciones o tareas, nuevamente la solicitud llega por WhatsApp.
  - El encargado ingresa al usuario y edita permisos individualmente.
  - No se registra:
    - Motivo del cambio
    - Fecha formal de modificación
    - Responsable que lo aprobó
  - Todo queda en memoria o en mensajes informales.

- Eliminación / desactivación de usuarios
  - Cuando un funcionario termina contrato, el área informa por WhatsApp o verbalmente al encargado de Siigo, VPN y escritorio remot RDP.
  - El encargado entra al sistema y desactiva manualmente el usuario.
  - En algunos casos:
    - Los usuarios antiguos quedan visibles como "inactivos"
    - Se elimina la clave dentro de la plataforma
  - No existe acta de retiro, ni ticket, ni correo de cierre de acceso.

  - No se mantiene un registro de cuándo se hizo la eliminación ni quién la solicitó.

- Revisión de usuarios activos
  - No hay revisión periódica documentada.
  - Eventualmente, el encargado envía pantallazos al grupo de WhatsApp para que las jefaturas “verifiquen” quiénes siguen activos.
  - No existen conciliaciones formales ni reportes periódicos.

Hallazgo:

Durante la revisión de la administración de usuarios del sistema SIIGO Pyme, se evidenció que no existe un procedimiento formal documentado para la solicitud, aprobación, asignación, modificación y eliminación de usuarios.

El proceso se realiza de manera informal, según lo informado por el personal, mediante comunicaciones vía WhatsApp, donde se comparten pantallazos de usuarios activos para verificar necesidades de eliminación o activación.

La creación, configuración y desactivación de usuarios se encuentra bajo la responsabilidad exclusiva del funcionario encargado de SIIGO en contabilidad y del Coordinador de Sistemas para acceso al escritorio remoto y VPN, sin requerimientos formales, sin registros de aprobación, y sin evidencia documental que soporte las decisiones.

Se observó además que no existen roles ni perfiles predefinidos, sino que cada usuario recibe permisos individuales sobre documentos o funcionalidades, según experiencia del encargado, lo que implica una administración manual, heterogénea y sin estandarización.

Finalmente, se identificó que cuando un funcionario termina contrato, la eliminación del usuario también se gestiona de forma informal; si bien se elimina de la plataforma, no existe trazabilidad del proceso, ni actas de retiro o evidencias de cierre.

Recomendación:
Se recomienda establecer y formalizar un procedimiento documentado para la administración del ciclo de vida de usuarios de SIIGO, que incluya:

- Formato de solicitud de creación/modificación/eliminación (Practicas de Itil).
- Flujo de aprobación por jefe inmediato o área de talento humano.
- Registro y archivo de evidencias.
- Definición de roles y perfiles estándar (según área, función o proceso).
- Revisión periódica de usuarios y permisos.
- Prohibición del uso de medios informales como WhatsApp para el control de accesos.
- Trazabilidad de bajas de personal (retiros o cambios de rol).

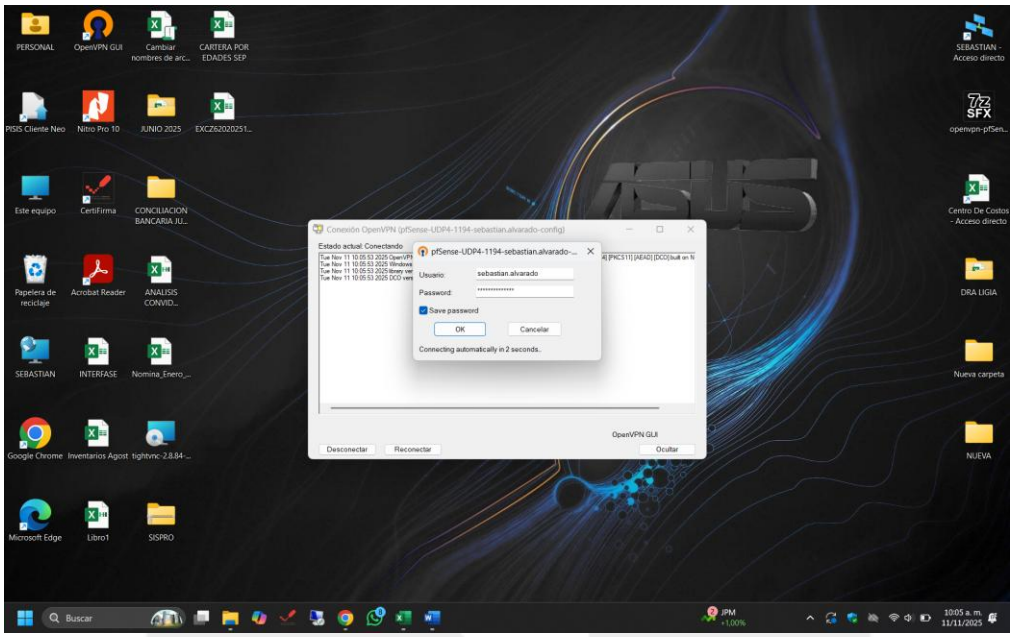
Implementar estos controles permite asegurar la adecuada gestión del acceso, la protección de la información y el cumplimiento normativo.

c) Gestión de Credenciales y Autenticación

- **Configuración de parámetros mínimos de contraseñas (longitud, complejidad, caducidad)**

A partir de la revisión con el personal encargado y las pruebas realizadas en el sistema, se identificó lo siguiente:

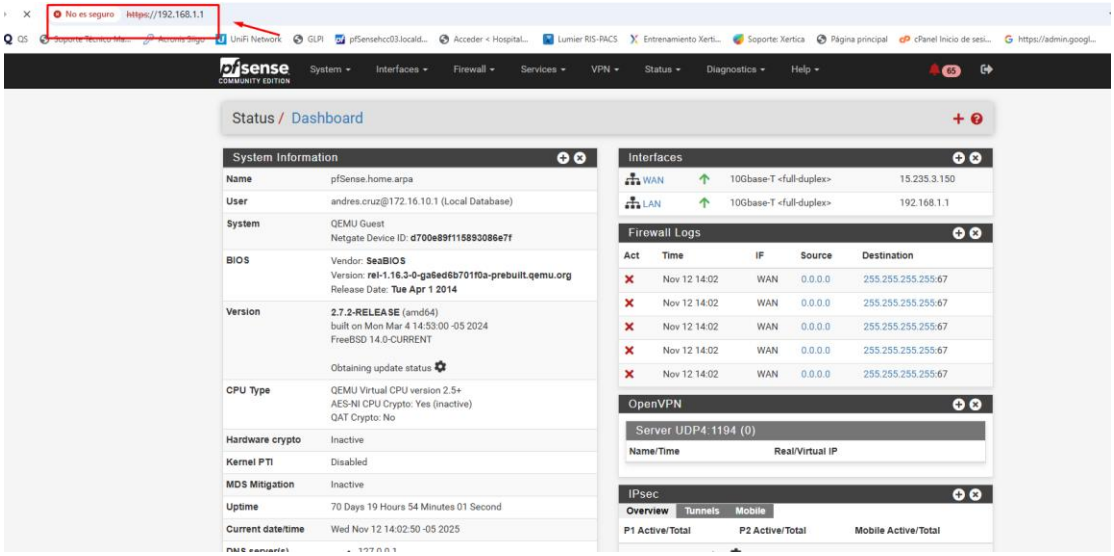
- Longitud permitida: Las contraseñas en SIIGO pueden tener entre 4 y 8 caracteres. No permite contraseñas superiores a 8 caracteres (limitación propia de SIIGO Pyme).
- Complejidad: El sistema sí permite uso de caracteres especiales, números, letras mayúsculas y minúsculas; sin embargo, la complejidad no es obligatoria.
- Caducidad: SIIGO Pyme no tiene configurada caducidad automática de contraseñas. No existe política de expiración periódica.
- Práctica actual de creación de usuarios: Cuando se crea un usuario, se le asigna una contraseña simple como: usuario: marcela Contraseña 1234, al primer ingreso, el sistema obliga al usuario a cambiar la contraseña, pero el cambio sigue limitado a máximo 8 caracteres. No se exige complejidad mínima
- No se establece periodicidad de cambio
- No existe política institucional de contraseñas
- La entidad no tiene documento formal que establezca requisitos de contraseñas.
- No se adoptan lineamientos de seguridad (longitud, historial, caducidad, intentos fallidos, etc.).
- El control se limita a las restricciones técnicas del sistema.



Hallazgo:
Se identificó que el sistema SIIGO Pyme permite contraseñas entre 4 y 8 caracteres, sin requerir complejidad obligatoria ni caducidad periódica. Además, la entidad no cuenta con una política formal de contraseñas que defina los parámetros mínimos de seguridad para la creación, uso y renovación de credenciales.
Las cuentas se crean con claves simples (1234), obligando al usuario a cambiarlas solo en el primer inicio, sin controles adicionales. Esta situación evidencia debilidades en la gestión del acceso y aumenta el riesgo de uso de contraseñas débiles o comprometidas.

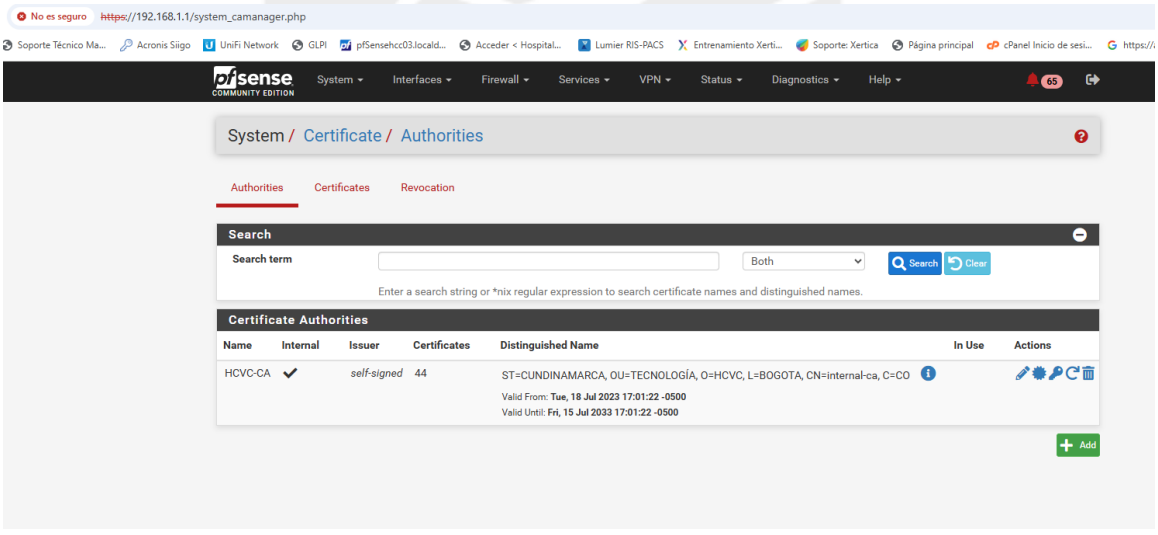
Recomendación: Se recomienda formalizar una **política de contraseñas institucional**, definiendo parámetros mínimos (longitud, complejidad, caducidad, historial, intentos fallidos) y aplicarla a todos los sistemas, incluido SIIGO. Adicionalmente, se sugiere implementar procedimientos complementarios como doble autenticación para accesos remotos (VPN y RDP), sensibilización a usuarios y revisión semestral de la fortaleza de contraseñas.

- **Inicio de sesión seguro (HTTPS / TLS):**
  Al ingresar al firewall pfSense mediante la URL https://192.168.1.1, el navegador muestra el mensaje “No es seguro”.



Sin embargo, esto no significa que la conexión no esté cifrada, significa que:

- El certificado usado es HTTPS, pero no está firmado por una entidad pública (CA pública).
- El certificado es auto firmado o emitido por la autoridad certificadora (CA) interna del mismo pfSense.
- Este certificado sí cifra la conexión entre el navegador y el firewall.
- El navegador lo marca como “no seguro” únicamente porque no puede validar la identidad del servidor con una entidad de confianza pública.
- En las imágenes se evidencia:
  - Una CA interna (HCVC-CA) creada en el firewall.



- Certificados emitidos por esa CA para:
  - El webadmin del firewall
  - Las conexiones VPN
- El algoritmo utilizado es seguro y usa TLS moderno.

En resumen, toda la administración del firewall y las VPN sí utilizan HTTPS/TLS, pero con certificados emitidos localmente.

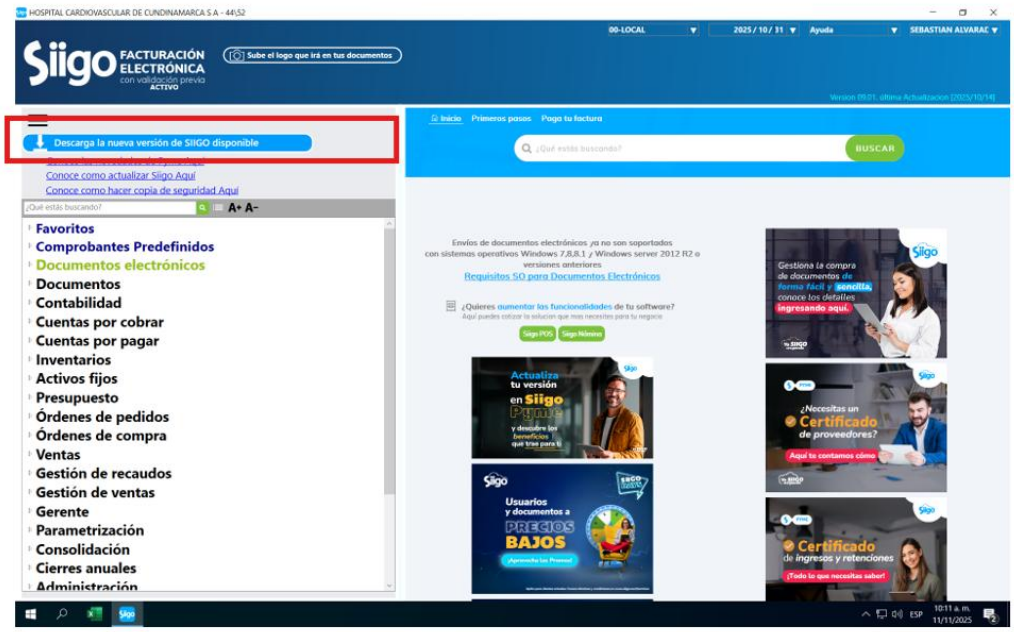
Conclusión:

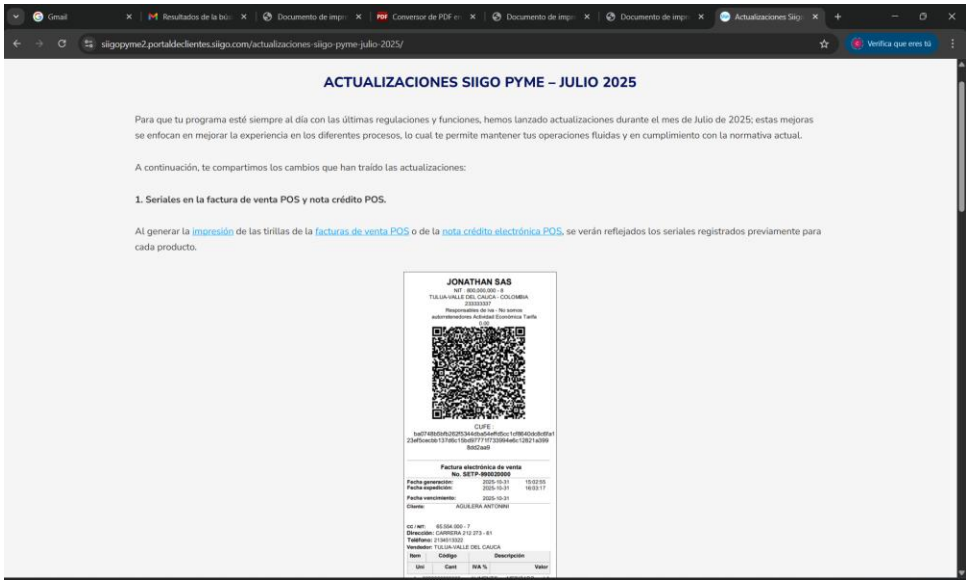
- El firewall pfSense utiliza conexión segura mediante HTTPS/TLS; sin embargo, emplea un certificado auto firmado o emitido por una autoridad certificadora interna, por lo que los navegadores lo marcan como “No seguro”.
- A pesar de la advertencia visual, la conexión está cifrada adecuadamente, tanto para el acceso web del firewall como para las conexiones VPN, ya que se utilizan certificados SSL válidos dentro de la infraestructura interna.
- La alerta del navegador se debe únicamente a que el certificado no proviene de una entidad pública, no a un problema de cifrado o vulnerabilidad.

d) Gestión de Cambios

Durante la revisión del sistema SIIGO Pyme instalado en el servidor 192.168.1.5, se observó la notificación *“Descarga la nueva versión de SIIGO disponible”.* Sin embargo, el proceso de actualización no puede realizarse desde el mismo SIIGO, debido a que:

- El servidor no tiene acceso a Internet para realizar descargas directas desde la aplicación.
- La arquitectura actual (servidor RDP alojado en el cloud privado) mantiene bloqueadas las conexiones externas para evitar riesgos de seguridad.
- El módulo de actualización de SIIGO requiere conectividad hacia los servidores del fabricante, la cual no está habilitada en la configuración del firewall pfSense.





Por este motivo, la actualización debe ejecutarse de forma manual, siguiendo estos pasos:

- Se notifica que hay una nueva versión disponible dentro de SIIGO Pyme.
- Debido a la falta de acceso a Internet no se puede actualizar desde la interfaz del sistema.
- Se coordina una ventana de mantenimiento con el área contable y de acuerdo con la disponibilidad de la versión púbica en la página web del proveedor.
- Todos los usuarios deben salir del sistema y cerrar sesión en Escritorio Remoto.
- Se realiza un reinicio del servidor remoto 192.168.1.5, donde está instalado SIIGO.
- El proceso tarda en promedio 30 minutos, mientras se aplican los ajustes o actualizaciones locales.
- Las actualizaciones suelen realizarse los viernes, en horario no operativo (aprox. 4:00 p.m.), para no afectar la labor del área contable.

Este procedimiento es manual, operativo y depende completamente del administrador del servidor y del encargado de SIIGO.

Oportunidad de mejora:
Se identifica como oportunidad de mejora la formalización de un procedimiento documentado para la actualización de SIIGO, que incluya pasos, responsables, tiempos, validaciones previas y posteriores, y un mecanismo de comunicación a los usuarios. Asimismo, se recomienda evaluar alternativas seguras para facilitar el acceso controlado a las actualizaciones (por ejemplo, habilitación temporal de conectividad restringida o descarga certificada por parte del proveedor), con el fin de optimizar el proceso, reducir dependencia operativa y disminuir impacto en la disponibilidad del servicio.

e) Disponibilidad y Continuidad:

- Análisis de SLA, contingencia y soporte del servicio SIIGO
  - Disponibilidad Garantizada: SmoothCloud garantiza una disponibilidad de infraestructura del 99.95% mensual.
  - Soporte y Respuesta: El soporte estándar se presta 8x5 en idioma español, con tiempo de respuesta de hasta 4 horas hábiles para incidentes que afecten la continuidad del servicio. El soporte avanzado puede contratarse como servicio adicional.
  - Mantenimientos Programados: Los mantenimientos programados se coordinan con el distribuidor mediante notificación previa, quien es responsable de notificar a sus clientes finales. El horario se define junto con el gerente de cuenta.

- El servicio presenta SLA claros de disponibilidad definidos con el proveedor
  El servicio de SIIGO Pyme utilizado por el Hospital Cardiovascular no es un servicio SaaS administrado por Siigo, sino una instalación local del software en un servidor Windows (192.168.1.5) alojado en la infraestructura cloud privada de Smoothcloud.
  Por esta razón:
  - Los únicos SLA formales existentes corresponden a la infraestructura (hosting, firewall, VPN, almacenamiento y disponibilidad del servidor).
  - Smoothcloud establece tiempos de atención por criticidad:
    - Alta: 4 horas hábiles
    - Media: 24 horas
    - Baja: hasta 24 horas hábiles
  - Durante la auditoría se constató que el personal del Hospital desconocía estos SLA, por lo que no existe un uso operativo ni seguimiento formal de dichos tiempos.
  - No se identificó un SLA específico para el funcionamiento del aplicativo SIIGO, ya que este no está bajo soporte directo del proveedor de infraestructura.

  Conclusión:
  Existen SLA para la infraestructura donde está alojado SIIGO, pero no para la operación del aplicativo SIIGO como tal, y estos tiempos no son conocidos por los usuarios ni han sido divulgados internamente.

- Mecanismos de contingencia para continuidad operativa cuando SIIGO no está disponible:
  No se identificó un plan formal de contingencia que permita continuar la operación contable, financiera o administrativa en caso de que SIIGO:
  - Presente indisponibilidad
  - Tenga errores funcionales
  - Requiera mantenimiento
  - Deba reiniciarse o no sea accesible por problemas del servidor o VPN.
  -

  Si bien Smoothcloud garantiza continuidad a nivel de infraestructura (replicación, respaldo, disponibilidad del vDatacenter), la continuidad operativa depende totalmente del servidor 192.168.1.5, y no existe un procedimiento que defina:
  - Actividades autorizadas durante la caída
  - Controles manuales temporales
  - Mecanismos de validación de información
  - Uso de formatos alternos
  - Responsables de activar la contingencia o procesos de reanudación.

  Conclusión:
  No existen mecanismos documentados de contingencia para mantener la operación cuando SIIGO no está disponible, por lo que la continuidad operativa no está garantizada frente a fallas del aplicativo o del servidor.

- Canal documentado de soporte y escalamiento
  El proveedor Smoothcloud cuenta con un canal de soporte formal para incidentes de infraestructura mediante su mesa de ayuda (helpdesk), con horarios y tiempos de atención definidos; sin embargo, este soporte no cubre SIIGO como aplicativo en la documentación revisada.

  No existe un documento institucional que establezca el proceso de soporte funcional de SIIGO ni los pasos para escalamiento interno o externo.

En la práctica, los incidentes de SIIGO se gestionan de manera **informal**, directamente entre el

administrador de Siigo, el administrador del servidor y el proveedor de SIIGO, sin registro ni procedimiento estandarizado.

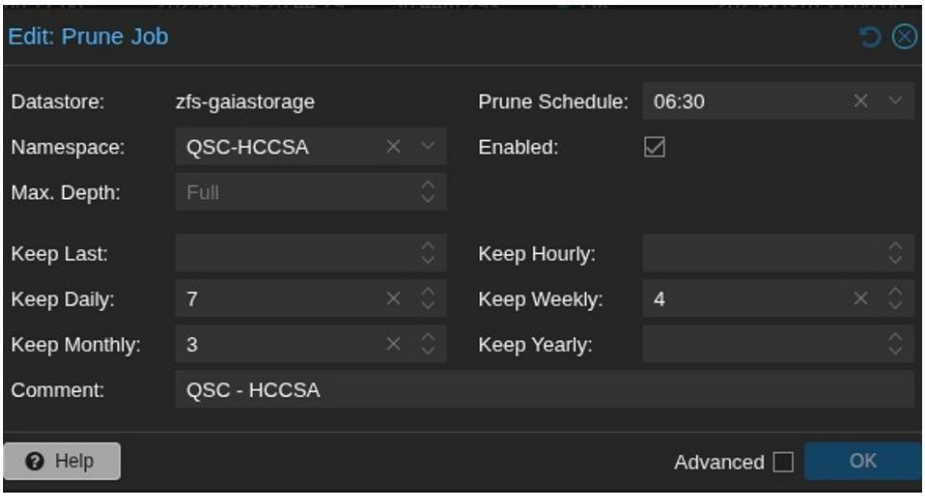
Conclusión:
Existe un canal formal solo para soporte de infraestructura, pero no existe un canal documentado ni procedimiento de escalamiento para incidentes del aplicativo SIIGO.

f) Respaldo y recuperación

Según el documento del proveedor Smoothcloud, el entorno donde está alojado el servidor 192.168.1.5 que contiene la instalación de SIIGO sí cuenta con un esquema robusto de respaldo y recuperación, el cual incluye:

- Copias de seguridad (Backups) diarias, semanales y mensuales
  En el documento se evidencia lo siguiente:
  - 7 copias diarias
  - 4 copias semanales
  - 3 copias mensuales

Programación de la tarea de backup para el tenant del hospital, 7 diarios, 4 semanales y 3 mensuales, es la política de retención.



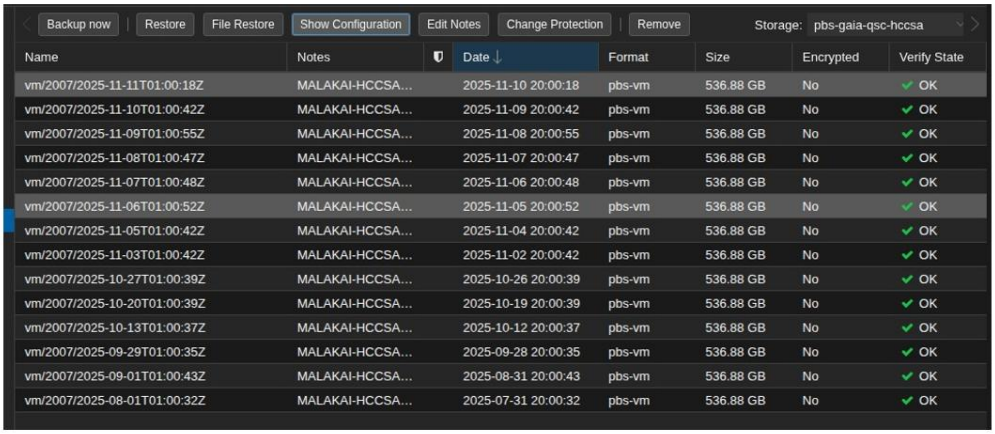
Esto corresponde a la política de retención definida por Smoothcloud, claramente documentada:
"*La programación de la tarea de backup para el tenant del hospital, 7 diarios, 4 semanales y 3 mensuales, es la política de retención*."

- Copias de seguridad (Backups) diarias, semanales y mensuales
  - Smoothcloud realiza verificación automática de integridad, lo cual garantiza que las copias no estén corruptas y puedan restaurarse cuando sea necesario.
  - El documento indica:
    "Se evidencian las copias de seguridad y su estado de verificación de integridad (lo que garantiza que la copia de seguridad tiene viabilidad para ser restaurada y no está corrupta)."

    "La evidencia de la configuración de los Jobs que verifican diariamente todas las copias de seguridad para garantizar su integridad… Se hace una verificación de la copia diaria, y nuevamente se agenda a los 30 días."

- Esto confirma que los backups son auditados y validados de forma continua.
- El proveedor indica que el almacenamiento del datacenter utiliza tecnología de triple replicación, lo que significa que, ante fallas de hardware o corrupción del disco, la información sigue disponible. *"El almacenamiento del datacenter tiene triple replicación para garantizar la continuidad de negocio."*
- Además de la triple replicación local, los respaldos se guardan en dos datacenters adicionales, aumentando enormemente la capacidad de recuperación ante desastres.

Se evidencian las copias de seguridad y su estado de verificación de integridad (Lo que garantiza que la copia de seguridad tiene viabilidad para ser restaurada y no está corrupta):



Name	Notes	Date	Format	Size	Encrypted	Verify State
vm/2007/2025-11-11T01:00:18Z	MALAKAI-HCCSA...	2025-11-10 20:00:18	pbs-vm	536.88 GB	No	OK
vm/2007/2025-11-10T01:00:42Z	MALAKAI-HCCSA...	2025-11-09 20:00:42	pbs-vm	536.88 GB	No	OK
vm/2007/2025-11-09T01:00:55Z	MALAKAI-HCCSA...	2025-11-08 20:00:55	pbs-vm	536.88 GB	No	OK
vm/2007/2025-11-08T01:00:47Z	MALAKAI-HCCSA...	2025-11-07 20:00:47	pbs-vm	536.88 GB	No	OK
vm/2007/2025-11-07T01:00:48Z	MALAKAI-HCCSA...	2025-11-06 20:00:48	pbs-vm	536.88 GB	No	OK
vm/2007/2025-11-06T01:00:52Z	MALAKAI-HCCSA...	2025-11-05 20:00:52	pbs-vm	536.88 GB	No	OK
vm/2007/2025-11-05T01:00:42Z	MALAKAI-HCCSA...	2025-11-04 20:00:42	pbs-vm	536.88 GB	No	OK
vm/2007/2025-11-03T01:00:42Z	MALAKAI-HCCSA...	2025-11-02 20:00:42	pbs-vm	536.88 GB	No	OK
vm/2007/2025-10-27T01:00:39Z	MALAKAI-HCCSA...	2025-10-26 20:00:39	pbs-vm	536.88 GB	No	OK
vm/2007/2025-10-20T01:00:39Z	MALAKAI-HCCSA...	2025-10-19 20:00:39	pbs-vm	536.88 GB	No	OK
vm/2007/2025-10-13T01:00:37Z	MALAKAI-HCCSA...	2025-10-12 20:00:37	pbs-vm	536.88 GB	No	OK
vm/2007/2025-09-29T01:00:35Z	MALAKAI-HCCSA...	2025-09-28 20:00:35	pbs-vm	536.88 GB	No	OK
vm/2007/2025-09-01T01:00:43Z	MALAKAI-HCCSA...	2025-08-31 20:00:43	pbs-vm	536.88 GB	No	OK
vm/2007/2025-08-01T01:00:32Z	MALAKAI-HCCSA...	2025-07-31 20:00:32	pbs-vm	536.88 GB	No	OK

Conclusión: El entorno donde se aloja SIIGO cuenta con un esquema de respaldo robusto administrado por Smoothcloud, el cual incluye copias de seguridad diarias, semanales y mensuales, verificación automática de integridad, almacenamiento con triple replicación y replicación adicional en dos datacenters. Esto garantiza disponibilidad de restauración ante fallas del servidor, del sistema de archivos o del almacenamiento.

g) Integridad y Trazabilidad

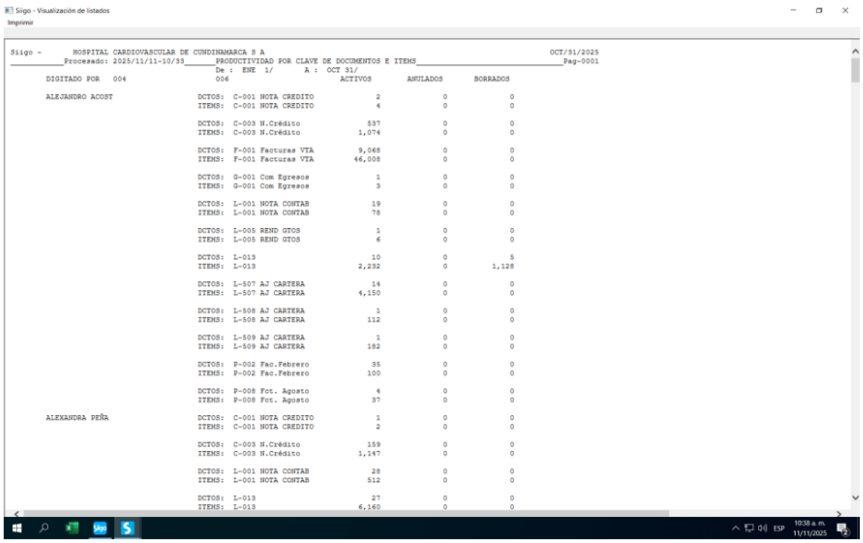
El seguimiento se realiza directamente sobre cada documento, verificando de manera individual las modificaciones aplicadas, los eventos registrados y los cambios efectuados en su ciclo de vida.
En este proceso se valida la integridad, confirmando que la información contenida en el documento no haya sido alterada de manera no autorizada, y que los datos se mantengan completos, exactos y coherentes con el registro original.
Así mismo, se revisa la trazabilidad, identificando las acciones realizadas sobre el documento, los usuarios que intervinieron, la fecha y hora de los cambios y el historial de versiones, cuando el sistema lo permite.
Este método permite garantizar que cada modificación esté debidamente soportada y que exista claridad respecto al flujo de gestión del documento, asegurando transparencia, control y confiabilidad en los procesos evaluados.

HISTÓRICO DE DOCUMENTOS CON PERSONAL QUE NO ESTÁ ACTIVO
La evidencia muestra un listado de documentos elaborados, anulados o borrados por usuarios que hoy ya no se encuentran activos en la institución. En el ejemplo aparecen usuarios como *Alejandro Acost* y *Alexandra Peña*, con registros históricos asociados a diferentes tipos de documentos contables, cartera, notas crédito, ingresos, etc.
Esto permite concluir lo siguiente:

- El sistema no elimina los registros creados por el usuario al desactivarlo.
- Se puede identificar qué usuario creó qué documento, incluso después de retirado.

- Permite auditoría retrospectiva y reconstrucción de eventos si es necesario.

Histórico de documentos con personal que no esta activo



Siigo - Visualización de listados
Imprimir

Siigo - HOSPITAL CARDIOVASCULAR DE CUNDINAMARCA S A OCT/31/2025
Procesado: 2025/11/11-10/33 PRODUCTIVIDAD POR CLAVE DE DOCUMENTOS E ITEMS Pag-0001
De : ENE 1/ A : OCT 31/

DIGITADO POR 004		ACTIVOS	ANULADOS	BORRADOS
ALEJANDRO ACOST	DCTOS: C-001 NOTA CREDITO	2	0	0
	ITEMS: C-001 NOTA CREDITO	4	0	0
	DCTOS: C-003 N.Crédito	537	0	0
	ITEMS: C-003 N.Crédito	1,074	0	0
	DCTOS: F-001 Facturas VTA	9,068	0	0
	ITEMS: F-001 Facturas VTA	46,008	0	0
	DCTOS: G-001 Com Egresos	1	0	0
	ITEMS: G-001 Com Egresos	3	0	0
	DCTOS: L-001 NOTA CONTAB	19	0	0
	ITEMS: L-001 NOTA CONTAB	78	0	0
	DCTOS: L-005 REND GTOS	1	0	0
	ITEMS: L-005 REND GTOS	6	0	0
	DCTOS: L-013	10	0	5
	ITEMS: L-013	2,232	0	1,128
	DCTOS: L-507 AJ CARTERA	14	0	0
	ITEMS: L-507 AJ CARTERA	4,150	0	0
	DCTOS: L-508 AJ CARTERA	1	0	0
	ITEMS: L-508 AJ CARTERA	112	0	0
	DCTOS: L-509 AJ CARTERA	1	0	0
	ITEMS: L-509 AJ CARTERA	182	0	0
	DCTOS: P-002 Fac.Febrero	35	0	0
	ITEMS: P-002 Fac.Febrero	100	0	0
	DCTOS: P-008 Fct. Agosto	4	0	0
	ITEMS: P-008 Fct. Agosto	37	0	0
ALEXANDRA PEÑA	DCTOS: C-001 NOTA CREDITO	1	0	0
	ITEMS: C-001 NOTA CREDITO	2	0	0
	DCTOS: C-003 N.Crédito	159	0	0
	ITEMS: C-003 N.Crédito	1,147	0	0
	DCTOS: L-001 NOTA CONTAB	28	0	0
	ITEMS: L-001 NOTA CONTAB	512	0	0
	DCTOS: L-013	27	0	0
	ITEMS: L-013	6,160	0	0

ESP 10:38 a. m. 11/11/2025

ANÁLISIS DE COMPROBANTES BORRADOS, ANULADOS Y MODIFICADOS EN SIIGO
Las siguientes imágenes muestran reportes generados desde SIIGO Pyme donde se listan los comprobantes que han sido borrados, anulados o modificados en diferentes fechas. Esto permite realizar varias observaciones importantes en términos de control interno, integridad y trazabilidad:

SIIGO conserva trazabilidad de operaciones sensibles, los reportes evidencian:

- Tipo de documento
- Comprobante
- Fecha
- Motivo (BORRADO / ANULACIÓN / MODIFICADO)
- Usuario que realizó la acción
- Cuenta contable afectada
- Descripción del movimiento
- Débitos y créditos
- Código consecutivo

Esto confirma que SIIGO sí registra operaciones de alto riesgo, lo cual es positivo desde el punto de vista de auditoría y permite reconstruir eventos.

Se evidencia volumen de operaciones críticas
En los reportes aparecen:

- Movimientos contables sensibles
- Notas contables modificadas
- Ajustes
- Documentos de cartera
- Comprobantes con impacto financiero

Esto demuestra que usuarios tienen capacidad de realizar operaciones que afectan estados financieros, por lo que se requiere mayor segregación de funciones y flujos de aprobación.

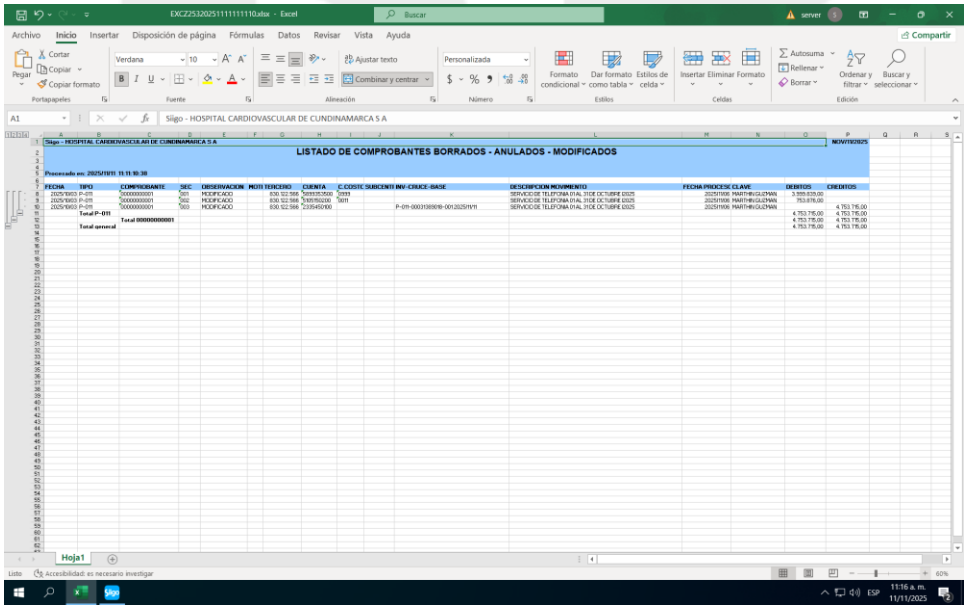
Oportunidad de mejora:
No existe control formal sobre quién puede borrar, anular o modificar
Aunque el sistema registra la acción, el proceso de autorización es inexistente:

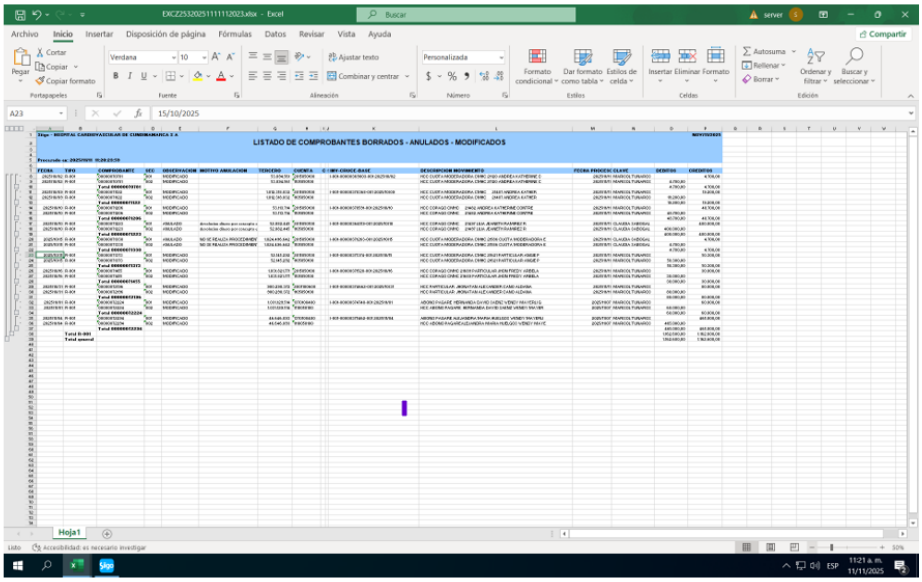
- No hay un flujo de aprobación TI
- No hay una validación previa
- Un usuario con permiso puede modificar o borrar documentos directamente
- No se identificó política formal que regule el uso de estas funciones

Esto coincide con los hallazgos previos sobre falta de procedimientos formales de permisos y roles.

Riesgo: manipulación, corrección no autorizada o borrado indebido de documentos contables, afectando la integridad de la información financiera.

Conclusión
El sistema SIIGO registra y permite la exportación de comprobantes borrados, anulados o modificados, lo que garantiza trazabilidad técnica; sin embargo, no existe control formal para regular estas acciones ni evidencia de revisión periódica. Las modificaciones pueden ser realizadas directamente por los usuarios con permisos asignados, sin flujo de aprobación ni segregación de funciones, lo que representa un riesgo para la integridad de la información contable.

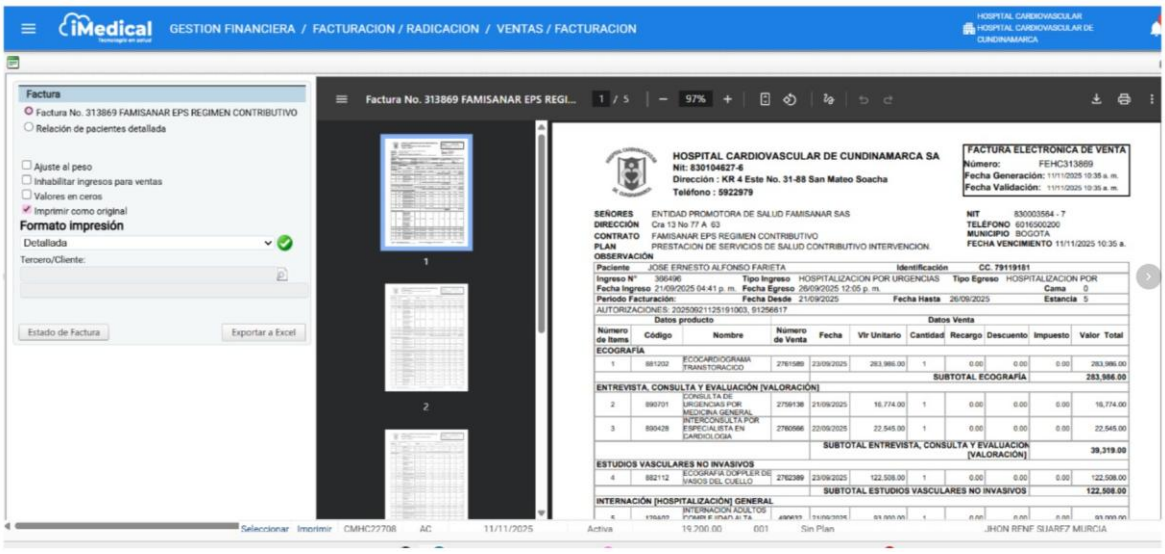




h) Cumplimiento normativo

Durante la revisión de los aspectos asociados al cumplimiento normativo, se validó específicamente el proceso de facturación electrónica, verificando la herramienta utilizada para la generación, transmisión y validación de los documentos electrónicos exigidos por la DIAN.
Se constató que la facturación electrónica no se realiza a través del sistema SIIGO, sino mediante la plataforma IMedical Cloud, es la herramienta que tienen para emitir las facturas electrónicas y transmitirlas a los proveedores y usuarios finales en cumpliendo con los requisitos legales vigentes.
Por tanto, SIIGO no interviene en el proceso normativo de facturación electrónica, y su uso se limita a la operación contable interna y los registros administrativos del Hospital.

Factura electrónica Imedical Cloud:



CONCLUSIONES DE LA REUNIÓN

En el marco del entendimiento realizado sobre el funcionamiento de la plataforma SIIGO se obtuvo la información correspondiente (fotos, archivos, registros) solicitados. No obstante, con la información disponible se procede con la revisión y análisis, con el fin de determinar oportunidades de mejora o confirmar que la plataforma SIIGO cumple adecuadamente con los criterios técnicos a nivel de software y hardware.

COMPROMISOS O ACTIVIDADES PENDIENTES

No Aplica

COMPROMISOS DE LA REUNIÓN

ITEM	ACTIVIDAD	RESPONSABLE	FECHA DE ENTREGA
1			
2			