TRABAJO DE GRADO
Opción Seminario-Diplomado.

Informe Técnico - Análisis De Ciberseguridad En IPS Salud Abierta

Corporación Universitaria Remington.

Ingeniería De Sistemas - Tecnología en desarrollo de software.

Seminario de Ciberseguridad

Jasseph Antonio Sánchez Granados

Juan Ángel Rodríguez García

Yonny Murcia Pineda

Docente Ing. Jorge Leonardo Ramírez Restrepo

2026

Tabla de Contenido

1 Resumen

El presente informe se centra en el análisis de ciberseguridad de una Institución Prestadora de Salud (IPS) llamada Salud Abierta, una empresa de pequeña escala, la cual cuenta con una nómina de 20 trabajadores y opera como una infraestructura crítica debido al manejo de datos sensibles.

El propósito de este trabajo es diagnosticar el estado actual de la organización, la cual presenta un bajo nivel de madurez digital, evidenciado en la ausencia de controles básicos como la autenticación de usuarios, la protección de puntos finales (antivirus rigurosos) y el uso de canales de comunicación corporativos.

El enfoque aplicado se basa en la ciberseguridad organizacional, priorizando la tríada de la información la cual nos habla de la confidencialidad, integridad y disponibilidad. En este contexto, se desarrollaron actividades clave, iniciando con la identificación de activos, donde se determinó que las historias clínicas y los datos de afiliación son los activos de mayor valor.

Posteriormente, se realizó un análisis de amenazas y vulnerabilidades, identificando que el uso de cuentas genéricas, la navegación sin restricciones y el uso de correos personales incrementan la superficie de ataque, facilitando incidentes como la fuga de datos no autorizada, en incumplimiento de la Ley 1581 de 2012.

Asimismo, se plantea un proceso de análisis y gestión de riesgos, con el fin de identificar posibles escenarios adversos, evaluar su probabilidad de ocurrencia y establecer medidas preventivas que reduzcan la exposición a ciberataques.

Finalmente, se aborda la cultura organizacional como el pilar preventivo más relevante, promoviendo buenas prácticas en el manejo de contraseñas, la higiene digital y el uso adecuado de canales de comunicación corporativos. De esta manera, la IPS no solo cumple con la

normativa legal vigente, sino que también fortalece la seguridad del paciente mediante la protección de su información personal.

2 Palabras claves

Ciberseguridad: Conjunto de prácticas y medidas utilizadas para proteger sistemas, redes y datos frente a ataques o accesos no autorizados.

Seguridad de la Información: Es la práctica de proteger los datos y sistemas de información de amenazas como el acceso no autorizado o la fuga de datos que provocan la divulgación, alteración o destrucción de información sensible.

Vulnerabilidad: Debilidades o fallos en sistemas, procesos o personas que pueden ser aprovechados por una amenaza.

Gestión de Riesgos: Es el proceso de identificar, evaluar y abordar cualquier riesgo financiero, legal, estratégico y de seguridad para una organización.

Protección de Datos: Se refiere a estrategias y procesos de seguridad que ayudan a proteger o salvaguardar la información digital frente a accesos no autorizados, robo, corrupción o pérdida.

3 Marco Conceptual.

La ciberseguridad de una organización comprende un conjunto de prácticas, políticas y tecnologías diseñadas para proteger los activos de información frente a amenazas internas y externas. En el entorno sanitario, su importancia es crítica debido al procesamiento de datos sensibles, como registros médicos e historias clínicas, los cuales requieren niveles superiores de protección para salvaguardar la intimidad de los pacientes (ISO/IEC 27001, 2022). Además, la transformación digital en el sector salud ha incrementado la dependencia de plataformas tecnológicas y sistemas de información, lo que hace indispensable implementar controles de seguridad que permitan prevenir incidentes cibernéticos y garantizar la continuidad operativa de los servicios médicos (ENISA, 2023). De igual manera, los ataques dirigidos a hospitales y clínicas han aumentado considerablemente en los últimos años, afectando la disponibilidad de los servicios médicos y comprometiendo información confidencial de miles de pacientes, lo que demuestra la necesidad de fortalecer los mecanismos de protección en las instituciones de salud (OMS, 2023).

La seguridad de la información se fundamenta en la tríada de confidencialidad, integridad y disponibilidad (ISO/IEC 27002, 2022). La confidencialidad asegura que la información no sea accesible para personas no autorizadas; la integridad garantiza que los datos permanezcan inalterados; y la disponibilidad asegura el acceso oportuno a la información cuando esta se requiere. En la IPS Salud Abierta, esta tríada se encuentra actualmente comprometida debido al caos identitario, ya que la falta de cuentas individuales impide garantizar que únicamente el personal autorizado acceda a la información. Además, esta situación facilita que los datos puedan ser modificados por terceros sin dejar rastro (NIST, 2020). A esto se suma el riesgo derivado del uso inadecuado de credenciales compartidas, ya que dificulta la trazabilidad de las acciones

realizadas dentro de los sistemas institucionales y aumenta la probabilidad de accesos indebidos o fugas de información sensible (Cisco, 2022). En el sector salud, estas fallas pueden generar consecuencias graves, como retrasos en la atención médica, pérdida de información clínica y afectaciones directas en la seguridad del paciente, especialmente cuando los sistemas hospitalarios dependen completamente de herramientas digitales para operar (Health Sector Cybersecurity Coordination Center, 2022).

Un elemento clave en este proceso es la identificación de los activos de información, definidos como los recursos con valor para la organización, tales como sistemas, datos y personal (ISO/IEC 27001, 2022). Asimismo, la correcta clasificación de estos activos permite a la IPS priorizar la protección de las historias clínicas sobre otros recursos menos críticos. Posteriormente, el análisis de amenazas —entendidas como eventos con potencial de causar daño, como ataques informáticos— y de vulnerabilidades —fallas explotables en los sistemas— permite determinar el nivel de riesgo al que está expuesta la organización (NIST, 2020). Del mismo modo, la gestión de riesgos permite establecer estrategias preventivas y correctivas orientadas a minimizar el impacto de posibles incidentes de seguridad y fortalecer la resiliencia institucional frente a ataques cibernéticos (ISO 31000, 2018). En las organizaciones de salud, esta gestión resulta fundamental debido a que la interrupción de los servicios tecnológicos puede afectar directamente la prestación de servicios médicos esenciales y comprometer la continuidad asistencial de los pacientes (HHS, 2023).

En cuanto a la Ley 1581 de 2012, esta establece el marco legal para la protección de datos personales en Colombia (Congreso de la República de Colombia, 2012). Para la IPS, su

cumplimiento no representa únicamente una recomendación técnica, sino también una obligación legal, ya que el uso de correos personales y cuentas genéricas para gestionar datos de salud vulnera los principios de seguridad y privacidad exigidos por esta normativa, exponiendo a la organización a posibles sanciones administrativas. Igualmente, la normativa colombiana exige que las entidades implementen medidas de seguridad adecuadas para proteger la información personal de accesos no autorizados, pérdida o alteración indebida (Superintendencia de Industria y Comercio, 2021). En el caso específico del sector salud, el tratamiento de datos clínicos exige mayores niveles de protección debido a que son considerados datos sensibles, cuya divulgación indebida puede afectar la intimidad y los derechos fundamentales de los pacientes.

Para concluir, la cultura organizacional es un factor crítico en la ciberseguridad porque el comportamiento humano afecta directamente la seguridad del sistema. Sensibilizar a los empleados y capacitarlos sobre buenas prácticas, como el uso de contraseñas seguras y la identificación de correos electrónicos fraudulentos, reduce significativamente el riesgo (ISO/IEC 27002, 2022). Asimismo, fomentar una cultura de seguridad basada en la concientización y el cumplimiento de políticas internas fortalece la capacidad de la organización para prevenir incidentes y responder adecuadamente ante posibles amenazas digitales (Kaspersky, 2023). En las instituciones de salud, la capacitación constante del personal administrativo y asistencial resulta indispensable, debido a que gran parte de los incidentes de seguridad se originan por errores humanos, malas prácticas en el manejo de la información o desconocimiento de los protocolos de seguridad informática.

4 Marco Contextual.

La organización investigada es la Institución Prestadora de Salud (IPS) “Salud Abierta”, una microempresa del sector salud con aproximadamente 20 empleados. Su actividad económica se centra en la prestación de servicios sanitarios, que incluye el tratamiento continuo de información sensible, como historias clínicas y datos personales de los pacientes. Este tipo de información, por su propia naturaleza, requiere de un alto nivel de protección, tanto técnica como jurídica, bajo normas como la Ley 1581 de 2012.

La IPS opera bajo un modelo de trabajo "nómada", donde los asociados no cuentan con estaciones de trabajo fijas, sino que utilizan diferentes equipos según la disponibilidad. Si bien este modelo puede ofrecer flexibilidad operativa, también plantea desafíos importantes para la seguridad de la información, particularmente en torno a la gestión de identidades y el control de acceso.

En este contexto, se identifica como principal problema el llamado “caos identitario” caracterizado por la falta de mecanismos de autenticación y trazabilidad en el uso de los sistemas. La falta de cuentas de usuario individuales hace imposible determinar quién en la organización accede, cambia o elimina información que representa un riesgo crítico en caso de un incidente de seguridad, como registros alterados o violaciones de datos.

Además, IPS tiene varias vulnerabilidades que aumentan considerablemente su exposición a riesgos cibernéticos. Primero, la falta de control de acceso permite que cualquier persona, incluidos visitantes o terceros no autorizados, acceda a las computadoras y a la red interna sin restricciones. En segundo lugar, el uso de cuentas generales y correos electrónicos personales para gestionar información institucional conduce a una pérdida de control sobre los

datos, ya que pueden almacenarse fuera del entorno organizacional y seguir siendo propiedad de los empleados incluso después de su separación. También, la navegación por Internet sin restricciones es otro inconveniente importante, ya que facilita el acceso a sitios web potencialmente maliciosos que pueden comprometer la seguridad del sistema al descargar malware. Esta situación se ve exacerbada por la falta de soluciones de protección un antivirus actualizado, lo que deja a la organización vulnerable a amenazas como el ransomware. Este tipo de incidentes puede comprometer la disponibilidad de la información, el cifrado de los registros médicos y afectar gravemente la continuidad del servicio.

La cultura de ciberseguridad de la organización presenta una baja madurez, lo que se manifiesta en una falta de políticas, controles y capacitación del personal sobre buenas prácticas de seguridad. Esta situación aumenta el riesgo, considerando que el factor humano es uno de los principales vectores de ataque en las organizaciones.

Es importante desarrollar un análisis de ciberseguridad que permita identificar y gestionar los riesgos existentes, establecer controles adecuados y fortalecer la protección de los activos de información. Esto no lo promoverá el cumplimiento de la normativa vigente, sino que también garantizará la seguridad del paciente y la continuidad de los servicios prestados por IPS “Salud Abierta”.

5 Desarrollo e Implementación del Aprendizaje

Durante el proceso de investigación y diagnóstico realizado en la IPS ***Salud Abierta***, observamos una brecha significativa entre la importancia de la información manejada y los controles de seguridad aplicados a esta; si bien es cierto la entidad opera con datos de alta sensibilidad, la infraestructura que emplea carece de una división clara de funciones.

Para abordar estos hallazgos, comenzamos con una fase de identificación técnica, en la que clasificamos los recursos que soportan las operaciones de IPS, permitiéndonos priorizar aquellos activos cuya pérdida representaría un riesgo crítico para los pacientes y la estabilidad jurídica de la organización, teniendo en cuenta la responsabilidad de la organización con información según la ley 1581 de 2012.

5.1 Identificación de Activos

Con base en el análisis realizado, se trazó una hoja de ruta orientada a identificar los principales activos de información de la IPS. Para ello, dichos activos fueron clasificados en tres grupos relevantes: activos físicos, activos de procesos e información, y activos humanos o de personas. Esta clasificación permite comprender de manera más clara los recursos críticos de la organización y establecer medidas de protección acordes con su nivel de importancia dentro de la operación médica y administrativa (ISO/IEC 27001, 2022).

5.1.1 Activos Físicos - Hardware e Infraestructura

Los activos físicos corresponden a los elementos tangibles que soportan la operación tecnológica y el almacenamiento de la información dentro de la organización. Debido a que la IPS se encuentra en una etapa de crecimiento y posee un bajo nivel de madurez digital, se identificaron los siguientes activos físicos:

Tabla 1

Activos Físico

Activo	*Descripción*	*Dueño del Activo*	*Ubicación*
Servidores Locales	*Equipos que guardan bases de datos, historias clínicas y facturación.*	*Soporte Técnico (TI)*	*Oficina TI*
Estaciones de Trabajo	*PCs, laptops y equipos biomédicos conectados digitalmente.*	*Cada usuario asignado*	*Consultorios y Recepción*
Dispositivos de Red	*Routers, switches y puntos de acceso (AP).*	*Soporte Técnico (TI)*	*Infraestructura de la IPS*
Almacenamiento Externo	*USBs o discos duros para copias de seguridad manuales.*	*Soporte Técnico (TI)*	*Archivo del personal TI*

Dentro de los activos físicos; los servidores locales son considerados los activos críticos porque almacenan las historias clínicas y las bases de datos institucionales. Ya que una falla o acceso no autorizado a estos podrían generar pérdida de información médica, interrupción en la atención de pacientes y afectaciones legales relacionadas con la protección de datos personales.

5.1.2 Activos de Procesos - Información y Software

corresponden a recursos intangibles esenciales para el funcionamiento institucional. Aunque no son elementos físicos, representan uno de los activos más importantes de la organización, ya que permiten la operación diaria, el almacenamiento de información sensible y la continuidad de los servicios médicos y administrativos. Dentro de este grupo se identificaron los siguientes activos:

Tabla 2

Activo Procesos

Activo	*Descripción*	*Dueño del Activo*	*Ubicación*
Historias Clínicas Digitales	*Activo de mayor valor con intervenciones y atenciones médicas.*	*Dirección Médica*	*Servidor de Base de Datos*
Datos de Afiliación	*Información personal sujeta a la Ley 1581 de 2012.*	*Coordinación Administrativa*	*Servidor de Base de Datos*
Datos de Empleados	*Información sensible del personal médico y administrativo.*	*Talento Humano*	*Servidor de Base de Datos*

Bases de Datos (SQL/PHP)	*Sistemas de gestión de resultados y almacenamiento masivo.*	*Soporte Técnico (TI)*	*Servidor Local*
Canales de Comunicación	*Flujos de información técnica (actualmente en correos personales).*	*Soporte Técnico (TI)*	*Equipos Personales y de la organización.*
Software de Aplicación	*Herramientas médicas y administrativas para la operación diaria.*	*Gerencia*	*Estaciones de Trabajo*

En este grupo contiene los activos más valiosos y críticos de toda la IPS dentro de los cuales destacan las historias clínicas digitales, bases de datos de pacientes, debido a que contienen información confidencial sobre diagnósticos, tratamientos e intervenciones médicas. La pérdida, alteración o divulgación de estos datos podría comprometer la salud de los pacientes, afectar la calidad del servicio médico y generar sanciones legales por incumplimiento de las normas de protección de datos

5.1.3 Activos Personas

El activo humano está conformado por todas las personas que interactúan con los sistemas, equipos y procesos de la IPS, el personal médico, administrativo y técnico desempeña un papel fundamental en la protección de la información. Lo anterior, teniendo en cuenta que son

quienes lo operan, además mediante su buen o mal uso podemos hacer que herramientas o sistemas pueden convertirse en un factor de vulnerabilidad o de protección para la organización.

Tabla 3

Activo Persona

Activo	*Descripción*	*Dueño del Activo*	*Ubicación*
Personal Asistencial	*Encargados del ciclo de vida de la historia clínica (médicos y enfermeros).*	*Dirección Médica*	*Consultorios - Áreas asistenciales*
Personal Administrativo	*Gestión de afiliaciones, trámites de ley e ingreso al sistema.*	*Coordinación Administrativa*	*Oficina Administrativa - Recepción*
Pacientes	*Titulares de la información; su privacidad depende de la integridad de los datos.*	*Gerencia*	*Entorno externo - Base de datos*

Por último, el activo humano representa uno de los elementos más importantes dentro de la organización, debido a que tiene acceso directo a las historias clínicas y participa activamente en el registro y consulta de información médica.

6 Amenazas y Vulnerabilidades

6.1 La amenaza

Es un evento interno o externo que tiene el potencial de causar daño a la organización.

6.2 La vulnerabilidad

Es una debilidad o un fallo en nuestros controles que permite que la amenaza tenga éxito.

Una vez identificados los activos con los que cuenta la organización, se realizó un análisis de posibles amenazas y vulnerabilidades a las que pueden estar expuestos, con el fin de garantizar la funcionalidad de la IPS, aspecto fundamental para el adecuado desarrollo y continuidad del negocio.

Tabla 4

Amenazas y Vulnerabilidades

Activo	*Amenaza*	*Vulnerabilidad*
Personal Asistencial y Administrativo	*Phishing: mediante correos personalizados roban credenciales para acceder a sistemas de la organización.*	*Falta de concienciación: Si el personal no tiene la capacitación para detectar*

		comunicaciones fraudulentas puede ser víctima.
Historias Clínicas y Datos de Afiliación	*Fuga de datos: extracción no autorizada de información de los pacientes o usuarios.*	*Uso de cuentas genéricas: si varios empleados comparten credenciales impide el control individual de datos.*
Estaciones de Trabajo y Equipos Biomédicos	*Malware - Ransomware: Este programa malicioso infecta a los equipos de cómputo, secuestrando la información.*	*Antivirus deficiente: Ausencia de protecciones técnicas rigurosas y parches de seguridad desactualizados.*
Bases de Datos y Software Médico	*Intrusión externa: Acceso de personas ajenas a los sistemas centrales de la IPS.*	*Navegación libre: falta de restricciones en el uso de internet, esto expone los equipos a sitios inseguros.*
Canales de Comunicación	*Interceptación de información: Robo de datos mientras se envían por medios digitales.*	*Uso de correos personales: Al enviar datos sensibles a través de plataformas externas que la IPS no controla.*

Servidores y Sistemas de Almacenamiento	*Pérdida de disponibilidad: Daño o borrado de la información por fallos técnicos o físicos "humanos".*	*Copias de seguridad informales: Uso de discos manuales en lugar de un sistema de respaldo profesional.*

7 Evaluación de Riesgos

Es el proceso para identificar, evaluar y priorizar posibles amenazas y vulnerabilidades dentro del entorno de una organización.

7.1 Identificación de Riesgos

La valoración de los riesgos de la IPS "Salud Abierta" se realizó tomando como referencia la metodología de gestión y evaluación de riesgos ISO 27005. Esta establece que el nivel de riesgo se determina a partir de dos factores principales: la probabilidad de ocurrencia y el impacto que tendría el incidente sobre la organización.

En la matriz se utilizaron niveles de impacto como "Alto" y "Muy Alto", y niveles de riesgo como "Importante", "Alto" y "Crítico", con el fin de representar el grado de afectación que podría sufrir la IPS frente a cada escenario identificado.

Tabla 5

Evaluación de Riesgos

Activo	*Escenario de Riesgo*	*Probabilidad*	*Impacto*	*Nivel de Riesgo*
Historias Clínicas	*Fuga de información sensible debido al uso de cuentas genéricas sin trazabilidad.*	*Alta*	*Muy Alto*	*Crítico*
Estaciones de Trabajo	*Infección por ransomware ocasionada por protección antivirus insuficiente.*	*Alta*	*Muy Alto*	*Crítico*
Bases de Datos	*Acceso no autorizado por navegación insegura y ausencia de restricciones web.*	*Alta*	*Muy Alto*	*Crítico*
Personal Médico y Administrativo	*Robo de credenciales mediante ataques de phishing por falta de capacitación en ciberseguridad.*	*Alta*	*Alto*	*Importante*
Canales de Comunicación	*Filtración de información institucional por uso de correos personales no corporativos.*	*Media*	*Alto*	*Importante*

Servidores	*Pérdida de disponibilidad de información por ausencia de políticas formales de respaldo.*	*Media*	*Muy Alto*	*Alto*

7.2 Análisis y Evaluación de Riesgos

7.2.1 Riesgos Críticos:

Estos escenarios presentan una Probabilidad Alta debido a las vulnerabilidades actuales de la IPS (como la falta de antivirus robustos y el uso de cuentas compartidas). El impacto se califica como Muy Alto porque afectaría directamente la seguridad del paciente y la continuidad del servicio médico. Si las historias clínicas son cifradas por un ransomware, la IPS se enfrenta a una parálisis operativa total y a riesgos legales severos bajo la Ley 1581 de 2012.

7.2.2 Riesgos Importantes:

Escenarios como el phishing se consideran de alta probabilidad dado el bajo nivel de madurez digital del personal. El impacto es Alto porque compromete la identidad institucional; sin embargo, se diferencia del nivel "Crítico" en que inicialmente afecta a cuentas individuales antes de comprometer la infraestructura central de la IPS.

7.2.3 Riesgo Alto:

La pérdida de disponibilidad en servidores por falta de respaldos formales tiene una probabilidad Media, ya que los fallos de hardware no son diarios. No obstante, su impacto es Muy Alto debido a que, de ocurrir un fallo físico sin un sistema de respaldo profesional, la pérdida de información histórica de los pacientes sería irreversible.

8 Políticas y Controles de Ciberseguridad – IPS Salud Abierta

Con base en el diagnóstico de activos, amenazas y vulnerabilidades realizado previamente, se establecen las siguientes directrices institucionales. Estas políticas tienen como propósito garantizar la tríada de la seguridad de la información “confidencialidad, integridad y disponibilidad”, garantizar la continuidad de los servicios médicos y reducir la exposición frente a incidentes de ciberseguridad.

8.1 Política Gestión de cuentas y control de accesos.

El acceso a los sistemas de información de la IPS es nominal, personal e intransferible. Se prohíbe estrictamente el uso compartido de credenciales y el acceso a módulos que no correspondan a las funciones asignadas al cargo.

8.1.1 Control Practico

Se implementará un directorio activo con perfiles basados en roles (RBAC), las cuales se inhabilitarán automáticamente luego de 5 días de inactividad.

El departamento de TI será quien ejecute esta política y la asignación de las cuentas estará a cargo del área de talento humano.

Adicionalmente, se realizará una revisión trimestral de privilegios de usuario y auditoría mensual de intentos de acceso

8.2 Política de Protección de Equipos y Estaciones de Trabajo

Todo dispositivo conectado a la red institucional debe cumplir con el estándar de configuración segura definido por la organización, prohibiendo la alteración de parámetros de seguridad por parte del usuario final.

8.2.1 Control Practico

El equipo de soporte técnico será el responsable de blindar y mantener protegidos los equipos de la organización, mediante la utilización de antivirus corporativos, protección de endpoints (EDP/Antivirus) con administración centralizada y bloqueo de puertos USB físicos y las restricciones de instalación de software no autorizado.

De lo anterior se realizarán revisiones mensuales de seguridad en las estaciones de trabajo para validar el estado de actualización y funcionamiento de las herramientas de protección implementadas.

8.3 Política de Comunicaciones Internas Corporativas

El correo electrónico institucional es el único medio autorizado para el intercambio de información corporativa y datos sensibles de pacientes (Historias Clínicas). Queda prohibido el envío de información institucional a través de servicios de mensajería personal o correos externos.

8.3.1 Control Practico

El área de TI supervisará el uso adecuado de los canales corporativos y bloqueará el envío o recepción de información sensible a través de correos personales o plataformas no autorizadas

Además, serán los responsables del Monitoreo semanal de alertas de fuga de información y revisión semestral de logs de comunicación.

8.4 Política de Capacitación y Conciencia en Ciberseguridad

La IPS fomentará una cultura de seguridad mediante la capacitación obligatoria de todo su personal, orientada a la identificación de riesgos latentes como la ingeniería social.

8.4.1 Control Practico

La ejecución de esta política recae sobre el área TI y la coordinación administrativa quienes será los responsables de programar jornadas de capacitación trimestrales sobre:

Phishing, manejo seguro de contraseñas, protección de datos, uso adecuado de sistemas, y reporte de actividades sospechosas.

Asimismo, serán obligatorias para nuevos ingresos a la organización antes de iniciar su periodo laboral.

8.5 Política de Navegación Segura en Internet

El acceso a internet dentro de la IPS deberá utilizarse únicamente para actividades relacionadas con las funciones institucionales y la prestación de servicios de salud.

8.5.1 Control Practico

El profesional en redes del área TI, será el responsable de implementar filtros de navegación y restricciones sobre páginas web potencialmente peligrosas o no relacionadas con las actividades laborales.

Semanalmente se supervisará los accesos realizados desde la red institucional para identificar comportamientos inseguros o descargas sospechosas.

8.6 Política de Copias de Seguridad y Recuperación de Información

La organización garantiza la disponibilidad de la información mediante un sistema de copias de seguridad automatizado, cifrado y bajo el esquema 3-2-1 (tres copias, dos medios distintos, uno fuera de sitio).

8.6.1 Control Practico

Migración de backups manuales a un sistema de almacenamiento en nube cifrado con versionamiento, eliminando la dependencia de medios extraíbles.

El responsable de ejecutar el control será el área TI, quienes llevarán a cabo backups incrementales diarios y completos semanales. Además, Se realizará una prueba de restauración de datos cada 90 días para validar la integridad.

9 Incidentes y Respuesta

Después de identificar los activos, analizar las amenazas, evaluar los riesgos y establecer políticas de seguridad, es importante definir un procedimiento organizado para responder ante posibles incidentes de ciberseguridad dentro de la IPS.

Por esta razón, contar con un plan de respuestas a posibles incidentes permitirá de manera rápida y controlada actuar frente a eventos que comprometan la tríada de la información, reduciendo así el impacto sobre la operación y continuidad del servicio médico.

Para ello se tuvieron en cuenta 5 elementos fundamentales que ayudan a evaluar y neutralizar la amenaza. Así: Identificación, Contención, Erradicación, Recuperación y Lecciones Aprendidas

9.1 Incidente N.º 1 Ataque de Ransomware (Cifrado de Datos)

Al inicio de la jornada laboral, el personal administrativo de la IPS intenta ingresar al sistema de citas e historias clínicas; sin embargo, observa que no es posible acceder a la información. En pantalla aparece un mensaje indicando que las bases de datos fueron cifradas y que, para recuperar el acceso, la organización debe realizar un pago económico.

9.1.1 Respuesta a incidente:

Identificación: El equipo de TI confirma la imposibilidad de acceder a las historias clínicas y bases de datos del servidor principal. Posteriormente, se evidencia un ataque de ransomware debido al mensaje que muestran los equipos afectados.

Contención: se desconectan los equipos afectados para evitar que el malware se siga propagando a otros equipos.

Como segunda medida, se realiza el aislamiento temporal del servidor afectado.

Erradicación: Ejecución de un escaneo profundo con herramientas EDR (Endpoint Detection and Response) para eliminar los binarios del ransomware y cierre de las vulnerabilidades.

Restauración: La IPS restablece la operación de los servicios mediante la recuperación de la información desde las copias de seguridad automáticas más recientes implementadas en la nueva política de backups.

Seguidamente se valida el correcto funcionamiento de los datos y sistemas médicos antes de habilitar el acceso al personal.

Lecciones Aprendidas: Este incidente nos deja en evidencia, la necesidad de fortalecer los controles de protección en estaciones de trabajo, mantener actualizados los sistemas y siendo prioritario fortalecer los procesos de concientización del personal sobre la navegación segura y prevención de malware.

9.2 Incidente N.º 2 Fuga de Información Por Uso de Cuentas Genéricas.

Durante una revisión interna, la IPS identifica una modificación no autorizada en la historia clínica de una paciente. Sin embargo, debido al uso compartido de cuentas y credenciales genéricas, no es posible determinar con exactitud qué usuario realizó el acceso y modificación de la información.

9.2.1 Respuesta Incidente:

Identificación: El área administrativa detecta inconsistencias en la información registrada dentro de la historia clínica y notifica el incidente al personal de TI para iniciar el proceso de revisión del caso, logrando identificar que la modificación se hizo de una cuenta compartida utilizada por varias personas.

Contención: Bloqueo inmediato de la cuenta genérica comprometida para detener nuevas modificaciones

Erradicación: se inicia el proceso de eliminación gradual de cuentas compartidas y la asignación de credenciales individuales al personal según el rol dentro de la organización.

Recuperación: La IPS procede a restaurar la información clínica afectada utilizando los registros y respaldos disponibles, garantizando la integridad de los datos médicos de la paciente.

Lecciones aprendidas: El incidente demuestra la importancia de implementar mecanismos de trazabilidad y autenticación individual dentro de la organización, ya que el uso de cuentas genéricas impide identificar responsables y aumenta el riesgo de fuga o alteración de información sensible.

10 Cultura Organizacional El Factor Humano en la Seguridad

Durante el análisis realizado en la IPS “Salud Abierta”, se logró identificar que uno de los principales factores de riesgo no se encuentra únicamente en los procesos tecnológicos que se emplean, sino también en el comportamiento humano.

Aspectos como el uso de contraseñas compartidas, el manejo de correos personales y la falta de conocimiento sobre amenazas digitales evidencian el poco conocimiento de los empleados en cuanto a la seguridad informática, lo que conlleva a un enorme riesgo de incidentes en los cuales se vea comprometido el funcionamiento de la organización como los datos que en ella se manipulan.

En este contexto, fortalecer la cultura organizacional se convierte en un elemento fundamental para reducir riesgos y prevenir incidentes de ciberseguridad. Cuando el personal comprende la importancia de proteger la información y aplica buenas prácticas en sus actividades diarias, disminuye considerablemente la posibilidad de ataques relacionados con errores humanos.

Por esta razón, la IPS debe promover estrategias de concientización y capacitación orientadas al personal médico, administrativo y técnico, donde se aborden temas como:

- Uso seguro de contraseñas.
- Identificación de correos fraudulentos (phishing).
- Manejo adecuado de información sensible.
- Uso responsable de equipos y sistemas institucionales.
- Importancia de los canales corporativos de comunicación.

De esta manera, se logra crear una cultura organizacional sólida del personal de la IPS, lo que permitirá fortalecer la confidencialidad, integridad y disponibilidad de la información, mitigando así cualquier incidente y garantizando la continuidad de los servicios prestados por la IPS.

11 Conclusiones

El análisis realizado en la IPS Salud Abierta nos permitió comprender que la ciberseguridad no depende únicamente de contar con herramientas tecnológicas avanzadas, sino también de la manera en que las personas manejan la información dentro de la organización. Durante el diagnóstico se evidenció que existen múltiples riesgos relacionados con la falta de controles básicos, como el uso de cuentas compartidas, correos personales y la ausencia de políticas claras de seguridad, situaciones que pueden comprometer seriamente la información sensible de los pacientes.

Uno de los hallazgos más importantes fue identificar que las historias clínicas y los datos personales de los pacientes representan los activos más críticos de la IPS, ya que cualquier pérdida, modificación o filtración de esta información puede generar consecuencias legales, operativas y reputacionales para la organización. Esto demuestra la necesidad de fortalecer los mecanismos de protección y garantizar el cumplimiento de la Ley 1581 de 2012 sobre protección de datos personales.

Además, se pudo concluir que el factor humano sigue siendo una de las principales vulnerabilidades en materia de ciberseguridad. La falta de capacitación y de cultura organizacional facilita que amenazas como el phishing, el malware o la fuga de información tengan un mayor impacto dentro de la empresa. Por esta razón, la concientización del personal debe convertirse en una prioridad constante y no únicamente en una medida temporal.

También se evidenció que, aunque la IPS presenta un bajo nivel de madurez digital, existen oportunidades claras de mejora mediante la implementación de políticas de acceso, controles de navegación, respaldos automáticos y el uso de herramientas de protección adecuadas. Estas acciones no solo ayudarían a reducir los riesgos actuales, sino que también permitirían garantizar la continuidad de los servicios médicos y aumentar la confianza de los pacientes en la organización.

Finalmente, este trabajo permitió entender que la ciberseguridad en el sector salud debe ser vista como una responsabilidad integral que involucra tecnología, procesos y personas. Proteger la información no solo significa evitar ataques informáticos, sino también preservar la privacidad, la integridad y la seguridad de los pacientes, quienes son el eje principal de la organización.

12 Bibliografía

Babilonia Presentacion, G. S. (2023). BENEFICIOS DE LAS NORMAS ISO 27000. HIGH TECH-ENGINEERING JOURNAL, 3(2), 86–88. https://doi.org/10.46363/high-tech.v3i2.4

Marco, M. (2024, agosto 16). ¿Qué es el Nist y para qué sirve? Seifti. https://seifti.io/es/que-es-el-nist-y-para-que-sirve/

Orrego, V. M. (2013). La gestión en la seguridad de la información según Cobit, Itil e Iso 27000. 4. https://www.academia.edu/27191007/La_gesti%C3%B3n_en_la_seguridad_de_la_informaci%C3%B3n_seg%C3%BAn_Cobit_Itil_e_Iso_27000

Quirumbay Yagual, D. I., Castillo Yagual, C., & Coronel Suárez, I. (2022). Una revisión del Aprendizaje profundo aplicado a la ciberseguridad. Revista Científica y Tecnológica UPSE, 9(1), 57–65. https://doi.org/10.26423/rctu.v9i1.671

Universidad San Sebastián. (s/f). USS. Recuperado el 12 de mayo de 2026, de https://repositorio.uss.cl/items/8a046340-37ec-4456-a2f3-e61765b94b0e

Auquilla, C., & Raul, S. (2025). Modelo Integral de Gestión de Riesgos Cibernéticos para PYMEs, utilizando el Marco de Ciberseguridad NIST CSF 2.0. Quito, Ecuador: UISRAEL

Bot detection. (s/f). Edu.Co. Recuperado el 12 de mayo de 2026, de https://repositorio.itc.edu.co/handle/20.500.14329/1590

Cascón-Katchadourian, J., Ruiz-Rodríguez, A. Á., & Alberich-Pascual, J. (2018). Revisión, análisis y evaluación de sistemas para la gestión de activos multimedia en organizaciones. Revista espanola la de documentacion cientifica, 41(1), 196. https://doi.org/10.3989/redc.2018.1.1481

Robles, T., & Alberto, C. (2016). La importancia de realizar un análisis de riesgo en las empresas. Universidad Piloto de Colombia http://repository.unipiloto.edu.co:8080/handle/20.500.12277/2728

(S/f). Unav.edu. Recuperado el 12 de mayo de 2026, de https://dadun.unav.edu/server/api/core/bitstreams/8fee7751-cdb2-450e-9bd3-a1412b96b8df/content

Grande, L., & Edgardo, C. (2015, diciembre). Ingeniería social : el ataque silencioso. ITCA, Editores. http://www.redicces.org.sv/jspui/handle/10972/2910

Guaña-Moya, J., Sánchez-Zumba, A., Chérrez-Vintimilla, P., Chulde-Obando, L., Jaramillo-Flores, P., & Pillajo-Rea, C. (s/f). Ataques informáticos más comunes en el mundo digitalizado. Proquest.com. Recuperado el 12 de mayo de 2026, de https://www.proquest.com/openview/02492b51bc001f7bf3254a198698d1d7/1?pq-origsite=gscholar&cbl=1006393

(S/f). Com.co. Recuperado el 12 de mayo de 2026, de https://books.google.com.co/books?hl=es&lr=&id=xrm9DwAAQBAJ&oi=fnd&pg=PA57&dq=MATRIZ+DE+RIESGOS&ots=XqlYt-01_f&sig=nX80XKBZWotTmYkQSl08KrSU8OE&redir_esc=y#v=onepage&q&f=false

World health organization (WHO). (s/f). Who.int. Recuperado el 16 de mayo de 2026, de https://www.who.int/