TRABAJO DE GRADO
Opción Seminario-Diplomado.

Corporación Universitaria Remington

Facultad de Ingeniería

Programa de Ingeniería de Sistemas

Informe Técnico de Ciberseguridad: Filtración de Registros Clínicos

Caso: Clínica Santa Rosa — Amenaza de Origen Interno (Insider Threat)

Sebastián Díaz Castaño

Anderson Ramos Mendieta

Trabajo de Grado — Opción Seminario-Diplomado

Director: Jorge Leonardo Ramírez Restrepo

2026

Tabla de Contenido

Resumen

El presente informe analiza un incidente de seguridad de la información ocurrido en la Clínica Santa Rosa, una institución prestadora de servicios de salud de segundo nivel ubicada en Colombia. A diferencia de las amenazas externas que habitualmente acaparan la atención mediática, este caso tuvo su origen dentro de la propia organización: una colaboradora con acceso legítimo al sistema de información y conocimiento del entorno laboral extrajo y comercializó registros clínicos sensibles durante aproximadamente cuatro meses, sin que ningún mecanismo institucional detectara la actividad.

La situación puso en evidencia ausencias fundamentales en el gobierno de seguridad: falta de segmentación de permisos por rol, inexistencia de registros de auditoría y carencia de herramientas de prevención de pérdida de datos. Esas omisiones convirtieron una vulnerabilidad organizacional en un incidente con consecuencias jurídicas, reputacionales y operativas de considerable magnitud.

El análisis se desarrolla a partir del inventario y valoración de activos críticos, la identificación de amenazas y vulnerabilidades, y la evaluación de riesgos bajo la metodología ISO 27001:2022. Se reconstruye cronológicamente el incidente mediante la técnica de los cinco por qué, y se propone un conjunto de controles preventivos, detectivos y correctivos articulados en un cronograma de implementación por fases. Además, se profundiza en tres dimensiones que el análisis técnico tradicional suele dejar en segundo plano: las políticas de seguridad organizacional, la respuesta estructurada a incidentes y continuidad operacional, y el factor humano como variable determinante en la materialización del riesgo.

Las conclusiones señalan que la causa raíz del incidente no fue de naturaleza técnica sino directiva, y que los controles requeridos para haberlo prevenido eran accesibles y de bajo costo relativo en comparación con el daño ocasionado.

Palabras clave: ciberseguridad, amenaza interna, gestión de riesgos, activos de información, ISO 27001, Ley 1581, datos sensibles de salud.

1. Marco Conceptual y Contextual

Para entender por qué ocurrió este incidente y por qué permaneció sin detectarse durante tanto tiempo, resulta indispensable conocer el entorno en que operaba la Clínica Santa Rosa antes de que saliera a la luz. No se trata únicamente de describir una infraestructura tecnológica, sino de comprender el funcionamiento de una organización que crecía a un ritmo superior al que sus controles de seguridad podían sostener. La brecha entre el avance operativo y la madurez en gestión de la información es, precisamente, el terreno donde los incidentes de origen interno encuentran las condiciones para desarrollarse sin resistencia.

1.1. Características de la Organización

La Clínica Santa Rosa es una institución de mediana complejidad con cerca de 180 colaboradores distribuidos entre áreas médicas, administrativas y de apoyo operativo. En su actividad cotidiana atiende alrededor de 200 pacientes en especialidades como medicina general, ortopedia, cardiología y ginecología.

Al momento del incidente, la clínica se encontraba en plena transición hacia la digitalización de sus historias clínicas. Vista desde el exterior, esa transformación representaba un avance organizacional significativo. Desde adentro, sin embargo, implicaba también un riesgo concreto: trasladar información confidencial desde un archivador físico a un sistema informático sin los controles necesarios equivale a cambiar una cerradura antigua por una puerta sin llave. La digitalización, sin gobernanza, amplía la superficie de ataque.

Desde el punto de vista normativo, los datos clínicos que maneja una institución de este tipo tienen una categoría jurídica especial. La Ley 1581 de 2012 los clasifica como datos sensibles, lo cual exige un nivel de protección reforzado tanto en la dimensión técnica como en la

administrativa (Congreso de Colombia, 2012). Ese estándar legal no era desconocido en abstracto, pero tampoco había sido traducido en políticas, procedimientos o controles concretos al interior de la institución.

1.2. Entorno Tecnológico Previo al Incidente

La infraestructura tecnológica de la clínica correspondía a la de una organización que había incorporado herramientas digitales de forma progresiva, pero sin el respaldo de una arquitectura de seguridad coherente. Sus componentes principales incluían: un Sistema de Historia Clínica Electrónica (HCE) con dos años de funcionamiento y 15.000 registros activos de pacientes; un servidor PACS para almacenamiento y consulta de imágenes diagnósticas (radiografías, ecografías y resonancias magnéticas); un aplicativo de facturación con integración directa a aseguradoras y entidades promotoras de salud (EPS); y una red Wi-Fi con segmentación básica entre zonas médica y administrativa como único mecanismo de control de red. Los puestos de trabajo operaban con Windows 10 integrados al dominio corporativo mediante Active Directory en configuración básica.

Dos aspectos merecen especial atención. En primer lugar, las labores tecnológicas estaban a cargo de un auxiliar administrativo sin formación técnica especializada, lo que significaba que la seguridad de la información dependía de una persona sin los conocimientos ni la autoridad institucional para gestionarla adecuadamente. En segundo lugar, la institución operaba sin una política formal de seguridad de la información aprobada por la dirección. De acuerdo con los principios de la norma ISO/IEC 27001:2022, esa política constituye el fundamento sobre el que se construye cualquier sistema de gestión de seguridad de la información (SGSI); sin ella, los demás

controles carecen de sustento y orientación (International Organization for Standardization [ISO], 2022a).

1.3. Modelo de Control de Accesos Vigente

Uno de los hallazgos más críticos del diagnóstico fue la configuración de permisos del sistema HCE. El sistema únicamente distinguía dos tipos de usuario: Administrador y Usuario estándar. Sin ninguna diferenciación por cargo, función o responsabilidad, todo el personal quedaba asignado automáticamente al rol de usuario estándar, el cual otorgaba permisos de lectura y descarga sobre la totalidad de los 15.000 expedientes.

En la práctica, una recepcionista cuya función real era verificar citas y actualizar datos de contacto tenía exactamente el mismo nivel de acceso a la historia clínica completa de un paciente que el médico especialista que lo atendía. Este escenario contraviene directamente el principio de mínimo privilegio, reconocido en el control A.5.15 de la norma ISO/IEC 27001:2022 y en el Marco de Ciberseguridad del NIST, el cual establece que cada persona debe contar únicamente con el acceso necesario para cumplir su función específica (ISO, 2022a; National Institute of Standards and Technology [NIST], 2018). La consecuencia de ignorar este principio no fue abstracta: fue el incidente objeto de este informe.

2. Inventario y Valoración de Activos de Información

Los activos de información comprenden todos los elementos que tienen valor para la organización y que, por tanto, requieren algún grado de protección. Para su valoración se emplean tres dimensiones: Confidencialidad (C), Integridad (I) y Disponibilidad (D), medidas en una escala de uno a cinco, donde el valor más alto representa mayor criticidad. La combinación de estas dimensiones permite estimar el impacto potencial que tendría la afectación de cada activo sobre la operación de la clínica y sobre sus obligaciones legales. Este análisis responde al numeral 6.1.2 de la norma ISO/IEC 27001:2022 (ISO, 2022a).

Tabla 1

Inventario y valoración de activos críticos — Clínica Santa Rosa

Activo	Descripción	C	I	D	Criticidad
HCE — Historias Clínicas	15.000 registros: diagnósticos, medicamentos, datos personales sensibles.	5	5	4	CRÍTICA
Servidor PACS	Imágenes diagnósticas asociadas a la identidad del paciente.	5	5	3	CRÍTICA
Sistema de facturación	Datos financieros de aseguradoras, coberturas y planes de salud.	4	5	4	ALTA
Estaciones médicas	Equipos en consultorios con acceso directo al HCE y PACS.	3	4	4	ALTA
Red Wi-Fi segmentada	Infraestructura de conectividad; la segmentación era el único control de red.	3	3	5	MEDIA
Credenciales HCE	Usuarios y contraseñas sin política de complejidad ni caducidad establecida.	5	4	2	CRÍTICA

Nota. La escala C/I/D va de 1 (criticidad mínima) a 5 (criticidad máxima). Los activos clasificados como CRÍTICA requieren atención prioritaria e inmediata.

El Sistema de Historia Clínica Electrónica, las credenciales de acceso y el servidor PACS concentran el mayor nivel de riesgo. Son precisamente los activos que estuvieron en el centro del incidente: un sistema con 15.000 expedientes clínicos al que cualquier empleado podía acceder sin

restricciones, protegido por contraseñas que nunca caducaban y que no requerían un mínimo de complejidad. Cuando el activo más valioso carece de la protección más básica, el riesgo no es una posibilidad: es una certeza diferida.

3. Mapa de Amenazas y Debilidades de Seguridad

Identificar las amenazas y vulnerabilidades de una organización no es un ejercicio académico: es el paso que permite comprender qué puede ocurrir, por qué y con qué consecuencias. Una amenaza es cualquier fenómeno capaz de causar daño sobre los activos de información; una vulnerabilidad es la condición que permite que esa amenaza se materialice. En el caso analizado, ninguna de las vulnerabilidades identificadas era de naturaleza sofisticada: todas eran deficiencias básicas acumuladas por omisión a lo largo del tiempo, lo cual hace aún más relevante la reflexión sobre cómo se construyen —o se descuidan— los controles en organizaciones de mediana complejidad.

3.1. Amenazas Reconocidas

Tabla 2

Amenazas identificadas en la Clínica Santa Rosa

#	Amenaza	Categoría	Actor	Activo comprometido
1	Consulta no autorizada de registros clínicos	Insider Threat	Empleado interno	HCE — Historias Clínicas
2	Sustracción y venta de datos a terceros	Fraude / Exfiltración	Empleado interno	HCE — Historias Clínicas
3	Uso indebido de privilegios de acceso excesivos	Amenaza interna	Recepcionista con permisos amplios	Credenciales / HCE
4	Actividad ilícita sin detección por carencia de monitoreo	Fallo detectivo	Organización (omisión)	Registros de auditoría (inexistentes)
5	Incumplimiento de normativa de protección de datos	Riesgo legal	Organización (negligencia)	Totalidad de activos de datos personales

Nota. Las amenazas de categoría Insider Threat son las de mayor dificultad de detección al operar desde dentro del perímetro de confianza organizacional.

3.2. Vulnerabilidades Detectadas

A continuación se describen las condiciones que convirtieron las amenazas anteriores en riesgos reales. Cada una se vincula con los controles del marco ISO/IEC 27002:2022 (ISO, 2022b).

Ausencia de control de acceso diferenciado por función (RBAC)

El control A.5.15 de la norma ISO/IEC 27002:2022 exige que los permisos de acceso se definan según el rol y la responsabilidad de cada usuario (ISO, 2022b). En la clínica, todos los operadores del HCE contaban con el mismo nivel de acceso, sin distinción entre quien necesitaba el expediente clínico completo para ejercer su labor asistencial y quien únicamente requería el número de teléfono del paciente para confirmar una cita. Esta fue la condición estructural que hizo posible el incidente.

Inexistencia de registros de actividad (Audit Logs)

El control A.8.15 establece que las organizaciones deben generar, resguardar y revisar periódicamente registros de eventos de seguridad (ISO, 2022b). El HCE no conservaba ningún historial que indicara qué usuario había consultado qué expediente, en qué momento ni con qué frecuencia. Cuando la situación fue descubierta, no existían registros que permitieran dimensionar con precisión el alcance total de lo ocurrido. La ausencia de trazabilidad impidió tanto la respuesta oportuna como la evaluación forense posterior.

Carencia de alertas ante comportamientos inusuales

No existía ningún mecanismo activo capaz de identificar patrones anómalos en el uso del sistema: descargas masivas de expedientes, consultas repetidas a registros de pacientes de alto perfil o accesos realizados fuera del horario laboral habitual. La actividad irregular operó durante

cuatro meses sin generar ninguna señal de alerta, precisamente porque nadie había definido qué comportamiento debería considerarse anormal.

Inexistencia de herramienta de prevención de pérdida de datos (DLP)

El control A.8.12 de la norma ISO/IEC 27002:2022 contempla medidas para impedir la divulgación no autorizada de información (ISO, 2022b). La institución no contaba con ningún mecanismo que restringiera la copia de registros a dispositivos externos, su envío mediante correo personal o su carga en servicios de almacenamiento en la nube. La extracción se realizó mediante dispositivos USB sin ningún tipo de restricción técnica. Un control de bajo costo habría bloqueado el canal de exfiltración por el que salió la información.

Ausencia de política formal de seguridad de la información

Conforme al control A.5.1 de la norma ISO/IEC 27002:2022, toda organización debe contar con una política de seguridad de la información aprobada por la dirección y comunicada a todo el personal (ISO, 2022b). Los colaboradores de la clínica no habían recibido instrucción sobre el manejo adecuado de datos clínicos ni habían suscrito ningún acuerdo de confidencialidad, no porque no quisieran cumplirlo, sino porque nunca se les informó que existía algo que debían respetar. La ausencia de norma explícita no elimina la responsabilidad, pero sí revela un déficit de liderazgo en la dirección de la institución.

Asignación de accesos sin evaluación de necesidad funcional

Al incorporar un nuevo colaborador, se le otorgaba acceso al sistema sin analizar qué información era estrictamente necesaria para su trabajo. Asignar el perfil estándar era más rápido que diseñar uno diferenciado. Esa comodidad operativa se tradujo en un riesgo estructural que

eventualmente tuvo consecuencias concretas. La eficiencia en el proceso de onboarding no puede ser un argumento para prescindir del principio de mínimo privilegio.

4. Evaluación y Matriz de Riesgos

La evaluación del riesgo combina la probabilidad de que una amenaza se concrete con el nivel de impacto que generaría sobre la organización. El resultado se expresa en una escala de uno a veinticinco, obtenida al multiplicar ambas variables en línea con la metodología cualitativa-cuantitativa aplicada. Este enfoque responde al numeral 6.1.2 de la norma ISO/IEC 27001:2022, que exige establecer criterios de aceptación del riesgo y estimar las consecuencias potenciales sobre la confidencialidad, integridad y disponibilidad de los activos (ISO, 2022a). La coherencia entre el riesgo identificado, la política aplicable y el control propuesto se refleja en cada escenario descrito a continuación.

Tabla 3

Escala de valoración de riesgos aplicada

Puntuación 1–5	Puntuación 6–12	Puntuación 13–18	Puntuación 19–25
Bajo	Medio	Alto	Crítico

Tabla 4

Resultados de la evaluación de riesgos

Escenario de riesgo	Activo expuesto	Probabilidad	Impacto	Nivel	Política aplicable	Control asociado
Exfiltración de HCE por colaborador interno	HCE — 15.000 pacientes	Alta	Muy alto	CRÍTICO (25)	Política de control de accesos y clasificación de datos	A.5.15 RBAC + A.8.15 Audit Log
Comercialización de datos a aseguradoras	HCE / Datos personales	Alta	Muy alto	CRÍTICO (25)	Política de confidencialidad y NDAs	A.8.12 DLP + A.6.6 Acuerdos
Sanción por incumplimiento Ley 1581 ante la SIC	Organización completa	Alta	Alto	CRÍTICO (20)	Política de cumplimiento normativo	A.5.1 Política formal aprobada

Permisos de acceso desproporcionados respecto al rol	HCE / Credenciales	Alta	Alto	ALTO (16)	Política de gestión de identidades	A.5.18 Revisión de derechos
Fuga de imágenes diagnósticas del servidor PACS	Servidor PACS	Media	Alto	ALTO (15)	Política de protección de activos críticos	A.8.12 DLP + segmentación red
Compromiso de credenciales del dominio AD	Active Directory	Media	Medio	MEDIO (9)	Política de contraseñas y autenticación	A.8.5 Autenticación segura
Interrupción del HCE por uso inadecuado	Disponibilidad HCE	Baja	Alto	MEDIO (8)	Política de continuidad operacional	A.5.29 Continuidad de SI

Nota. Los riesgos CRÍTICOS requieren intervención inmediata. Los ALTOS deben atenderse entre los primeros 30 y 90 días. Los MEDIOS pueden gestionarse a mediano plazo. La columna "Política aplicable" refleja el instrumento organizacional que regula cada escenario; la columna "Control asociado" señala el mecanismo técnico o administrativo derivado de dicha política conforme a la norma ISO/IEC 27001:2022.

Los dos escenarios con puntuación máxima de 25 —la exfiltración interna del HCE y la comercialización de datos— no son hipotéticos: el incidente ya se materializó dentro de la organización. Eso los convierte en los de mayor urgencia a la hora de definir acciones de mejora. Lo más relevante de la matriz no es la puntuación en sí, sino la coherencia que debe existir entre el riesgo identificado, la política que lo regula y el control que lo mitiga. Esa cadena lógica es la que da sentido operativo al análisis.

5. Estudio del Incidente y Plan de Controles

5.1. Reconstrucción Cronológica del Incidente

La siguiente línea de tiempo permite reconstruir el desarrollo del incidente y precisar durante cuánto tiempo la actividad ilícita se mantuvo activa sin ser identificada por ningún mecanismo de control institucional. La secuencia no solo documenta lo ocurrido, sino que pone de manifiesto en qué puntos específicos un control adecuado habría interrumpido el proceso.

Tabla 5

Línea de tiempo del incidente — Clínica Santa Rosa

Período	Descripción del evento	Control que habría intervenido
Mes 1	La colaboradora de recepción (denominada Empleada X) descubre que su perfil en el HCE le permite acceder a la totalidad de los expedientes clínicos, incluidos los de pacientes de alto perfil. Inicia consultas no autorizadas de manera esporádica.	RBAC: acceso limitado por función habría impedido la consulta desde el primer momento.
Meses 1–2	Establece contacto con un representante de una aseguradora privada interesado en adquirir información clínica. Se acuerda un esquema de pago proporcional al volumen de registros entregados.	Acuerdo de confidencialidad (NDA): habría establecido marco legal disuasorio.
Meses 2–3	La Empleada X extrae expedientes clínicos de forma sistemática mediante una memoria USB personal, habitualmente al concluir la jornada laboral. El sistema no genera alertas ni registra las operaciones.	Restricción de puertos USB (GPO) y DLP: habrían bloqueado el canal de exfiltración.
Mes 4	Un familiar de uno de los pacientes afectados recibe propuestas comerciales de seguros que contienen información médica confidencial. El paciente presenta queja formal ante la SIC.	Monitoreo UEBA: debería haber detectado el patrón anómalo semanas antes.
Semana de la denuncia	La SIC notifica a la clínica. Una revisión interna revela la conducta de la Empleada X. Se termina el contrato laboral y se activa el proceso penal conforme a la Ley 1273 de 2009.	Plan de respuesta a incidentes: habría acelerado la contención y notificación formal.
Etapa post-incidente	La SIC abre proceso de investigación formal. La clínica contrata consultoría especializada en ciberseguridad para un diagnóstico integral y la elaboración del presente plan de remediación.	Protocolo de comunicación de crisis: habría ordenado la respuesta institucional pública.

Nota. La columna "Control que habría intervenido" ilustra la articulación entre el evento ocurrido y el mecanismo específico que, de haber estado vigente, habría reducido o eliminado el daño.

5.2. Análisis Causal Mediante el Método de los Cinco por Qué

Para identificar la causa raíz del incidente más allá de sus manifestaciones inmediatas, se aplicó la técnica de los cinco por qué, herramienta ampliamente utilizada en el análisis de eventos de seguridad y en los procesos de mejora continua. El razonamiento se desarrolló de la siguiente manera.

El primer interrogante —por qué se produjo la filtración de datos— revela que una colaboradora con acceso habilitado los extrajo y transfirió a un tercero a cambio de una compensación económica. El segundo interrogante cuestiona por qué contaba con acceso a esa información: porque el HCE le otorgaba permisos sobre la totalidad de los registros, sin segmentación por función ni por responsabilidad. El tercer nivel indaga por qué existía ese nivel de acceso irrestricto: porque durante la configuración del sistema no se estableció un esquema de control de acceso diferenciado por roles. El cuarto interrogante pregunta por qué no se estableció ese esquema: porque la organización carecía de una política de seguridad de la información que lo exigiera y de un responsable designado para velar por su cumplimiento. El quinto nivel cuestiona por qué no existía esa política: porque la dirección de la institución nunca incorporó la gestión de la seguridad de la información como un elemento estratégico prioritario.

La causa raíz del incidente puede describirse, en consecuencia, como un déficit de gobierno de seguridad de la información en el nivel directivo, que se tradujo técnicamente en la ausencia de controles de acceso diferenciado, mecanismos de monitoreo y herramientas de prevención de

pérdida de datos. Esta conclusión es coherente con los hallazgos del informe de Ponemon Institute (2023), que identifica la falta de políticas formales y la ausencia de controles técnicos básicos como los factores más frecuentes en incidentes de origen interno.

5.3. Alcance del Impacto Jurídico y Normativo

El ordenamiento jurídico colombiano establece un marco de protección especialmente exigente para los datos de salud. El incidente analizado genera responsabilidad legal simultánea en varios frentes normativos.

En materia de protección de datos personales, la Ley 1581 de 2012 clasifica los registros médicos como datos sensibles y obliga a quienes los tratan a implementar medidas técnicas y administrativas para preservar su confidencialidad e integridad (Congreso de Colombia, 2012). El incumplimiento de esta obligación puede derivar en sanciones económicas de hasta 2.000 salarios mínimos mensuales legales vigentes por parte de la Superintendencia de Industria y Comercio. El Decreto 1377 de 2013, por su parte, obliga a los responsables del tratamiento a contar con políticas internas documentadas, actualizadas y efectivamente divulgadas al personal (Gobierno de Colombia, 2013).

En el ámbito penal, la Ley 1273 de 2009 tipifica como delitos la consulta abusiva de sistemas de información y la violación de datos personales, con penas privativas de la libertad de entre cuatro y ocho años, según la gravedad de los hechos demostrados (Congreso de Colombia, 2009). Adicionalmente, los pacientes cuyos datos fueron comprometidos tienen derecho a ejercer acciones de responsabilidad civil extracontractual contra la institución por los daños patrimoniales y morales ocasionados, lo que convierte a cada paciente afectado en un demandante potencial.

5.4. Consecuencias Reputacionales y Operativas

Más allá del plano jurídico, existe un tipo de daño que no se mide en multas ni en sentencias, pero que puede ser igualmente devastador para una institución de salud: la erosión de la confianza. Cuando un paciente descubre que su información médica fue vendida, no solo pierde la confianza en la institución específica; también comienza a cuestionar si la digitalización de su historial clínico es segura en cualquier parte.

El incidente generó deterioro en la relación con los pacientes, en especial del segmento que constituyó el objetivo directo de la filtración. Produjo también exposición mediática negativa con potencial incidencia sobre el volumen de consultas y la continuidad de contratos con aseguradoras y entidades promotoras de salud. A esto se sumó una sobrecarga de gestión sobre la dirección durante el manejo de la crisis, los procesos de investigación interna y los trámites legales correspondientes, así como costos adicionales por consultoría externa especializada, honorarios jurídicos y posibles indemnizaciones a los pacientes afectados.

5.5. Políticas de Seguridad Organizacional

Una política de seguridad de la información no es un documento que se redacta para cumplir un requisito y se archiva en una carpeta. Es el instrumento mediante el cual la dirección expresa su compromiso con la protección de los activos críticos, define el marco de responsabilidades y establece las consecuencias del incumplimiento. Sin ese instrumento, cualquier control técnico queda suspendido en el aire: no tiene autoridad formal, no tiene alcance definido y no puede exigirse con fundamento.

La Clínica Santa Rosa debe desarrollar y formalizar un conjunto articulado de políticas, organizadas en tres niveles jerárquicos. El primer nivel corresponde a la Política General de

Seguridad de la Información, documento maestro que debe ser aprobado y firmado por la dirección general, publicado en todos los canales internos de comunicación y revisado al menos una vez al año. Este documento debe definir el alcance del sistema de gestión de seguridad, los principios que lo rigen y la estructura de responsabilidades. De acuerdo con el control A.5.1 de la norma ISO/IEC 27002:2022, esa política es el punto de partida obligatorio de cualquier SGSI (ISO, 2022b).

El segundo nivel comprende políticas específicas por dominio, cada una derivada de la política general y referenciada a los controles aplicables. En el contexto de la clínica, las prioritarias son: la Política de Control de Accesos (que establece los criterios de asignación de permisos por rol, los procesos de solicitud, aprobación y revocación de accesos, y los plazos de revisión periódica); la Política de Clasificación y Manejo de la Información (que diferencia los niveles de sensibilidad de los datos —pública, interna, confidencial y restringida— y asocia a cada nivel los controles aplicables); la Política de Uso Aceptable de Tecnología (que regula el uso de dispositivos corporativos, conexiones externas, correo electrónico y almacenamiento en la nube); y la Política de Confidencialidad (que formaliza la obligación de reserva sobre la información de los pacientes y establece el marco para la suscripción de acuerdos de no divulgación).

El tercer nivel corresponde a los procedimientos operativos que traducen cada política en pasos concretos y verificables: el proceso de alta y baja de usuarios, el procedimiento de gestión de incidentes, el protocolo de clasificación documental y el proceso de revisión periódica de permisos. La coherencia entre estos tres niveles —política, norma y procedimiento— es lo que convierte la intención declarada en una práctica sostenible.

Para que las políticas sean eficaces, su implementación debe complementarse con tres condiciones organizacionales: un responsable designado con autoridad real para velar por su cumplimiento (idealmente un Oficial de Seguridad de la Información o equivalente), un canal accesible para reportar dudas o incidentes sin temor a represalias, y un mecanismo de seguimiento que permita verificar su adopción efectiva en las prácticas cotidianas del personal.

Tabla 6

Controles preventivos propuestos

Control	Descripción	Referencia ISO 27001	Política vinculada	Prioridad
Control de acceso RBAC	Redefinir perfiles en el HCE según función: Recepción (datos de contacto y citas), Enfermería (signos vitales), Médico (expediente propio), Administración (facturación sin datos clínicos).	A.5.15 — Gestión de accesos	Política de Control de Accesos	INMEDIATA
Política formal de seguridad	Elaborar, aprobar y comunicar una política institucional suscrita por la dirección que incluya clasificación de datos, uso aceptable y consecuencias del incumplimiento. Revisión anual obligatoria.	A.5.1 — Políticas	Política General de Seguridad	INMEDIATA
Acuerdos de confidencialidad (NDA)	Todo el personal con acceso a datos de salud suscribe un acuerdo con cláusulas explícitas sobre el tratamiento de información sensible y las consecuencias legales de su divulgación.	A.6.6 — Confidencialidad	Política de Confidencialidad	INMEDIATA
Restricción de puertos USB (GPO)	Deshabilitar mediante GPO en Active Directory el uso de medios extraíbles en puestos del área clínica. Solo se admiten dispositivos previamente autorizados por TI.	A.8.12 — DLP	Política de Uso Aceptable de Tecnología	CORTO PLAZO
Revisión trimestral de permisos	Cada trimestre, TI y los jefes de área revisan y validan los permisos del HCE. Los accesos sin justificación funcional se	A.5.18 — Derechos de acceso	Política de Control de Accesos	CORTO PLAZO

	revocan de inmediato y se documentan.			

Nota. Cada control preventivo está vinculado a la política organizacional que le da sustento formal. La columna "Política vinculada" refleja el instrumento que debe aprobarse antes o simultáneamente con la implementación del control técnico.

Tabla 7

Controles detectivos propuestos

Control	Descripción	Referencia ISO 27001	Política vinculada	Prioridad
Registros de auditoría (Audit Log)	Habilitar logging en el HCE: usuario, fecha, hora, expediente consultado y acción ejecutada. Almacenamiento en servidor independiente con acceso restringido. Retención mínima de 12 meses.	A.8.15 — Registros de actividad	Política de Monitoreo y Auditoría	INMEDIATA
Alertas por comportamiento inusual (UEBA)	Generar alerta automática cuando un usuario duplique su promedio histórico de consultas o descargue más de 10 expedientes en una misma sesión.	A.8.16 — Monitoreo	Política de Monitoreo y Auditoría	CORTO PLAZO
Solución DLP para endpoints	Implantar herramienta que supervise y bloquee transferencias de datos clínicos a dispositivos externos, correo personal o servicios de almacenamiento no autorizados.	A.8.12 — DLP	Política de Uso Aceptable de Tecnología	MEDIANO PLAZO
Revisión periódica de logs	El responsable de TI analiza mensualmente los registros del HCE, identificando accesos fuera del horario laboral, IPs no reconocidas o volúmenes de actividad inusuales.	A.8.15 — Registros	Política de Monitoreo y Auditoría	CORTO PLAZO

Nota. Los controles detectivos son tan importantes como los preventivos. Detectar una anomalía en los primeros días puede limitar el alcance de un incidente que, de otro modo, podría escalar durante meses.

5.6. Respuesta a Incidentes y Continuidad Operacional

La respuesta a incidentes de seguridad no puede improvisarse en el momento en que ocurren. Una organización que no tiene definido qué hacer cuando algo falla tarda más en actuar, comunica de forma desorganizada y, en consecuencia, amplifica el daño. El caso de la Clínica Santa Rosa ilustra esta situación con claridad: al momento de la notificación de la SIC, la institución no contaba con ningún protocolo documentado para gestionar la crisis.

El plan de respuesta a incidentes de seguridad es el instrumento que organiza la actuación institucional desde el momento en que se detecta una posible brecha hasta el cierre formal del caso. Su estructura debe contemplar, como mínimo, las siguientes fases metodológicas: preparación, detección y análisis, contención, erradicación, recuperación y lecciones aprendidas. Cada fase debe tener responsables definidos, plazos orientativos y criterios de decisión claros.

La fase de preparación incluye la designación del equipo de respuesta, la definición de roles y canales de comunicación, la disponibilidad de herramientas forenses básicas y la capacitación periódica del equipo mediante ejercicios de simulación. La fase de detección y análisis depende directamente de la existencia de los controles detectivos ya descritos: sin registros de auditoría ni alertas automáticas, la detección quedará siempre sujeta a la casualidad. La contención debe ejecutarse en las primeras horas tras la confirmación del incidente: aislamiento de sistemas comprometidos, revocación de credenciales afectadas y bloqueo de canales de exfiltración activos.

Respecto a las obligaciones de notificación, la Ley 1581 de 2012 y las directrices de la Superintendencia de Industria y Comercio (2023) establecen que las organizaciones deben reportar las brechas que afecten datos personales en plazos que no deben exceder los quince días hábiles

desde el conocimiento del incidente. La demora en la notificación agrava las sanciones y deteriora adicionalmente la confianza institucional. El plan de respuesta debe incluir plantillas prediseñadas para la comunicación a la SIC, a los titulares de datos afectados y a los medios de comunicación, de modo que la presión del momento no conduzca a mensajes descoordinados o contradictorios.

La continuidad operacional, por su parte, se refiere a la capacidad de la organización para mantener sus funciones esenciales durante y después de un incidente de seguridad. Para la Clínica Santa Rosa, la disponibilidad del HCE es crítica: su interrupción impacta directamente la atención a los pacientes. El plan de continuidad debe contemplar procedimientos de respaldo y restauración del sistema, definir el tiempo máximo aceptable de interrupción (RTO) y el punto máximo de pérdida de datos tolerable (RPO), e incluir un esquema de operación manual de emergencia para las funciones asistenciales más críticas mientras el sistema se recupera. El control A.5.29 de la norma ISO/IEC 27001:2022 establece específicamente la obligación de planificar la seguridad de la información durante las interrupciones del negocio (ISO, 2022a).

5.7. Factor Humano y Cultura de Seguridad Organizacional

Los datos técnicos de este informe podrían conducir a una conclusión simple: si se hubieran instalado los controles adecuados, el incidente no habría ocurrido. Esa lectura es correcta, pero incompleta. Detrás de cada vulnerabilidad técnica hay una decisión humana: la de quien configuró el sistema sin diferenciar permisos, la de quien asignó el presupuesto sin incluir ciberseguridad, la de quien nunca informó a los empleados qué podían o no podían hacer con los datos que manejaban cada día. Comprender el factor humano no es relativizar la responsabilidad: es identificar con precisión dónde se originó el fallo.

La investigación en psicología organizacional y gestión de la seguridad distingue entre dos tipos de amenaza interna. El primero es el empleado malicioso, que actúa con intención deliberada de causar daño o de obtener un beneficio ilícito, como ocurrió en este caso. El segundo es el empleado negligente, que expone información sin intención de hacerlo, simplemente porque nadie le explicó los riesgos o porque los procedimientos vigentes hacen más difícil actuar bien que mal. Ambos tipos de amenaza requieren respuestas distintas, y la organización debe tener capacidad para gestionar los dos.

La cultura de seguridad de una organización se construye a través de experiencias acumuladas, no de documentos publicados. Una política de confidencialidad que nadie leyó, una capacitación que se realizó una sola vez hace tres años o un sistema de permisos que nadie explicó al incorporarse a la organización son señales de que la seguridad está presente en los papeles, pero ausente en la práctica cotidiana. Según el informe de Verizon (2024), el factor humano está presente en la mayoría de los incidentes de seguridad documentados, ya sea como actor principal o como elemento facilitador.

La Clínica Santa Rosa debe trabajar en tres dimensiones del factor humano de manera simultánea y sostenida. La primera es la sensibilización y formación: todo el personal debe recibir formación básica en protección de datos y seguridad de la información al incorporarse a la organización, y al menos una actualización anual durante su permanencia. La formación debe ser concreta, basada en ejemplos del propio entorno sanitario, y debe comunicar de forma clara las consecuencias legales y laborales del manejo indebido de información. La segunda dimensión es la comunicación y el reporte: los empleados deben saber a quién dirigirse si detectan una anomalía, y deben sentir que pueden hacerlo sin temor a consecuencias negativas. Los canales de reporte

confidencial son un mecanismo preventivo de primer orden. La tercera dimensión es la supervisión y el reconocimiento: las prácticas de seguridad deben estar integradas en las evaluaciones de desempeño, y el cumplimiento debe ser reconocido de forma positiva, no solo sancionado cuando se incumple.

El análisis de la conducta de la Empleada X revela también que las señales de comportamiento atípico —consultas fuera del horario habitual, acceso sistemático a expedientes de pacientes de alto perfil sin relación con su función— eran observables en el sistema, aunque nadie las observaba. La implementación de herramientas de análisis de comportamiento de usuarios (UEBA) no sustituye al juicio humano, pero sí permite estructurar la supervisión de manera sistemática y proporcional al riesgo, sin depender de la suerte o de la denuncia de terceros.

5.8. Controles de Recuperación

Los controles correctivos tienen como propósito reducir el impacto una vez que el incidente ya se ha materializado y facilitar la recuperación de las condiciones normales de operación y seguridad. Su diseño debe ser coherente con el plan de respuesta a incidentes descrito en la sección anterior.

El plan de respuesta a incidentes de seguridad formaliza el procedimiento para actuar frente a una brecha de datos de salud, incluyendo plazos definidos de notificación a la SIC conforme a la Ley 1581 de 2012. Actuar con rapidez y criterio en las primeras horas puede ser determinante para contener el daño antes de que se amplíe.

El protocolo de atención a titulares de datos afectados establece un proceso formal para contactar, informar y acompañar a los pacientes cuyos datos hayan sido comprometidos. Su

propósito trasciende el cumplimiento legal: es una expresión de responsabilidad ética con personas reales que han sufrido una vulneración de su privacidad.

El plan de comunicación de crisis proporciona una guía para gestionar la comunicación interna, con medios de comunicación y ante organismos reguladores frente a un incidente de alto impacto reputacional. Comunicar bien en una situación de crisis no es improvisación: es el resultado de una preparación previa que define quién habla, qué se dice y en qué momento.

La sesión de lecciones aprendidas es una reunión post-incidente de carácter obligatorio, prevista dentro de los quince días siguientes a cualquier brecha confirmada, orientada a actualizar el análisis de riesgos y fortalecer los controles existentes. Todo incidente, bien gestionado, debe dejar un aprendizaje documentado que mejore la capacidad de respuesta futura y retroalimente la cultura de seguridad de la organización.

5.9. Cronograma de Implementación

Las acciones propuestas se distribuyen en tres fases de ejecución progresiva. Los controles más urgentes son de bajo costo relativo y pueden activarse en las primeras semanas tras la aprobación del plan. Ninguna de las acciones de la fase inicial implica inversiones extraordinarias en infraestructura; en cambio, sí requieren voluntad institucional, coordinación entre áreas y el respaldo activo de la dirección.

Tabla 8

Cronograma de implementación de controles

Fase	Acción	Responsable	Plazo	Costo estimado	Política habilitante
FASE 1	Implantar RBAC en el HCE y revocar accesos no justificados.	TI + Jefes de área	Semana 1	Bajo	Política de Control de Accesos

FASE 1	Activar registros de auditoría y redirigir a servidor independiente.	TI	Semanas 1–2	Bajo	Política de Monitoreo y Auditoría
FASE 1	Bloquear puertos USB en puestos del área clínica vía GPO.	TI	Semana 2	Bajo	Política de Uso Aceptable de Tecnología
FASE 1	Redactar y aprobar la Política General de Seguridad de la Información.	Dirección + TI	Semanas 3–4	Bajo	Compromiso directivo
FASE 1	Firma de acuerdos de confidencialidad (NDA) con todo el personal.	RRHH + Legal	Semana 4	Bajo	Política de Confidencialidad
FASE 2	Configurar alertas de comportamiento anómalo (UEBA) en el HCE.	TI	Mes 2	Medio	Política de Monitoreo y Auditoría
FASE 2	Capacitar al 100 % del personal en protección de datos, Ley 1581 y cultura de seguridad.	RRHH + TI	Mes 2	Bajo	Política General de Seguridad
FASE 2	Elaborar plan de respuesta a incidentes y protocolo de comunicación de crisis.	Dirección + Legal	Mes 3	Bajo	Política de Gestión de Incidentes
FASE 2	Diseñar protocolo de atención a titulares de datos afectados.	Legal + Dirección	Mes 3	Bajo	Política de Gestión de Incidentes
FASE 3	Implementar solución DLP para endpoints y correo electrónico.	TI + Proveedor	Meses 4–5	Alto	Política de Uso Aceptable de Tecnología
FASE 3	Designar un Oficial de Seguridad de la Información (CISO o equivalente).	Dirección	Mes 5	Medio	Política General de Seguridad
FASE 3	Realizar auditoría interna de seguridad y actualizar el análisis de riesgos.	TI + Consultoría	Mes 6	Medio	Política General de Seguridad

Nota. La columna "Política habilitante" señala el instrumento organizacional que debe estar vigente para que el control técnico o administrativo correspondiente tenga respaldo formal. La implementación de controles sin política aprobada es técnicamente posible pero institucionalmente frágil.

6. Conclusiones

El análisis del caso de la Clínica Santa Rosa deja lecciones que van mucho más allá de un incidente puntual. Son lecciones aplicables a cualquier organización que maneje datos de salud, porque el escenario descrito no es excepcional: es el resultado previsible de operar sin controles básicos en un entorno donde la información tiene valor real y sus consecuencias se extienden a personas concretas.

6.1. El Mayor Riesgo Puede Estar Dentro de la Organización

La mayoría de los equipos de seguridad concentra sus esfuerzos en el perímetro externo: cortafuegos, antivirus, protección contra intrusos. Es una orientación comprensible, pero insuficiente. Este caso demuestra que un colaborador con acceso habilitado puede ocasionar un daño equivalente o superior al de cualquier atacante externo, y hacerlo de forma completamente invisible cuando no existen controles internos. Según el informe de Ponemon Institute (2023), el costo promedio de un incidente de amenaza interna supera en múltiples métricas al de los ataques externos convencionales, precisamente por la dificultad de detección. La norma ISO/IEC 27001:2022 contempla controles específicos para reducir los riesgos asociados a este tipo de amenazas (ISO, 2022a).

6.2. La Seguridad de la Información es Responsabilidad de Toda la Organización

La causa raíz identificada no fue técnica: fue una omisión de carácter directivo. Ningún control tecnológico puede ser completamente eficaz sin el respaldo activo de la alta dirección, la implicación del área de recursos humanos y el área jurídica, y el compromiso de los jefes de cada unidad funcional. Cuando la responsabilidad por la seguridad queda delegada en un auxiliar sin autoridad formal ni formación especializada, la organización asume un riesgo institucional de

primer orden sin ser consciente de ello. El Informe de Investigaciones sobre Brechas de Datos de Verizon (2024) señala consistentemente que los incidentes más costosos se originan en fallos de gobierno, no en vulnerabilidades técnicas.

6.3. El Principio de Mínimo Privilegio es Simple, Económico y Efectivo

Si la recepcionista hubiera tenido acceso únicamente a los datos necesarios para su función —agenda de citas e información de contacto— este incidente no habría ocurrido. El principio de mínimo privilegio, contemplado en el control A.5.15 de la norma ISO/IEC 27001:2022, es uno de los controles más accesibles y eficaces en términos de relación costo-beneficio (ISO, 2022a). No requiere adquirir software ni contratar consultores externos: requiere tomarse el tiempo de analizar qué acceso necesita realmente cada persona para desempeñar su función.

6.4. Lo que No se Observa No Puede Detenerse

Durante cuatro meses, la Empleada X realizó cientos de consultas y extracciones sin que ningún sistema emitiera una señal de alerta. No porque su conducta fuera especialmente elaborada —utilizó una memoria USB y su propio acceso habilitado— sino porque no había nada que la observara. Los registros de auditoría y las alertas ante comportamientos inusuales, exigidos por los controles A.8.15 y A.8.16 de la norma ISO/IEC 27002:2022, no son elementos sofisticados: son los mecanismos básicos que permiten detectar irregularidades antes de que sus consecuencias sean irreversibles (ISO, 2022b).

6.5. El Factor Humano Requiere una Estrategia Propia

Los controles técnicos son necesarios, pero ninguno por sí solo puede reemplazar a una cultura organizacional en la que cada colaborador entienda su papel en la protección de la información. La formación continua, los canales de reporte, el reconocimiento de las buenas

prácticas y la supervisión del comportamiento son componentes de esa cultura que deben construirse de manera deliberada y sostenida. Una organización que invierte solo en herramientas, pero no en las personas que las usan, seguirá siendo vulnerable.

6.6. El Cumplimiento Normativo es el Punto de Partida, no la Meta

Cumplir la Ley 1581 de 2012 es el mínimo exigible por ley, no un indicador de madurez en gestión de seguridad (Congreso de Colombia, 2012). Las organizaciones que administran información de salud de manera responsable no se limitan a evitar sanciones: adoptan marcos integrales como la norma ISO/IEC 27001:2022, que articula un sistema de gestión continua y adaptable. La implementación de los controles propuestos en este informe reduciría el nivel de riesgo de CRÍTICO a BAJO en los escenarios más graves, y posicionaría a la Clínica Santa Rosa en un nivel de madurez coherente con los estándares del sector salud en Colombia. El costo de los controles propuestos representa una fracción mínima frente a las consecuencias económicas, jurídicas y reputacionales de un incidente de esta naturaleza. La inversión en ciberseguridad no es un gasto operativo: es una decisión estratégica que define el tipo de institución que se quiere ser.

Referencias

Congreso de Colombia. (2009). Ley 1273 de 2009 — Por medio de la cual se modifica el Código Penal, creando un nuevo bien jurídico tutelado denominado la protección de la información y de los datos. Diario Oficial No. 47223.

Congreso de Colombia. (2012). Ley 1581 de 2012 — Por la cual se dictan disposiciones generales para la protección de datos personales. Diario Oficial No. 48587.

Gobierno de Colombia. (2013). Decreto 1377 de 2013 — Por el cual se reglamenta parcialmente la Ley 1581 de 2012. Presidencia de la República de Colombia.

International Organization for Standardization. (2022a). ISO/IEC 27001:2022 — Information security, cybersecurity and privacy protection — Information security management systems — Requirements. ISO.

International Organization for Standardization. (2022b). ISO/IEC 27002:2022 — Information security, cybersecurity and privacy protection — Information security controls. ISO.

National Institute of Standards and Technology. (2018). Framework for improving critical infrastructure cybersecurity (NIST Cybersecurity Framework v1.1). U.S. Department of Commerce. https://www.nist.gov/cyberframework

Ponemon Institute. (2023). 2023 cost of insider threats global report. Proofpoint & Ponemon Institute.

Superintendencia de Industria y Comercio. (2023). Guía para la implementación del principio de responsabilidad demostrada (Accountability). SIC Colombia.

Verizon. (2024). Data breach investigations report (DBIR) 2024. Verizon Business. https://www.verizon.com/business/resources/reports/dbir/