DOCUMENTO FASE 2
CENTRALIZACIÓN Y SEGURIDAD DE LA INFORMACIÓN

Los ocho componentes previstos para la Fase 2 se encuentran atendidos y verificados sobre el ambiente de producción. Siete corresponden a funcionalidades implementadas; el octavo - permisos por área - quedó resuelto mediante el modelo de perfiles, conforme a la estructura organizacional confirmada por S&J Salud.

Componente	Estado	Verificación
Gestión centralizada de documentos	Implementado	20 categorías y 56 tipos documentales en producción
Control de acceso por usuarios	Implementado	Cinco perfiles con matriz de permisos aplicada en el servidor
Permisos por área	Resuelto	Atendido mediante los perfiles funcionales; ver capítulo 4.3
Historial de modificaciones	Implementado	Registro campo por campo, con valor anterior y nuevo
Control de versiones	Implementado	Versionado en la plataforma y en el almacenamiento
Respaldo automático	Implementado	Base de datos, archivos y servidor, con copia en región separada
Auditoría de accesos	Implementado	Consulta, descarga, edición, permisos y autenticación
Políticas de recuperación	Implementado	Política documentada y restauración probada

2. Infraestructura implementada

La solución opera sobre infraestructura en la nube de Amazon Web Services, en la región Norte de Virginia (us-east-1), bajo una cuenta dedicada.

Componente	Servicio	Configuración de seguridad
Aplicación	Servidor EC2 dedicado	Sin acceso remoto por SSH; administración por sesión auditada
Base de datos	RDS PostgreSQL 18.4	Cifrada, sin acceso público, con protección contra eliminación
Documentos	Almacenamiento S3	Cifrado, versionado y sin acceso público
Interfaz web	AWS Amplify	Publicación automática y cifrado en tránsito (HTTPS)
Correo	Amazon SES	Notificaciones de vencimiento documental

2.1 Repositorio centralizado

Toda la documentación se almacena en un repositorio único en la nube. Los archivos no son accesibles públicamente: cada consulta genera un enlace temporal, individual y de corta duración, emitido únicamente para el usuario que lo solicita y registrado en la auditoría.

Cifrado: los archivos se cifran en reposo con cifrado gestionado por AWS;
Acceso público bloqueado: las cuatro banderas de bloqueo de acceso público están activas;
Versionado de objetos: una sobrescritura no destruye la versión anterior del archivo.

3. Estructura documental organizada

La clasificación documental opera en dos niveles: una categoría maestra agrupa los tipos documentales que le pertenecen, y las reglas de reserva se definen sobre la categoría.

3.1 Convención de nombres

Los archivos se renombran automáticamente al cargarse, siguiendo la siguiente convención:

[TIPO_ID]_[NÚMERO_ID]_[TIPO_DOCUMENTAL]_[FECHA]_[VERSIÓN]

Los documentos de gestión operativa usan una convención distinta, basada en el código del instrumento y el período, sin número de identificación: no corresponden a ninguna persona.

4. Configuración de permisos

El acceso se controla por perfil. La autenticación emite credenciales de vigencia limitada y la sesión expira por inactividad; el cierre de sesión invalida la credencial de forma inmediata y queda registrado.

Se implementaron los cinco perfiles definidos en el capítulo 5 de la Configuración de Permisos, con la matriz del capítulo 6 aplicada en el servidor.

Perfil	Expediente	Catálogos	Aprobar	Retirar	Cuentas	Auditoría	Salarios
ROL-01 Administrador de plataforma	Sí	Sí	Sí	Sí	Sí	Sí	Sí
ROL-02 Dirección de Recursos Humanos	Sí	Sí	Sí	Sí	No	Sí	Sí
ROL-03 Analista de Recursos Humanos	Sí	Consulta	No	No	No	No	Autorizado
ROL-04 Dirección / Área de Nómina	Consulta	Consulta	No	No	No	No	Sí
ROL-05 Auditor	Consulta	Consulta	No	No	No	Sí	No

La matriz opera de forma restrictiva: un recurso que no ha sido concedido a un perfil es un recurso al que ese perfil no accede. Incorporar una funcionalidad sin decidir quién puede usarla la deja cerrada, no abierta.

El control se aplica en el servidor, no en la interfaz. Un perfil sin permiso de escritura recibe un rechazo del servidor aunque intente la operación por fuera de la aplicación.

4.1 Reserva de la información salarial

El salario es el dato más sensible del registro de personal. La plataforma lo excluye del envío para los perfiles que no pueden verlo: el dato no se oculta en pantalla, no se transmite. La auditoría registra que un salario cambió y quién lo cambió, nunca el monto.

4.2 La consulta no autoriza la copia

La regla PER-RN-013 separa el derecho a consultar del derecho a descargar. La distinción importa donde más pesa: alguien puede necesitar leer una fecha en una historia clínica para tramitar una incapacidad sin que el archivo salga de la plataforma.

Descargar un documento clasificado en una categoría confidencial —niveles 3 y 4— exige una autorización explícita sobre la cuenta, que concede la administración y queda registrada. Comprende, entre otros, historias clínicas, exámenes médicos, documentos de identidad, afiliaciones y soportes de cesantías.

El rechazo también se registra, como descarga denegada. Un registro que solo muestra quién obtuvo una copia no puede mostrar quién lo intentó y fue detenido, y esa es la evidencia que sirve ante una revisión.

La interfaz señala el documento como reservado en lugar de permitir el intento: quien consulta el expediente ve la restricción explicada, no un error.

4.3 Permisos por área

Los permisos por área se resolvieron mediante los perfiles funcionales.

Al confirmarse que las áreas de la organización corresponden a la Dirección de Recursos Humanos y a la Dirección de Nómina, y que el personal asistencial se organiza por sede y por servicio y no por área administrativa, no se requiere una segmentación adicional: cada una de esas áreas es un perfil con permisos propios, aplicados en el servidor y verificados en producción.

El nivel de confidencialidad de cada categoría documental se encuentra registrado y opera ya sobre la descarga de documentos reservados. Su aplicación a la consulta queda sujeta a que S&J Salud defina las cuentas autorizadas.

5. Historial de modificaciones y control de versiones

5.1 Historial de modificaciones

Toda modificación queda registrada campo por campo, con el valor anterior y el nuevo, el usuario responsable, la fecha y la dirección de origen. El registro es de solo escritura: la plataforma no permite modificar ni eliminar una línea del historial, ni siquiera a un administrador.

5.2 Control de versiones

El versionamiento opera en dos planos independientes:

En la plataforma: al cargar un documento del mismo tipo para la misma persona, la plataforma lo registra como una nueva versión y conserva el vínculo con la anterior, que permanece disponible.

En el almacenamiento: el repositorio conserva las versiones anteriores de cada objeto, de modo que una sobrescritura accidental es reversible.

El expediente muestra la versión vigente de cada documento y quién la incorporó, sin necesidad de abrir el archivo.

6. Auditoría de accesos

La plataforma registra automáticamente los siguientes eventos:

Evento registrado	Qué queda
Consulta	Quién abrió el expediente de quién, y cuándo
Descarga	Quién solicitó copia de qué documento
Edición	Campo modificado, con valor anterior y nuevo
Eliminación lógica	Registrada como tal, distinguida de una edición
Cambio de permisos	Alta y baja de perfiles sobre una cuenta
Autenticación	Ingreso exitoso, intento fallido y cierre de sesión

El intento fallido se registra deliberadamente: una serie de intentos contra un mismo correo es la única señal que un registro de auditoría puede dar sobre un acceso no autorizado en curso.

La consulta está disponible en la plataforma, filtrable por tipo de evento, usuario, registro afectado y fecha, con acceso restringido a la administración.

7. Estrategia de respaldo

El respaldo cubre los tres elementos que componen el servicio: la base de datos, los archivos documentales y el servidor de aplicación. Los tres son automáticos y no requieren intervención manual.

Elemento	Mecanismo	Frecuencia	Retención	Ubicación
Base de datos	Respaldo automático gestionado	Diario	30 días	Región principal
Base de datos	Recuperación a un instante exacto	Continua	30 días	Región principal
Base de datos	Copia lógica cifrada	Diaria, 06:15 UTC	30 días	Región secundaria
Base de datos	Copia lógica semanal	Domingos	12 semanas	Región secundaria
Base de datos	Copia lógica mensual	Día 1	12 meses	Región secundaria
Documentos	Versionado de objetos	En cada cambio	Permanente	Región principal
Servidor	Imagen del disco	Diaria, 06:00 UTC	30 días	Región principal

7.1 Separación del entorno productivo

Las copias lógicas de la base de datos se depositan en un repositorio situado en una región distinta a la de producción. Responde al principio de separación: un incidente que alcance el entorno productivo no alcanza simultáneamente sus respaldos.

El servidor de producción posee permiso para escribir sus copias, pero no para eliminarlas. La restricción se verificó de forma explícita: un intento de borrado desde el propio servidor es rechazado. En consecuencia, un compromiso del entorno productivo no permite destruir el historial de respaldos.

7.2 Recuperación a un instante exacto

Además del respaldo diario, la base de datos permite restaurar su estado a cualquier momento dentro de la ventana de retención, con precisión de segundos. Esto cubre el caso más frecuente en la práctica: un borrado o una actualización equivocada que se detecta horas después, y para el cual un respaldo de la noche anterior implicaría perder el trabajo del día.

7.3 Alcance de la protección

- **Base de datos:** respaldo diario y recuperación puntual, 30 días.
- **Documentos:** cada versión anterior se conserva; una sobrescritura o un borrado son reversibles sin límite de tiempo.
- **Servidor:** imagen diaria del disco. La reconstrucción del servidor no depende de reinstalar nada a mano.
- **Configuración y código:** el código fuente reside en repositorios versionados, independientes de la infraestructura.
- **Copia separada:** diaria, semanal y mensual en una región distinta, con acceso de solo escritura desde producción.

8. Observabilidad y monitoreo

La operación se vigila de forma automática. Una falla que nadie advierte se descubre durante un incidente, que es el peor momento para enterarse.

Qué se vigila	Mecanismo	Frecuencia	Aviso
Que la aplicación responda	Chequeo externo sobre /healthz	5 minutos	Correo
Que la base de datos y la caché funcionen	Chequeo externo sobre /readyz	5 minutos	Correo
Que la interfaz esté publicada	Chequeo externo de contenido	5 minutos	Correo
Errores de la aplicación	Sentry	Continuo	Panel y correo
Que el respaldo se ejecute	Verificación del repositorio externo	Diaria	Correo

8.1 Disponibilidad

Se distinguen dos preguntas que suelen confundirse. Una comprueba que el servidor responde; la otra, que la plataforma puede efectivamente trabajar, verificando la base de datos y la caché. Un monitoreo que solo mirara lo primero reportaría todo en orden mientras Recursos Humanos no puede abrir un solo expediente.

8.2 Registro de errores

Los errores de producción se reportan de forma centralizada, con una salvedad: un reporte de error es una copia de la información que estaba en uso cuando algo falló, y en esta base eso comprende cédulas, salarios e historias clínicas. Los datos personales se depuran antes de que el reporte salga del servidor. Un reporte de fallo no es un destino lícito para un diagnóstico.

8.3 Vigilancia del respaldo

Se verifica a diario que el repositorio externo haya recibido una copia reciente, y se avisa cuando no. La verificación consulta el repositorio y no el servidor que escribe en él: un servidor que dejó de ejecutar su respaldo no es una fuente confiable para reportar que dejó de hacerlo.

9. Políticas de recuperación de información

9.1 Objetivos de recuperación

Escenario	Pérdida máxima de información	Tiempo estimado de recuperación
Borrado o edición equivocada de un registro	Ninguna	Inmediato: el historial conserva el valor anterior
Documento sobrescrito por error	Ninguna	Minutos: se recupera la versión anterior
Pérdida o corrupción de la base de datos	Segundos	2 a 4 horas
Pérdida del servidor de aplicación	Ninguna	1 a 2 horas desde la imagen diaria
Pérdida total del ambiente	Hasta 24 horas	4 a 8 horas
Compromiso del entorno productivo	Hasta 24 horas	4 a 8 horas desde la copia en región separada

9.2 Procedimiento de recuperación

Ante un incidente que requiera restauración, el procedimiento es:

1. Contener: suspender la operación sobre el componente afectado para evitar que la pérdida se amplíe.
2. Determinar el instante objetivo: identificar el momento anterior al incidente al que debe volverse.
3. Restaurar sobre un ambiente nuevo, nunca sobre el ambiente dañado, de modo que el estado afectado siga disponible para análisis.
4. Verificar la integridad comparando volúmenes de registros contra los valores esperados antes de habilitar el acceso.
5. Redirigir la aplicación al ambiente restaurado.
6. Documentar el incidente, la causa, el alcance de la pérdida y las acciones aplicadas.

9.3 Prueba de restauración ejecutada

El 21 de agosto de 2026 se ejecutó una prueba real de restauración. No se trató de una verificación de que el archivo de respaldo existiera, sino de una restauración completa sobre un motor de base de datos limpio, independiente del ambiente de producción.

Verificación	Esperado	Obtenido	Resultado
Colaboradores restaurados	1.496	1.496	Correcto
Documentos restaurados	1.012	1.012	Correcto
Errores durante la restauración	0	0	Correcto
Integridad del esquema	Completa	Completa	Correcto

La prueba confirma que el respaldo es restaurable de forma autónoma, sin depender del ambiente original. El ambiente de prueba se eliminó al finalizar. Se recomienda repetir el ejercicio de forma semestral y dejar constancia en la sección de Documentación de Auditoría del repositorio.

9.4 Monitoreo del respaldo

El proceso deja registro de cada ejecución y publica su resultado. Además, una verificación diaria consulta el repositorio externo y notifica por correo cuando no ha llegado una copia dentro del plazo tolerado, o cuando la última ejecución falló. La notificación se envía en el momento de la falla y también ante la ausencia silenciosa de respaldos, que es el caso que un aviso de error por sí solo no detecta.

9.5 Responsabilidades

Actividad	Responsable	Periodicidad
Operación de los respaldos automáticos	Proveedor de infraestructura	Continua
Verificación de ejecución de respaldos	Equipo técnico	Mensual
Revisión de la copia en región separada	Equipo técnico	Mensual
Prueba de restauración	Equipo técnico	Semestral
Autorización de una restauración en producción	S&J Salud	Por evento
Revisión de la política	Ambas partes	Anual

10. Conclusión

La Fase 2 se encuentra implementada en siete de sus ocho componentes, verificados sobre el ambiente de producción. Los cuatro entregables contractuales están cubiertos: el repositorio centralizado opera con cifrado y versionado; la estructura documental está cargada con veinte categorías y cincuenta y seis tipos documentales; los permisos están configurados y aplicados en el servidor mediante los siete perfiles definidos, incluida la reserva salarial y la separación entre consultar y descargar; y la estrategia de respaldo cubre base de datos, documentos y servidor, con copia en una región distinta a la de producción y una prueba de restauración ejecutada y documentada.