

TRABAJO DE GRADO
Opción Seminario-Diplomado.

**ANÁLISIS DE VULNERABILIDADES EN CIBERSEGURIDAD DE SEIS EMPRESAS
ASESORADAS POR PROF&TECH MEDIANTE UN DIAGNÓSTICO TÉCNICO**

Corporación Universitaria Remington.
facultad: Ingenierías
programa académico: Ingeniería de Sistemas

Estudiante:
Maikol Serrano Oviedo

Tutor:
Ing. Esp. ALFONSO VALENCIA MSc.
Seminario de ciberseguridad y ciberdefensas
2026

Dedicatoria

Dedico este trabajo a mi familia, por ser mi apoyo durante todo este camino y por acompañarme en cada etapa de mi formación profesional.

De manera especial, a mi esposa, por su paciencia, comprensión y apoyo incondicional, especialmente en los momentos en los que continuar no fue fácil.

A mi hijo, por ser una de mis principales motivaciones para seguir adelante y alcanzar esta meta. Cada esfuerzo realizado durante este proceso también representa el deseo de construir un mejor futuro para nuestra familia.

De manera muy especial, dedico también este trabajo a la memoria del ingeniero Luis Alberto Morales, mi buen amigo, quien, aunque ya no se encuentra en este mundo, fue una persona que me brindó un gran apoyo y dejó una huella importante en mi vida. Su amistad, sus palabras y los momentos compartidos permanecerán siempre en mi memoria. Aunque su ausencia se siente, su recuerdo seguirá presente y siempre será recordado con gratitud y cariño.

Este logro es también para ustedes.

Agradecimientos

Agradezco a Dios por permitirme llegar hasta esta etapa y darme la fortaleza necesaria para culminar este proceso de formación profesional.

A la Corporación Universitaria Remington y a los docentes que hicieron parte de mi formación, por los conocimientos y experiencias que contribuyeron a mi crecimiento profesional y que hoy me permiten desarrollar este trabajo.

A mi familia, por estar presente durante este camino y brindarme su apoyo en los momentos de mayor exigencia. Especialmente a mi esposa, por su comprensión y acompañamiento, y a mi hijo, por ser una motivación constante para seguir adelante.

Finalmente, agradezco a Prof&Tech y a las empresas que hacen parte de este proyecto por permitir el desarrollo del diagnóstico técnico y facilitar el acercamiento a situaciones reales de ciberseguridad, haciendo posible llevar a la práctica los conocimientos adquiridos durante mi formación.

Tabla de Contenidos

Resumen.....	7
Marco conceptual y contextual	8
Ciberseguridad:	8
Activos de información.....	8
Amenazas.....	9
Vulnerabilidades	9
Análisis de vulnerabilidades	10
Riesgo de ciberseguridad	10
Valoración y clasificación del riesgo.....	11
Marco normativo colombiano relacionado con la seguridad de la información.....	12
Normativa aplicable al sector salud	13
Contexto de las empresas objeto del diagnóstico	14
Objetivo General.....	17
Objetivos Específicos.....	17
Metodología del diagnóstico.....	18
Criterios de evaluación	19
Instrumento / matriz de diagnóstico.....	19
Tabla 2. Matriz de Diagnostico	19
Escala de probabilidad e impacto	20
Tabla 3. Probabilidad	20
Tabla 4. Impacto	20
Diagnósticos	21
Diagnóstico de Uronorte S.A.....	21
Resultados del análisis externo	21
Tabla 5. Resultados análisis externo Uronorte	22
Resultados de la evaluación interna.....	22
Tabla 6. Resultados análisis interno Uronorte	23
Usuarios y cuentas	24
Tabla 7. Accesos remotos Uronorte	25
Vulnerabilidades identificadas	25
Tabla 8. Vulnerabilidades Uronorte	25
URO-01 – Configuración criptográfica insegura en HTTPS.....	26
URO-02 – MariaDB fuera de soporte.....	26
URO-03 – Python desactualizado	26
URO-04 – Política CORS permisiva	27
URO-05 – Interfaz administrativa del firewall expuesta a Internet	27
URO-06 – Servicio FTP expuesto a Internet	28
Diagnóstico de Help Trauma IPS SAS	28

	5
Resultados del análisis externo	29
Tabla 9. Resultado de pruebas externas Help Trauma	29
Resultados de la evaluación interna	30
Tabla 10. Revisión interna Help Trauma	30
Usuarios y cuentas	30
Tabla 11. Usuarios servidor Help Trauma	31
Vulnerabilidades identificadas	31
Tabla 12. Vulnerabilidades Identificadas Help Trauma	31
HT-01 – Cuenta Invitado habilitada y con uso reciente	32
HT-02 – Política de contraseñas insuficiente.....	32
HT-03 – Configuración permisiva de acceso en MariaDB.....	33
HT-04 – Ausencia de protección antivirus en equipos de usuario.....	33
HT-05 – Múltiples herramientas de acceso remoto habilitadas.....	34
HT-06 – Cuentas de acceso remoto innecesarias.....	34
Diagnóstico de Sociedad Médica Los Samanes SAS	35
Resultados del análisis externo	36
Tabla 13. Análisis Externo Samanes	36
Resultados de la evaluación interna.....	37
Tabla 14. Sistemas Operativos Samanes	37
Tabla 15. Análisis interno Samanes	38
Usuarios y cuentas	38
Tabla 16. Accesos Samanes.....	39
Vulnerabilidades identificadas.....	39
Tabla 17. Vulnerabilidades Samanes.....	39
SAM-01 – Sistemas operativos fuera de soporte	40
SAM-02 – Ausencia de protección antivirus	40
SAM-03 – Ausencia de mecanismos de respaldo	41
SAM-04 – Obsolescencia de los equipos de cómputo.....	41
SAM-05 – Ausencia de firewall dedicado en la red interna	41
Análisis de las condiciones de ciberseguridad en las IPS evaluadas	42
Tabla 18. Comparación de las condiciones identificadas para empresas del sector salud	43
Reflexión sobre la información clínica y los riesgos identificados	44
Tabla 19. Relación entre los hallazgos y los principios de seguridad de la información en salud.....	44
Diagnóstico de MK Insumos Inc. S.A.S.	45
Resultados del análisis externo	46
Resultados de la evaluación interna.....	46
Vulnerabilidades identificadas.....	47
Tabla 20. Vulnerabilidades Identificadas en MK	47
MK-01. Sistema operativo Windows 10 Pro fuera de soporte general.....	47
MK-02. Firewall local de Windows deshabilitado	48
MK-03. Escritorio remoto habilitado sin necesidad declarada	48
MK-04. Política de contraseñas insuficiente	49
MK-05. Cuentas locales habilitadas sin actividad reciente	49

	6
MK-06. Múltiples herramientas de acceso remoto activas	50
Diagnóstico de Sureca Ltda.	50
Resultados del análisis externo	50
Resultados de la evaluación interna.....	51
Vulnerabilidades identificadas.....	51
Tabla 21. <i>Tabla de Vulnerabilidades encontradas Sureca</i>	52
SUR-01. Servicio de videovigilancia expuesto a Internet	52
SUR-02. Servidor sin actualizaciones recientes	53
SUR-03. Firebird 2.5 de 32 bits utilizado como motor de base de datos	53
SUR-04. Ausencia de antivirus institucional.....	54
SUR-05. Política de contraseñas insuficiente	54
SUR-06. Cuenta Invitado habilitada y con actividad reciente.....	55
SUR-07. Escritorio remoto habilitado	55
Diagnóstico de Indubolsas Contreras S.A.S.	56
Resultados del análisis externo	56
Resultados de la evaluación interna.....	56
Usuarios y cuentas	57
Vulnerabilidades identificadas.....	58
Tabla 22. <i>Vulnerabilidades Identificadas Indubolsas</i>	58
IND-01. Política de contraseñas insuficiente.....	59
IND-02. Cuenta Invitado habilitada y con actividad reciente.....	59
IND-03. Múltiples cuentas habilitadas sin actividad reciente	59
IND-04. Escritorio remoto habilitado	60
IND-05. Servicio MariaDB/MySQL accesible en todas las interfaces.....	61
IND-06. Alta cantidad de accesos remotos reportados	61
Análisis comparativo de las empresas evaluadas.....	62
Tabla 23. <i>Resumen de vulnerabilidades de las 6 empresas evaluadas</i>	62
Análisis comparativo de las empresas evaluadas.....	63
Conclusiones	64
Referencias.....	66
Anexos	68

Resumen

El presente trabajo tiene como propósito analizar las vulnerabilidades de ciberseguridad de seis empresas asesoradas por Prof&Tech: Uronorte S.A., Help Trauma IPS SAS, Sociedad Médica Los Samanes SAS, MK Insumos Inc. SAS, Sureca Ltda. e Indubolsas Contreras SAS. El diagnóstico busca identificar condiciones que puedan representar riesgos para los sistemas, la información y las operaciones de estas organizaciones, teniendo en cuenta sus características y actividades particulares.

Para realizar el análisis se revisaron diferentes aspectos de la infraestructura tecnológica, entre ellos equipos, servidores, redes, aplicaciones, actualizaciones, controles de acceso, usuarios, servicios habilitados, mecanismos de protección, respaldos y accesos remotos. Los hallazgos se sustentan en evidencias obtenidas durante la revisión técnica y se valoran mediante criterios de probabilidad e impacto, con el fin de establecer un nivel de riesgo y facilitar su priorización.

El trabajo también plantea recomendaciones orientadas al tratamiento de las condiciones identificadas, procurando que las acciones propuestas puedan ser verificadas mediante valores iniciales, metas e indicadores. En las empresas del sector salud se consideran además aspectos relacionados con la protección de la información clínica y los datos personales, debido a la naturaleza de la información que manejan.

Palabras clave

Ciberseguridad; Vulnerabilidades; Análisis de riesgos; Diagnóstico técnico; Seguridad de la información.

Marco conceptual y contextual

Ciberseguridad:

La ciberseguridad comprende las prácticas orientadas a prevenir, detectar, responder y recuperarse frente a situaciones que puedan afectar los sistemas, redes, dispositivos y la información de una organización. Su propósito está relacionado con la protección de propiedades como la confidencialidad, integridad y disponibilidad de la información y de los sistemas que la procesan. NIST contempla la ciberseguridad como la protección y restauración de sistemas de información y comunicaciones frente a diferentes tipos de afectaciones y ataques (National Institute of Standards and Technology [NIST], s. f.-a).

En el contexto empresarial, la ciberseguridad adquiere especial importancia debido a que las organizaciones dependen cada vez más de sistemas informáticos, redes, aplicaciones y servicios digitales para desarrollar sus actividades. Una debilidad en alguno de estos componentes puede generar condiciones que faciliten incidentes de seguridad y afectar las operaciones de la organización.

Activos de información

Un activo de información puede entenderse como un recurso que tiene valor para una organización y que requiere protección frente a diferentes amenazas (National Institute of Standards and Technology [NIST], s. f.-b) Dentro de un entorno empresarial pueden encontrarse activos como equipos de cómputo, servidores, dispositivos de red, aplicaciones, bases de datos, sistemas de información y la propia información utilizada para desarrollar las actividades de la organización.

La identificación de los activos es importante dentro de un análisis de vulnerabilidades, debido a que permite establecer qué elementos pueden verse afectados por una vulnerabilidad y cuáles podrían ser las consecuencias para la organización.

En el presente proyecto, los activos que se encuentren dentro del alcance del diagnóstico serán considerados como elementos sobre los cuales se identificarán y analizarán posibles vulnerabilidades.

Amenazas

Una amenaza corresponde a una circunstancia o evento con capacidad de producir un efecto adverso sobre las operaciones, los activos o la información de una organización mediante un sistema de información. Entre sus posibles efectos se encuentran el acceso no autorizado, la destrucción, divulgación o modificación de información y la interrupción de servicios (National Institute of Standards and Technology [NIST], s. f.-d)

Es importante diferenciar una amenaza de una vulnerabilidad. La amenaza representa el evento, circunstancia o actor que puede generar un daño, mientras que la vulnerabilidad corresponde a una debilidad que puede ser explotada o activada por dicha amenaza.

Vulnerabilidades

Una vulnerabilidad es una debilidad presente en un sistema de información, procedimientos de seguridad, controles internos o implementación que puede ser explotada o activada por una fuente de amenaza (National Institute of Standards and Technology [NIST], s. f.-e).

Las vulnerabilidades pueden estar relacionadas con diferentes elementos de una infraestructura tecnológica. Por ejemplo, pueden originarse por configuraciones inseguras, software desactualizado, controles de acceso deficientes, servicios innecesarios, contraseñas débiles o ausencia de determinados controles de seguridad.

Análisis de vulnerabilidades

El análisis de vulnerabilidades comprende un proceso sistemático orientado a examinar un sistema o producto con el propósito de identificar deficiencias de seguridad y obtener información que permita determinar medidas de protección o mitigación. NIST relaciona la evaluación de vulnerabilidades con la identificación y evaluación formal de las debilidades existentes en un sistema de información.

De acuerdo con NIST SP 800-115, las pruebas y evaluaciones técnicas de seguridad pueden utilizarse, entre otros propósitos, para encontrar vulnerabilidades en sistemas o redes, analizar los hallazgos y desarrollar estrategias de mitigación

Riesgo de ciberseguridad

El riesgo de ciberseguridad se relaciona con las posibles consecuencias que pueden producirse cuando una amenaza aprovecha una vulnerabilidad. NIST define el riesgo como una medida que considera tanto el impacto adverso que podría producirse como la probabilidad de ocurrencia del evento.

En el ámbito de la seguridad de la información, estos riesgos pueden estar relacionados con la pérdida de confidencialidad, integridad o disponibilidad de la información y de los sistemas, así como con consecuencias sobre las operaciones y los activos de una organización (National Institute of Standards and Technology [NIST], s. f.-c).

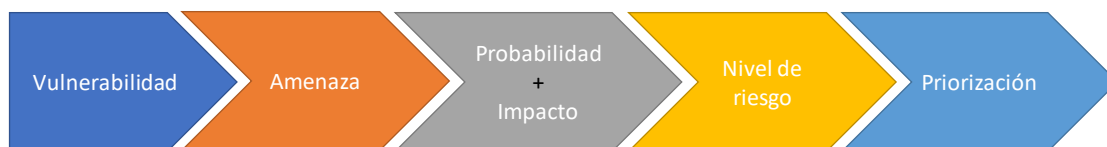
Valoración y clasificación del riesgo

La identificación de una vulnerabilidad permite reconocer una debilidad que puede afectar la seguridad de los sistemas, la información o los procesos de una organización. Sin embargo, la identificación por sí sola no permite establecer cuáles de los hallazgos requieren una atención prioritaria. Por esta razón, el presente trabajo incorpora una etapa de valoración y clasificación del riesgo asociada a las vulnerabilidades identificadas durante el diagnóstico técnico.

El riesgo de ciberseguridad se relaciona con la posibilidad de que una amenaza aproveche una vulnerabilidad y genere consecuencias adversas sobre los activos, la información o las operaciones de una organización. Para su valoración se tendrán en cuenta principalmente dos variables: probabilidad e impacto.

La probabilidad representa la posibilidad de que una vulnerabilidad pueda ser aprovechada o materializada, considerando aspectos como las condiciones existentes, la exposición del activo y las características de la vulnerabilidad identificada. Por otra parte, el impacto corresponde a las posibles consecuencias que tendría la materialización del riesgo sobre la organización (Joint Task Force Transformation Initiative, 2012).

Para efectos del diagnóstico se establecerán criterios cualitativos para ambas variables, permitiendo posteriormente determinar un nivel de riesgo. De manera general, el proceso puede representarse de la siguiente forma:



La clasificación obtenida permitirá organizar los hallazgos de acuerdo con su nivel de importancia y facilitará la formulación de recomendaciones orientadas a reducir la exposición de las organizaciones.

En el caso de las IPS, la valoración deberá considerar adicionalmente las posibles consecuencias que una vulnerabilidad pueda generar sobre la confidencialidad, integridad y disponibilidad de información relacionada con los pacientes, debido a la naturaleza sensible de la información manejada por estas organizaciones.

Marco normativo colombiano relacionado con la seguridad de la información

En Colombia, la seguridad de la información está relacionada con diferentes normas y políticas que buscan proteger los datos, los sistemas informáticos y la información que manejan las organizaciones. Estas disposiciones sirven como referencia para que las empresas adopten medidas que permitan reducir los riesgos relacionados con el uso de las tecnologías de la información. Para este proyecto, conocer este marco normativo permite tener un contexto sobre la importancia de proteger la información y prevenir situaciones que puedan afectar su confidencialidad, integridad y disponibilidad.

Entre las normas más importantes se encuentra la Ley 1581 de 2012, que establece disposiciones generales para la protección de datos personales (Congreso de Colombia, 2012). Esta norma es relevante para las empresas analizadas, ya que dentro de sus actividades pueden manejar información de clientes, empleados, proveedores y otras personas. Por esta razón, es necesario contar con medidas que ayuden a evitar accesos no autorizados, pérdida, modificación o divulgación indebida de estos datos. De igual manera, la Ley 1273 de 2009 incorporó al Código Penal colombiano diferentes conductas relacionadas con delitos informáticos, como el acceso abusivo a sistemas, el daño informático y la violación de datos personales (Congreso de Colombia, 2009).

Como antecedente de la política de ciberseguridad en Colombia se encuentra el CONPES 3701 de 2011, mediante el cual se establecieron lineamientos para fortalecer las capacidades del país frente a las amenazas cibernéticas y la atención de incidentes de seguridad (Departamento Nacional de Planeación, 2011). Posteriormente, el CONPES

3854 de 2016, relacionado con la Política Nacional de Seguridad Digital (Departamento Nacional de Planeación, 2016), y el CONPES 3995 de 2020, sobre confianza y seguridad digital, ampliaron este enfoque hacia la gestión de los riesgos asociados al entorno digital (Departamento Nacional de Planeación, 2020). Estos documentos muestran la evolución que ha tenido en Colombia la necesidad de fortalecer la seguridad de la información y la protección frente a las amenazas cibernéticas.

Dentro del presente proyecto, este marco normativo permite establecer el contexto en el cual se realiza el diagnóstico de las seis empresas seleccionadas. Su aplicación no busca realizar una auditoría jurídica ni determinar el cumplimiento total de cada norma, sino servir como referencia para comprender la importancia de identificar vulnerabilidades y riesgos que puedan afectar la información y los recursos tecnológicos.

Normativa aplicable al sector salud

Las características de la información manejada por las Instituciones Prestadoras de Servicios de Salud (IPS) hacen necesario considerar disposiciones adicionales relacionadas con la protección, manejo, custodia y confidencialidad de la información clínica.

Dentro de las organizaciones objeto del presente diagnóstico se encuentran Uronorte SA, Help Trauma SA y Sociedad Médica Los Samanes, las cuales serán consideradas dentro del análisis con criterios adicionales asociados al sector salud, de acuerdo con las actividades y sistemas de información que efectivamente se encuentren dentro del alcance del diagnóstico.

Uno de los principales referentes corresponde a la Resolución 1995 de 1999, relacionada con el manejo de la historia clínica (Ministerio de Salud, 1999). Esta disposición establece aspectos relacionados con la organización, manejo y conservación de la historia clínica y reconoce su carácter reservado. Por esta razón, los sistemas y

procedimientos utilizados para gestionar este tipo de información deben incorporar mecanismos que permitan preservar su confidencialidad.

Adicionalmente, el desarrollo de la Historia Clínica Electrónica Interoperable en Colombia ha incorporado disposiciones posteriores, entre ellas la Ley 215 de 2020 (Congreso de Colombia, 2020), la Resolución 866 de 2021 (Ministerio de Salud y Protección Social, 2021) y la Resolución 1888 de 2025 (Ministerio de Salud y Protección Social, 2025), relacionadas con el intercambio e interoperabilidad de información clínica.

Para efectos del presente trabajo, la normativa del sector salud será utilizada como referente para establecer criterios adicionales de análisis en las tres IPS, particularmente en aspectos relacionados con:

- confidencialidad de la información clínica;
- control de acceso;
- protección de datos personales;
- integridad de los registros;
- gestión de usuarios y permisos;
- almacenamiento de información;
- mecanismos de respaldo;
- seguridad de los sistemas utilizados para gestionar información clínica.

Contexto de las empresas objeto del diagnóstico

El presente trabajo se desarrolla en seis empresas asesoradas por Prof&Tech, seleccionadas para aplicar los conocimientos adquiridos durante el Seminario de Ciberseguridad. Las organizaciones consideradas son Uronorte S.A., Help Trauma IPS

SAS, Sociedad Médica Los Samanes SAS, MK Insumos Inc. SAS, Sureca Ltda. e Indubolsas Contreras SAS.

Para el diagnóstico se tienen en cuenta las características particulares de cada organización, su infraestructura tecnológica y los antecedentes relacionados con situaciones que hayan podido afectar la seguridad de la información. Este contexto permite interpretar los resultados del diagnóstico de acuerdo con las condiciones reales encontradas en cada empresa.

Uronorte S.A. cuenta con dos sedes y una infraestructura tecnológica compuesta por equipos de usuario, servidores, sistemas de información, almacenamiento en red y mecanismos de acceso remoto. La empresa ha presentado dos incidentes relevantes relacionados con archivos maliciosos. El primero ocurrió en octubre de 2024, cuando un archivo recibido mediante un correo electrónico malicioso fue descargado en el equipo de la gerente. El incidente fue identificado oportunamente, se aisló el equipo y posteriormente se realizó un formateo completo, evitando que la afectación se extendiera. El segundo incidente tuvo una mayor afectación y se originó cuando un funcionario de soporte desinstaló el antivirus para instalar una versión no oficial de Office. El archivo descargado posteriormente provocó la afectación de aproximadamente el 80 % de los archivos de ofimática, además de comprometer archivos .gdb asociados al sistema TNS y algunos archivos de configuración de Kubapp. La recuperación de Kubapp fue posible sin mayores dificultades. De acuerdo con la información suministrada para el diagnóstico, este último incidente generó cambios posteriores en los procedimientos y controles de seguridad de la organización.

Help Trauma IPS SAS presenta un antecedente relacionado principalmente con la alteración y manipulación de información. Según la información suministrada para este trabajo, se presentó una situación en la que personal interno, junto con el responsable de sistemas de ese momento, participó en procesos que ocasionaron afectaciones económicas y alteraciones en información y procesos manejados mediante archivos y el sistema Kubapp. Este antecedente resulta relevante para el diagnóstico debido a la importancia de

los controles de acceso, la gestión de usuarios y la trazabilidad de las operaciones realizadas sobre los sistemas de información.

Sociedad Médica Los Samanes SAS cuenta con una infraestructura de red de menor tamaño en comparación con las demás organizaciones evaluadas. Durante la revisión inicial se identificó además la presencia de equipos con varios años de uso, algunos de los cuales pueden encontrarse próximos a la obsolescencia. Estas condiciones serán consideradas durante el diagnóstico, especialmente al evaluar aspectos relacionados con actualización, soporte y capacidad tecnológica.

MK Insumos Inc. SAS será evaluada considerando los componentes tecnológicos, sistemas, usuarios, información y controles de seguridad que se encuentren dentro del alcance definido. Para esta organización no se cuenta, dentro de la información inicial suministrada, con antecedentes de incidentes de seguridad similares a los descritos para otras empresas, por lo que el diagnóstico permitirá establecer su situación actual a partir de la revisión técnica.

Sureca Ltda. presenta como antecedente un incidente relacionado con la presencia de software malicioso que ocasionó la interrupción del funcionamiento de un servidor durante aproximadamente dos días. La situación coincidió con la salida del anterior responsable de sistemas, quien no dejó disponible información suficiente sobre la infraestructura y configuración existente. Como consecuencia, la recuperación de los servicios requirió un proceso adicional de identificación y reconstrucción de la configuración necesaria para restablecer la operación.

Indubolsas Contreras SAS no registra, de acuerdo con la información suministrada para este diagnóstico, antecedentes de incidentes de características similares a los descritos en algunas de las demás empresas. Su evaluación se realizará a partir de las condiciones actuales de sus activos tecnológicos, sistemas, red, usuarios, información y controles de seguridad.

Las organizaciones se dividirán para efectos del análisis en dos grupos. El primero corresponde a las empresas del sector salud: Uronorte S.A., Help Trauma IPS SAS y Sociedad Médica Los Samanes SAS. En ellas, además de los criterios generales de ciberseguridad, se considerarán aspectos relacionados con la protección de información clínica y datos personales. El segundo grupo corresponde a MK Insumos Inc. SAS, Sureca Ltda. e Indubolsas Contreras SAS, en las cuales se aplicarán los criterios generales definidos para el diagnóstico.

Objetivo General

Analizar las vulnerabilidades de ciberseguridad presentes en seis empresas asesoradas por Prof&Tech, mediante un diagnóstico técnico que permita identificar sus principales riesgos y establecer recomendaciones orientadas al fortalecimiento de su postura de seguridad.

Objetivos Específicos

- Identificar las vulnerabilidades de ciberseguridad presentes en los componentes tecnológicos y procesos definidos dentro del alcance del diagnóstico de las seis empresas asesoradas por Prof&Tech.
- Analizar y valorar los riesgos asociados a las vulnerabilidades identificadas, considerando criterios de probabilidad e impacto y las características particulares de las organizaciones evaluadas.
- Establecer recomendaciones de seguridad orientadas a la mitigación de los riesgos identificados y al fortalecimiento de la postura de seguridad de las empresas objeto del diagnóstico.

Metodología del diagnóstico

El diagnóstico técnico se realizará en cuatro etapas: identificación de activos, identificación de vulnerabilidades, valoración del riesgo y análisis de resultados. El proceso se aplicará de manera similar en las seis empresas, teniendo en cuenta las características de cada infraestructura.

Primero se identificarán los activos incluidos en el diagnóstico, como equipos, servidores, redes, aplicaciones, bases de datos, usuarios, accesos remotos y sistemas de respaldo. Luego se revisarán sus condiciones de seguridad para detectar vulnerabilidades relacionadas con configuraciones, actualizaciones, contraseñas, usuarios, servicios, protección y copias de seguridad. Cada hallazgo será registrado con la evidencia correspondiente.

Las vulnerabilidades identificadas se valorarán mediante probabilidad e impacto, utilizando una escala de 1 a 3. El nivel de riesgo se determinará mediante la siguiente fórmula:

$$\text{Riesgo} = \text{Probabilidad} \times \text{Impacto}$$

Tabla 1. Clasificación del nivel de riesgo

<i>Puntaje</i>	<i>Nivel de riesgo</i>
1-2	Bajo
3-4	Medio
6-9	Alto

Fuente: Elaboración Propia

El nivel de riesgo se determinó mediante la multiplicación de la probabilidad por el impacto. Los resultados entre 1 y 2 se clasificaron como riesgo bajo, los resultados entre 3 y 4 como riesgo medio y los resultados entre 6 y 9 como riesgo alto.

Criterios de evaluación

La evaluación se realizará sobre las condiciones de seguridad encontradas en los activos incluidos en el diagnóstico. Según las características de cada empresa, se revisarán aspectos como actualización de sistemas y aplicaciones, configuraciones, usuarios y contraseñas, controles de acceso, servicios habilitados, protección de los equipos, copias de seguridad y acceso remoto.

Cada hallazgo se registrará junto con la evidencia obtenida y, cuando sea posible, se expresará mediante cantidad o porcentaje, con el fin de establecer una situación inicial de cada empresa.

El riesgo se determinará a partir de la probabilidad y el impacto, utilizando una escala de 1 a 3 para cada variable. El resultado permitirá clasificar los hallazgos en niveles bajo, medio o alto. Para las IPS también se considerarán aspectos relacionados con la protección de la información clínica y los datos personales.

Instrumento / matriz de diagnóstico

Para organizar los resultados se utilizará una matriz común para las seis empresas. En ella se registrarán los principales datos de cada hallazgo, desde el activo evaluado hasta su nivel de riesgo y la acción propuesta.

La matriz estará compuesta por los siguientes campos:

Tabla 2. *Matriz de Diagnostico*

Campo	Descripción
Empresa	Organización donde se realiza la evaluación.
Activo	Equipo, servidor, aplicación, red u otro recurso evaluado.
Aspecto evaluado	Condición de seguridad revisada.
Vulnerabilidad	Debilidad identificada durante el diagnóstico.
Evidencia	Resultado que sustenta el hallazgo.

Campo	Descripción
Cantidad / porcentaje	Magnitud del hallazgo cuando pueda ser cuantificada.
Probabilidad	Valor de 1 a 3 según la posibilidad de aprovechamiento.
Impacto	Valor de 1 a 3 según las posibles consecuencias.
Nivel de riesgo	Resultado obtenido de probabilidad $\times$ impacto.
Recomendación	Acción propuesta para tratar la vulnerabilidad.
Meta	Resultado cuantificable esperado después de aplicar la recomendación.

Fuente: Elaboración Propia

Escala de probabilidad e impacto

Para valorar los riesgos identificados se utilizará una escala de 1 a 3 para la probabilidad y el impacto. Esta clasificación permitirá aplicar el mismo criterio a los hallazgos de las seis empresas.

Tabla 3. Probabilidad

<i>Valor</i>	<i>Nivel</i>	<i>Criterio</i>
1	Baja	La vulnerabilidad presenta pocas condiciones para ser aprovechada.
2	Media	Existen condiciones que podrían facilitar su aprovechamiento.
3	Alta	La vulnerabilidad presenta condiciones claras para ser aprovechada.

Fuente: Elaboración Propia

Tabla 4. Impacto

<i>Valor</i>	<i>Nivel</i>	<i>Criterio</i>
1	Bajo	La afectación sería limitada y tendría pocas consecuencias para la organización.
2	Medio	La afectación podría comprometer parcialmente información, servicios u operaciones.
3	Alto	La afectación podría comprometer de forma significativa información, servicios u operaciones.

Fuente: Elaboración Propia

Diagnósticos

Diagnóstico de Uronorte S.A.

El diagnóstico técnico de Uronorte S.A. se realizó sobre la infraestructura tecnológica de sus sedes Caobos y Quirúrgica, tomando como referencia el inventario suministrado por la organización, compuesto por 66 equipos. La infraestructura cuenta además con dos servidores principales: el servidor ubicado en Caobos, destinado al funcionamiento del sistema TNS, y el servidor de la sede Quirúrgica, utilizado para el sistema Kubapp.

Las dos sedes se encuentran comunicadas mediante una VPN establecida a través de dispositivos Zyxel. Adicionalmente, la organización dispone de un servidor alternativo utilizado para las conexiones de contratistas externos que requieren acceder a Kubapp. Estas conexiones se realizan mediante escritorio remoto sobre una dirección IP interna y requieren previamente establecer la conexión a la VPN de la empresa.

En cuanto a los mecanismos de protección, los equipos evaluados cuentan con K7 Enterprise y firewall activo, registrándose una cobertura del 100 % sobre los 66 equipos. También se encuentra instalado AnyDesk para las labores de soporte técnico. En los equipos de usuario las conexiones requieren aceptación manual, mientras que los servidores principales cuentan con contraseña para el acceso remoto.

Resultados del análisis externo

La evaluación externa permitió identificar servicios accesibles desde Internet asociados principalmente a la infraestructura de red de la organización, así como se muestra en la Tabla 5.

Durante las pruebas se identificó el puerto 443/TCP asociado a la interfaz HTTPS de administración del dispositivo Zyxel USG60, y se comprobó externamente mediante navegador que la interfaz presentaba la pantalla de autenticación administrativa.

También se identificó el puerto 21/TCP abierto, asociado al servicio FTP del dispositivo USG60.

Adicionalmente, las pruebas sobre el servicio HTTPS permitieron identificar configuraciones criptográficas que requieren actualización.

Tabla 5. *Resultados análisis externo Uronorte*

<i>Elemento evaluado</i>	<i>Resultado</i>	<i>Interpretación</i>
<i>HTTPS</i>	443/TCP accesible	Interfaz HTTPS del Zyxel USG60 accesible desde Internet
<i>Administración del firewall</i>	Pantalla de autenticación visible	La interfaz administrativa puede ser alcanzada externamente
<i>FTP</i>	21/TCP abierto	Servicio FTP accesible desde Internet
<i>Certificado HTTPS</i>	Expirado	Requiere renovación
<i>SHA-1</i>	Identificado	Configuración criptográfica obsoleta
<i>RSA</i>	1024 bits	Tamaño de clave débil/obsoleto
<i>DH</i>	1024 bits	Grupo criptográfico obsoleto

Fuente: Elaboración Propia

Resultados de la evaluación interna

La revisión interna permitió analizar componentes relacionados con los servidores, sistemas de información, software instalado, mecanismos de protección, actualizaciones y servicios utilizados por la organización.

Se identificó que Uronorte cuenta con 66 equipos, todos registrados con cobertura de K7 Enterprise, además de dos servidores principales y un servidor alterno.

Durante la revisión también se identificaron diferencias en las fechas de actualización de algunos equipos. De los 66 equipos registrados, 20 presentaban fechas de actualización anteriores al 14 de septiembre de 2026, equivalentes al 30,30 % del inventario. Esta condición fue considerada para revisión, pero no se incorporó directamente como una vulnerabilidad dentro de los seis hallazgos finales.

También se identificaron 18 equipos con WPS registrado, equivalentes al 27,27 % del inventario. Esta condición quedó registrada como un aspecto que requiere verificación dentro del diagnóstico.

En los servidores se identificaron componentes de software que requieren atención, entre ellos MariaDB 10.5.29 y Python 3.10.1. Adicionalmente, se identificó una configuración CORS permisiva en uno de los servicios evaluados.

Tabla 6. Resultados análisis interno Uronorte

<i>Elemento evaluado</i>	<i>Resultado</i>	<i>Estado</i>
<i>Equipos evaluados</i>	66	Inventario
<i>Cobertura K7 Enterprise</i>	66/66 (100 %)	Control identificado
<i>Equipos con fechas de actualización anteriores al 14/09/2026</i>	20/66 (30,30 %)	Requiere verificación
<i>Equipos con WPS registrado</i>	18/66 (27,27 %)	Requiere verificación
<i>MariaDB</i>	10.5.29	Requiere actualización
<i>Python</i>	3.10.1	Requiere actualización
<i>Configuración CORS</i>	Access-Control-Allow-Origin: *	Requiere tratamiento
<i>NAS</i>	1	Control identificado

<i>Elemento evaluado</i>	Resultado	Estado
<i>Copias de seguridad</i>	Diarias	Control identificado

Fuente: Elaboración Propia

Usuarios y cuentas

Durante la revisión de la infraestructura se identificaron cinco cuentas destinadas al acceso remoto de contratistas. Estas cuentas son utilizadas para permitir conexiones hacia el sistema Kubapp mediante el servidor alterno.

De acuerdo con la información obtenida, durante el último mes se registraron conexiones mediante las cuentas remoto01 y remoto03, mientras que las demás cuentas no presentaron actividad durante dicho periodo.

La existencia de cuentas administrativas en los servidores forma parte de las necesidades normales de administración de estos equipos y, debido a que los servidores se encuentran destinados a funciones específicas y bajo control del personal encargado, no se consideró por sí misma una vulnerabilidad.

En relación con AnyDesk, se identificó su instalación en los equipos para actividades de soporte técnico. En los equipos de usuario las conexiones requieren aceptación manual, mientras que los servidores principales cuentan con contraseña para el acceso remoto. Por esta razón, la presencia de AnyDesk tampoco fue considerada por sí misma como una vulnerabilidad.

Tabla 7. *Accesos remotos Uronorte*

<i>Elemento</i>	<i>Resultado</i>
<i>Cuentas de acceso remoto</i>	5
<i>Cuentas con actividad reciente</i>	remoto01 y remoto03
<i>Cuentas sin actividad reciente</i>	3
<i>Servidor alterno para conexiones</i>	1
<i>AnyDesk</i>	Instalado para soporte
<i>Aceptación manual en equipos de usuario</i>	Sí
<i>Contraseña en servidores principales</i>	Sí

Fuente: Elaboración Propia

Vulnerabilidades identificadas

Tabla 8. *Vulnerabilidades Uronorte*

<i>Código</i>	<i>Vulnerabilidad identificada</i>	<i>Probabilidad</i>	<i>Impacto</i>	<i>Riesgo</i>	<i>Nivel</i>
URO-01	Configuración criptográfica insegura en HTTPS	3	2	6	Alto
URO-02	MariaDB fuera de soporte	3	3	9	Alto
URO-03	Python desactualizado	2	2	4	Medio
URO-04	Política CORS permisiva	2	2	4	Medio
URO-05	Interfaz administrativa del firewall expuesta a Internet	3	3	9	Alto
URO-06	Servicio FTP expuesto a Internet	2	2	4	Medio

Fuente: Elaboración Propia

URO-01 – Configuración criptográfica insegura en HTTPS

Se asignó probabilidad 3 e impacto 2, ya que el servicio utiliza un certificado expirado y configuraciones criptográficas obsoletas, incluyendo SHA-1, RSA de 1024 bits y DH de 1024 bits. Estas condiciones debilitan la protección de las comunicaciones, aunque durante las pruebas no se evidenció una interceptación o compromiso directo del servicio. Riesgo: 6 (alto).

Recomendación: reemplazar el certificado por uno vigente y utilizar claves y algoritmos criptográficos modernos, eliminando las configuraciones que empleen RSA o DH de 1024 bits.

Meta: alcanzar 0 certificados expirados y 0 configuraciones criptográficas con claves o grupos de 1024 bits en los servicios HTTPS evaluados.

URO-02 – MariaDB fuera de soporte

Se asignó probabilidad 3 e impacto 3, debido a que el servidor utiliza MariaDB 10.5.29, versión identificada durante el diagnóstico como fuera de soporte. Esta condición dificulta la aplicación de actualizaciones de seguridad y afecta un componente utilizado para soportar aplicaciones y datos operativos. Riesgo: 9 (alto).

Recomendación: actualizar MariaDB a una versión actualmente soportada, realizando previamente pruebas de compatibilidad y respaldo de las bases de datos.

Meta: tener el 100 % de los motores de base de datos en versiones soportadas.

URO-03 – Python desactualizado

Se asignó probabilidad 2 e impacto 2, debido a que se encontró Python 3.10.1 instalado en el servidor. Esta versión es antigua y puede limitar el acceso a actualizaciones

y correcciones de seguridad. Sin embargo, no se comprobó una vulnerabilidad explotable directamente asociada a las aplicaciones evaluadas. Riesgo: 4 (medio).

Recomendación: actualizar Python a una versión con soporte de seguridad vigente y verificar la compatibilidad de las aplicaciones y sus dependencias antes de realizar el cambio.

Meta: que el 100 % de las aplicaciones evaluadas utilicen versiones de Python con soporte de seguridad vigente.

URO-04 – Política CORS permisiva

Se asignó probabilidad 2 e impacto 2, debido a que el servicio respondió a un origen externo utilizando Access-Control-Allow-Origin: * junto con Access-Control-Allow-Credentials: true. La prueba confirmó la configuración, pero no demostró acceso no autorizado a información protegida. Riesgo: 4 (medio).

Recomendación: restringir CORS únicamente a los dominios que realmente necesitan consumir el servicio y evitar el uso de comodines cuando existan mecanismos de autenticación.

Meta: reducir a 0 los orígenes no autorizados dentro de la configuración CORS de los servicios evaluados.

URO-05 – Interfaz administrativa del firewall expuesta a Internet

Se asignó probabilidad 3 e impacto 3, debido a que la interfaz de administración del Zyxel USG60 puede ser alcanzada directamente desde Internet. Un eventual acceso administrativo no autorizado podría afectar configuraciones críticas de red y seguridad. Durante la evaluación no se realizaron pruebas de credenciales ni fuerza bruta. Riesgo: 9 (alto).

Recomendación: restringir la administración del firewall a la red interna, una VPN de administración o direcciones IP previamente autorizadas, evitando la exposición directa del panel administrativo a Internet.

Meta: reducir de 1 a 0 las interfaces administrativas de dispositivos de red accesibles directamente desde Internet.

URO-06 – Servicio FTP expuesto a Internet

Se asignó probabilidad 2 e impacto 2, debido a que el puerto 21/TCP se encuentra accesible desde Internet y corresponde al servicio FTP del USG60. Esta exposición puede representar un riesgo si el servicio no es necesario, permite acceso no autorizado o transmite información sin mecanismos adecuados de protección. No se comprobó acceso anónimo durante la evaluación. Riesgo: 4 (medio).

Recomendación: verificar la necesidad del servicio FTP y, si no es indispensable, deshabilitarlo. Si debe mantenerse, restringir su acceso a las redes autorizadas y utilizar mecanismos de transferencia segura.

Meta: reducir a 0 los servicios FTP innecesarios accesibles desde Internet.

Diagnóstico de Help Trauma IPS SAS

El diagnóstico se realizó mediante una combinación de revisión externa de la infraestructura y verificación interna de la configuración del servidor.

Desde el exterior se realizaron pruebas de identificación de servicios y puertos utilizando Nmap. Adicionalmente, se realizaron verificaciones sobre protocolos y servicios potencialmente expuestos.

En el entorno interno se revisaron configuraciones relacionadas con:

- Sistema operativo.
- Actualizaciones.
- Cuentas de usuario.
- Política de contraseñas.
- Firewall.
- Puertos en escucha.
- Servicios activos.
- SMB.
- RDP.
- Herramientas de acceso remoto.
- Base de datos MariaDB.
- Mecanismos de respaldo.

Resultados del análisis externo

La exploración mediante Nmap permitió determinar que el equipo se encontraba activo, pero los puertos incluidos en las pruebas externas no respondieron como servicios TCP accesibles desde Internet.

Tabla 9. Resultado de pruebas externas Help Trauma

<i>Prueba</i>	<i>Resultado</i>	<i>Interpretación</i>
<i>nmap -Pn -sV</i>	Puertos filtrados	No se identificaron servicios TCP accesibles entre los 1000 puertos analizados
<i>nmap -Pn --script vuln</i>	Sin servicios identificados	No se obtuvieron vulnerabilidades mediante esta prueba externa
<i>nmap -Pn -p 443 --script ssl-enum-ciphers</i>	Puerto filtrado	No fue posible realizar evaluación SSL externa
<i>Exploración de puertos</i>	Filtrados	Existe filtrado de tráfico entrante

Fuente: Elaboración Propia

Este resultado constituye un control positivo, debido a que durante la evaluación no se identificaron servicios TCP directamente accesibles desde Internet.

Resultados de la evaluación interna

La revisión interna permitió obtener información más detallada sobre la configuración del servidor.

El equipo analizado corresponde a un sistema Windows 10 Pro, versión 2009, compilación 19045, arquitectura de 64 bits.

Se identificó que el equipo cuenta con actualizaciones recientes, incluyendo la actualización KB5126256, instalada el 10 de septiembre de 2026.

Tabla 10. *Revisión interna Help Trauma*

<i>Elemento</i>	<i>Resultado</i>
<i>Sistema operativo</i>	Windows 10 Pro
<i>Versión</i>	2009
<i>Compilación</i>	19045
<i>Arquitectura</i>	64 bits
<i>Última actualización identificada</i>	KB5126256
<i>Fecha de instalación</i>	10/09/2026
<i>Estado</i>	Actualizado

Fuente: Elaboración Propia

No se identifica una vulnerabilidad asociada a la falta de actualización del sistema operativo.

Usuarios y cuentas

Durante la revisión se identificaron diferentes cuentas locales.

Entre ellas se encontraron cuentas deshabilitadas como Administrador, annes, banca, gerso y sopor, mientras que algunas cuentas permanecían habilitadas.

Un aspecto relevante fue la cuenta Invitado, que se encontraba habilitada y presentaba un registro de inicio de sesión reciente.

Tabla 11. *Usuarios servidor Help Trauma*

<i>Cuenta</i>	<i>Estado</i>	<i>Último acceso</i>
<i>Administrador</i>	Deshabilitada	—
<i>annes</i>	Deshabilitada	—
<i>banca</i>	Deshabilitada	—
<i>gerso</i>	Deshabilitada	—
<i>Invitado</i>	Habilitada	17/09/2026
<i>SERVIDOR-241</i>	Habilitada	—
<i>SISTEMAS</i>	Habilitada	—
<i>sopor</i>	Deshabilitada	—
<i>WDAGUtilityAccount</i>	Deshabilitada	—

Fuente: Elaboración Propia

Vulnerabilidades identificadas

Tabla 12. Vulnerabilidades Identificadas Help Trauma

<i>Código</i>	<i>Vulnerabilidad identificada</i>	<i>Probabilidad</i>	<i>Impacto</i>	<i>Riesgo</i>	<i>Nivel</i>
HT-01	Cuenta Invitado habilitada y con uso reciente	3	3	9	Alto
HT-02	Política de contraseñas insuficiente	3	3	9	Alto
HT-03	Configuración permisiva de acceso en MariaDB	2	3	6	Alto

Código	Vulnerabilidad identificada	Probabilidad	Impacto	Riesgo	Nivel
HT-04	Ausencia de protección antivirus en equipos de usuario	3	3	9	Alto
HT-05	Múltiples herramientas de acceso remoto habilitadas	2	2	4	Medio
HT-06	Cuentas de acceso remoto innecesarias	2	2	4	Medio

Fuente: Elaboración Propia

HT-01 – Cuenta Invitado habilitada y con uso reciente

Se asignó probabilidad 3 e impacto 3, debido a que la cuenta Invitado se encontraba habilitada y registraba un inicio de sesión reciente, correspondiente al 17 de septiembre de 2026. El uso de una cuenta genérica dificulta la trazabilidad de las actividades realizadas y puede facilitar accesos no autorizados si sus credenciales son conocidas o reutilizadas. Riesgo: 9 (alto).

Recomendación: deshabilitar la cuenta Invitado cuando no exista una necesidad operacional que justifique su utilización. Los accesos que requieran permisos especiales deben realizarse mediante cuentas individuales que permitan identificar al responsable de cada actividad.

Meta: alcanzar 0 cuentas genéricas o de invitado habilitadas sin justificación operacional.

HT-02 – Política de contraseñas insuficiente

Se asignó probabilidad 3 e impacto 3, debido a que la política de seguridad del equipo no establece una longitud mínima de contraseña, no utiliza historial de contraseñas

y no contempla un umbral de bloqueo por intentos fallidos. La configuración identificada puede facilitar ataques basados en contraseñas débiles o intentos repetitivos de autenticación. Riesgo: 9 (alto).

Recomendación: establecer una política de contraseñas que incluya una longitud mínima, historial de contraseñas y bloqueo temporal después de varios intentos fallidos. También se recomienda utilizar cuentas individuales y evitar credenciales compartidas.

Meta: alcanzar 100 % de los equipos con políticas de contraseña definidas y mecanismos de bloqueo ante intentos fallidos.

HT-03 – Configuración permisiva de acceso en MariaDB

Se asignó probabilidad 2 e impacto 3, debido a que se identificó la cuenta Prof&Tech configurada con el host %, permitiendo que la cuenta pueda autenticarse desde diferentes equipos que tengan conectividad con el servicio. Aunque las pruebas externas no evidenciaron que el puerto 3306 estuviera directamente expuesto a Internet, esta configuración amplía innecesariamente el origen desde el cual puede realizarse una conexión a la base de datos. Riesgo: 6 (alto).

Recomendación: restringir las cuentas de MariaDB a los equipos, servidores o segmentos de red que realmente requieran acceso, evitando el uso de % cuando no sea necesario. También se deben revisar periódicamente los usuarios y privilegios asignados.

Meta: alcanzar 100 % de las cuentas de MariaDB con el origen de conexión restringido de acuerdo con su necesidad operacional.

HT-04 – Ausencia de protección antivirus en equipos de usuario

Se asignó probabilidad 3 e impacto 3, debido a que, de acuerdo con la información recopilada durante el diagnóstico, ninguno de los 18 equipos de usuario cuenta con una

solución antivirus institucional. Esta situación reduce la capacidad de prevención y detección frente a malware, archivos maliciosos y otras amenazas que puedan ingresar a través de los equipos de los usuarios. En el servidor se identificó activo Microsoft Defender, por lo que el hallazgo corresponde específicamente a los equipos de usuario. Riesgo: 9 (alto).

Recomendación: implementar una solución antimalware administrada en los equipos de usuario, con actualización automática, monitoreo centralizado y mecanismos de detección y respuesta ante amenazas.

Meta: alcanzar 18 de 18 equipos protegidos, equivalente a una cobertura del 100 %.

HT-05 – Múltiples herramientas de acceso remoto habilitadas

Se asignó probabilidad 2 e impacto 2, debido a que durante la revisión se identificaron diferentes herramientas de acceso remoto instaladas o activas, entre ellas AnyDesk, TeamViewer y RustDesk. La utilización simultánea de varias herramientas puede aumentar la superficie de administración y dificultar el control de las conexiones remotas, especialmente cuando alguna de ellas no tiene una necesidad operacional vigente. Riesgo: 4 (medio).

Recomendación: realizar un inventario de las herramientas de acceso remoto y mantener únicamente aquellas que sean necesarias para las actividades de soporte. Las herramientas autorizadas deben contar con controles de autenticación, registro y revisión periódica de las conexiones.

Meta: mantener 100 % de las herramientas de acceso remoto identificadas, autorizadas y justificadas operacionalmente.

HT-06 – Cuentas de acceso remoto innecesarias

Se asignó probabilidad 2 e impacto 2, debido a que se identificaron dos cuentas destinadas al acceso remoto que, según la información suministrada durante el diagnóstico, no son necesarias actualmente. Mantener cuentas de acceso que no tienen una función vigente incrementa la superficie de ataque y puede generar accesos no autorizados si las credenciales permanecen activas. Riesgo: 4 (medio).

Recomendación: deshabilitar las cuentas de acceso remoto que actualmente no sean necesarias y establecer un procedimiento de revisión periódica para identificar y retirar cuentas que hayan dejado de cumplir una función operacional.

Meta: alcanzar 0 cuentas de acceso remoto innecesarias habilitadas.

Diagnóstico de Sociedad Médica Los Samanes SAS

El diagnóstico técnico de Sociedad Médica Los Samanes SAS se realizó sobre una infraestructura tecnológica de tamaño reducido, compuesta por 13 equipos de cómputo, sin servidores físicos propios. La organización se encuentra actualmente en proceso de liquidación, aunque continúa desarrollando actividades y utilizando sus sistemas tecnológicos para mantener la operación.

La infraestructura está conformada por 7 equipos con Windows 7, 3 equipos con Windows 8 y 3 equipos con Windows 10. Los equipos presentan varios años de uso y, de acuerdo con la información suministrada durante el diagnóstico, 6 de ellos han superado en más del doble la vida útil estimada para este tipo de equipos.

Debido a las limitaciones de recursos, la organización no cuenta con un servidor físico para alojar sus sistemas. Para el funcionamiento del sistema Kubapp se utiliza la modalidad en línea, por lo que las actividades relacionadas con este sistema dependen directamente de la disponibilidad de la conexión a Internet.

La organización cuenta con una conexión de 200 Mbps proporcionada por Movistar, sin dirección IP pública fija. La conexión se distribuye mediante el router suministrado por el operador y posteriormente mediante un switch. No se identificó un firewall dedicado entre la red interna y el equipo proporcionado por el operador.

La organización tampoco cuenta actualmente con mecanismos formales de respaldo de la información local ni realiza pruebas de recuperación. Estas condiciones adquieren especial importancia debido a que parte de la información de trabajo se almacena directamente en los equipos de los usuarios.

Resultados del análisis externo

Debido a que la organización no dispone de una dirección IP pública fija ni de servicios propios publicados hacia Internet, no se identificaron servicios externos específicos asociados a servidores de la organización.

La infraestructura depende principalmente de la conexión proporcionada por el operador de Internet y del servicio en línea de Kubapp.

Tabla 13. *Análisis Externo Samanes*

<i>Elemento evaluado</i>	<i>Resultado</i>	<i>Interpretación</i>
<i>Conexión a Internet</i>	200 Mbps	Servicio utilizado para la operación
<i>Proveedor</i>	Movistar	Proveedor de conectividad
<i>IP pública fija</i>	No dispone	La organización no cuenta con IP pública estática
<i>Servidor propio expuesto</i>	No identificado	No existen servidores propios publicados
<i>Servicios externos propios</i>	No identificados	La operación depende principalmente de servicios en línea
<i>RDP</i>	No disponible	No se identificó este mecanismo de acceso

Elemento evaluado	Resultado	Interpretación
<i>Base de datos expuesta</i>	No identificada	No existen bases de datos locales
<i>Kubapp</i>	Servicio en línea	Dependencia externa para la operación

Fuente: Elaboración Propia

Resultados de la evaluación interna

La revisión interna permitió identificar una infraestructura tecnológica limitada y con un nivel importante de obsolescencia.

De los 13 equipos evaluados, 7 utilizan Windows 7, 3 utilizan Windows 8 y 3 utilizan Windows 10. Por tanto, ninguno de los equipos utiliza actualmente una versión moderna de Windows.

Esta situación representa una condición relevante desde el punto de vista de seguridad. Windows 7 y Windows 8.1 se encuentran fuera de soporte, mientras que Windows 10 terminó su soporte general el 14 de octubre de 2025.

La organización tampoco cuenta con una solución antivirus instalada en los equipos evaluados.

Tabla 14. *Sistemas Operativos Samanes*

<i>Sistema operativo</i>	<i>Equipos</i>	<i>Porcentaje</i>
<i>Windows 7</i>	7	53,85 %
<i>Windows 8</i>	3	23,08 %
<i>Windows 10</i>	3	23,08 %
Total	13	100 %

Fuente: Elaboración Propia

Tabla 15. *Análisis interno Samanes*

<i>Elemento evaluado</i>	<i>Resultado</i>	<i>Estado</i>
<i>Equipos evaluados</i>	13	Inventario
<i>Servidores físicos</i>	0	No dispone
<i>Antivirus</i>	0/13	Requiere tratamiento
<i>Firewall dedicado</i>	0	Requiere tratamiento
<i>RDP</i>	No disponible	Control identificado
<i>AnyDesk</i>	Instalado	Requiere control
<i>Bases de datos locales</i>	No existen	Control/arquitectura
<i>Kubapp</i>	Servicio en línea	Dependencia externa
<i>Copias de seguridad</i>	No existen	Requiere tratamiento
<i>Pruebas de recuperación</i>	No se realizan	Requiere tratamiento
<i>Wi-Fi</i>	Disponible	Requiere verificación
<i>Equipos antiguos</i>	13/13	Requiere tratamiento
<i>Equipos con más del doble de vida útil</i>	6/13	Requiere tratamiento

Fuente: Elaboración Propia

Usuarios y cuentas

Cada equipo cuenta con un usuario para su funcionamiento, y no se reportó la existencia de cuentas compartidas entre diferentes equipos.

Esta condición permite mantener una separación básica entre los usuarios y evita que varias personas utilicen una misma cuenta para acceder al sistema operativo.

Sin embargo, debido a que la organización cuenta con poco personal y los funcionarios deben asumir diferentes responsabilidades, resulta importante mantener controles sobre los permisos de los usuarios y evitar que las necesidades operativas conduzcan al uso de cuentas con privilegios superiores a los necesarios.

En relación con el acceso remoto, se identificó AnyDesk instalado en los equipos. Las conexiones requieren la aceptación manual del usuario, por lo que no se consideró la herramienta como una vulnerabilidad por sí misma.

Tabla 16. Accesos Samanes

<i>Elemento</i>	<i>Resultado</i>
<i>Usuarios por equipo</i>	1
<i>Cuentas compartidas reportadas</i>	No
<i>AnyDesk</i>	Sí
<i>Contraseña permanente de AnyDesk</i>	No
<i>Aceptación manual de conexión</i>	Sí
<i>RDP</i>	No
<i>Personal dedicado exclusivamente a sistemas</i>	No

Fuente: Elaboración Propia

Vulnerabilidades identificadas

Tabla 17. Vulnerabilidades Samanes

<i>Código</i>	<i>Vulnerabilidad identificada</i>	<i>Probabilidad</i>	<i>Impacto</i>	<i>Riesgo</i>	<i>Nivel</i>
SAM-01	Sistemas operativos fuera de soporte	3	3	9	Alto
SAM-02	Ausencia de protección antivirus	3	3	9	Alto
SAM-03	Ausencia de mecanismos de respaldo	3	3	9	Alto
SAM-04	Obsolescencia de los equipos de cómputo	3	2	6	Alto
SAM-05	Ausencia de firewall dedicado en la red interna	2	3	6	Alto

Fuente: Elaboración Propia

SAM-01 – Sistemas operativos fuera de soporte

Se asignó probabilidad 3 e impacto 3, debido a que los 13 equipos evaluados utilizan sistemas operativos antiguos: 7 equipos con Windows 7, 3 con Windows 8 y 3 con Windows 10. Windows 7 y Windows 8.1 se encuentran fuera de soporte, mientras que Windows 10 terminó su soporte general el 14 de octubre de 2025. El uso de sistemas operativos sin soporte limita la disponibilidad de actualizaciones y correcciones de seguridad. Riesgo: 9 (alto).

Recomendación: establecer un plan progresivo de actualización o sustitución de los equipos, priorizando aquellos que no cumplen con los requisitos para utilizar una versión de Windows actualmente soportada.

Meta: alcanzar 100 % de los equipos utilizando sistemas operativos con soporte de seguridad vigente, o contar con una medida de soporte extendido formalmente implementada cuando corresponda.

SAM-02 – Ausencia de protección antivirus

Se asignó probabilidad 3 e impacto 3, debido a que ninguno de los 13 equipos evaluados cuenta con una solución antivirus instalada. Esta condición reduce la capacidad de prevención y detección frente a malware, archivos maliciosos y otras amenazas que puedan afectar los equipos utilizados para las actividades de la organización. Riesgo: 9 (alto).

Recomendación: implementar una solución antimalware en los equipos de la organización, preferiblemente con administración centralizada y actualización automática.

Meta: alcanzar 13 de 13 equipos protegidos, equivalente al 100 % de cobertura.

SAM-03 – Ausencia de mecanismos de respaldo

Se asignó probabilidad 3 e impacto 3, debido a que la organización no cuenta con un mecanismo formal de copias de seguridad de la información almacenada localmente y tampoco realiza pruebas de recuperación. Esta condición puede generar pérdida permanente de información ante fallas de hardware, malware, eliminación accidental o daños en los equipos. El riesgo adquiere mayor relevancia debido a que parte de la información operacional se encuentra almacenada en archivos de Excel. Riesgo: 9 (alto).

Recomendación: establecer un mecanismo de respaldo periódico para la información crítica, utilizando al menos una copia externa o en la nube y definiendo un procedimiento para comprobar periódicamente la recuperación de los archivos.

Meta: alcanzar 100 % de la información crítica identificada con respaldo periódico y realizar al menos una prueba de recuperación documentada por periodo definido por la organización.

SAM-04 – Obsolescencia de los equipos de cómputo

Se asignó probabilidad 3 e impacto 2, debido a que los 13 equipos presentan varios años de uso y seis de ellos han superado en más del doble la vida útil estimada. La antigüedad del hardware dificulta la actualización hacia sistemas operativos modernos y puede incrementar la probabilidad de fallas de hardware, problemas de compatibilidad y limitaciones para implementar controles de seguridad actuales. Riesgo: 6 (alto).

Recomendación: establecer un plan de renovación tecnológica gradual, priorizando los seis equipos que presentan mayor antigüedad y aquellos que no cumplen los requisitos técnicos para sistemas operativos soportados.

Meta: reducir de 6 a 0 los equipos que superan en más del doble la vida útil definida por la organización, mediante renovación o sustitución progresiva.

SAM-05 – Ausencia de firewall dedicado en la red interna

Se asignó probabilidad 2 e impacto 3, debido a que la infraestructura de red utiliza directamente el router proporcionado por el operador y posteriormente un switch, sin contar con un dispositivo firewall dedicado administrado por la organización. Esta condición limita la capacidad de establecer controles específicos sobre el tráfico de la red interna y la segmentación de los dispositivos. Riesgo: 6 (alto).

Recomendación: evaluar la implementación de un firewall administrable entre el router del operador y la red interna, acompañado de reglas de filtrado, control de tráfico y, cuando sea posible, segmentación de la red.

Meta: contar con 1 dispositivo o mecanismo de firewall administrable implementado y configurado para proteger la red interna.

Análisis de las condiciones de ciberseguridad en las IPS evaluadas

Las tres organizaciones del sector salud incluidas en el diagnóstico —Uronorte S.A., Help Trauma IPS SAS y Sociedad Médica Los Samanes SAS— presentan diferencias importantes en cuanto a infraestructura, capacidad tecnológica y controles de seguridad. Sin embargo, existe un elemento común que hace que los hallazgos identificados tengan una relevancia particular: las organizaciones desarrollan actividades relacionadas con la prestación de servicios de salud y, por tanto, pueden manejar información personal y datos relacionados con la salud de los pacientes.

En Colombia, la historia clínica tiene un carácter reservado y su acceso debe estar limitado a las personas autorizadas y a los fines establecidos por la normativa. La Resolución 1995 de 1999 establece además que los prestadores deben garantizar condiciones que preserven la integridad de la información y eviten su alteración. Por su parte, la Ley 215 de 2020 establece que la Historia Clínica Electrónica debe gestionarse bajo condiciones de seguridad, integridad, autenticidad, confiabilidad, conservación, disponibilidad y control del acceso.

Tabla 18. Comparación de las condiciones identificadas para empresas del sector salud

<i>Aspecto</i>	<i>Uronorte S.A.</i>	<i>Help Trauma IPS</i> <i>SAS</i>	<i>Sociedad Médica Los</i> <i>Samanes SAS</i>
<i>Equipos</i>	66	18	13
<i>Servidores</i>	2 principales + 1 alterno	1	0
<i>Sistema principal</i>	TNS / Kubapp	Kubapp	Kubapp en línea
<i>Base de datos</i>	MariaDB / otras según sistema	MariaDB	Sin BD local
<i>Protección antimalware</i>	K7 Enterprise	Sin protección institucional en equipos	Sin antivirus
<i>Copias de seguridad</i>	Diarias, múltiples destinos	Diarias, local + nube	No existen
<i>Recuperación</i>	Pruebas periódicas	Pruebas mensuales	No se realizan
<i>Acceso remoto</i>	AnyDesk + mecanismos adicionales	AnyDesk, TeamViewer y RustDesk	AnyDesk
<i>Estado de sistemas</i>	Se identificaron componentes desactualizados	Equipos reportados actualizados	7 Windows 7, 3 Windows 8 y 3 Windows 10
<i>Infraestructura de red</i>	VPN, firewall y NAS	Firewall en servidor	Router del operador + switch
<i>Principales riesgos identificados</i>	Exposición de servicios y componentes desactualizados	Cuentas, contraseñas, protección de endpoints y BD	Obsolescencia, ausencia de antivirus, respaldo y controles de red

Fuente: Elaboración Propia

Reflexión sobre la información clínica y los riesgos identificados

La comparación que se muestra en la Tabla 16 resulta especialmente relevante cuando se considera que la información relacionada con la salud requiere un tratamiento cuidadoso. La normativa colombiana establece que la historia clínica es reservada y que su custodia debe garantizar condiciones de integridad y acceso restringido. Además, la regulación actual de la Historia Clínica Electrónica Interoperable busca que los datos clínicos puedan ser compartidos entre los diferentes actores del sistema bajo condiciones de seguridad y confidencialidad.

En este contexto, una vulnerabilidad encontrada en un equipo de cómputo de una IPS no debe considerarse únicamente como un problema técnico del dispositivo. El impacto potencial puede extenderse a la información de los pacientes y a la continuidad de los procesos de atención. Por ejemplo, una infección de malware podría afectar la disponibilidad de los sistemas; una configuración inadecuada de usuarios podría facilitar el acceso a información que no corresponde a las funciones del trabajador; y la ausencia de copias de seguridad podría dificultar la recuperación de información ante una pérdida o alteración.

Tabla 19. *Relación entre los hallazgos y los principios de seguridad de la información en salud*

<i>Principio</i>	<i>Situaciones identificadas en las IPS</i>	<i>Posible consecuencia</i>
<i>Confidencialidad</i>	Cuentas con configuraciones inadecuadas, políticas de contraseñas débiles, servicios administrativos expuestos y ausencia de controles suficientes	Acceso de personas no autorizadas a información de pacientes o información administrativa
<i>Integridad</i>	Software desactualizado, configuraciones inseguras, ausencia de controles y antecedentes de malware	Modificación, corrupción o alteración de información

Principio	Situaciones identificadas en las IPS	Posible consecuencia
Disponibilidad	Ausencia de respaldos, equipos obsoletos, dependencia de Internet y exposición a malware	Interrupción de sistemas o dificultad para recuperar información
Trazabilidad	Cuentas genéricas, gestión insuficiente de usuarios o controles de acceso limitados	Dificultad para determinar quién realizó determinada actividad
Continuidad	Dependencia de infraestructura limitada y ausencia de mecanismos formales de recuperación	Mayor tiempo de recuperación ante fallas o incidentes

Fuente: Elaboración Propia

El análisis de las tres IPS presentado en la Tabla 17, permite observar que la ciberseguridad en el sector salud no depende exclusivamente del tamaño o del nivel de inversión tecnológica de una organización. Uronorte dispone de una infraestructura más robusta y de múltiples controles, pero presenta vulnerabilidades en determinados servicios y componentes; Help Trauma cuenta con una infraestructura intermedia, aunque mantiene debilidades relacionadas con autenticación, cuentas y protección de los equipos; mientras que Sociedad Médica Los Samanes presenta limitaciones estructurales que incrementan su exposición tecnológica.

Diagnóstico de MK Insumos Inc. S.A.S.

El diagnóstico técnico de MK Insumos Inc. S.A.S. se realizó sobre una infraestructura compuesta por 14 equipos y un servidor, todos basados en Windows y ubicados en una única sede. La organización cuenta con conexión a Internet mediante una infraestructura de router con firewall, utiliza herramientas de acceso remoto y dispone de mecanismos de respaldo de información.

Para la evaluación externa se realizaron pruebas de reconocimiento sobre la dirección IP pública, utilizando Nmap para identificar puertos, servicios y posibles vulnerabilidades conocidas. Los resultados mostraron que los puertos analizados se encontraban filtrados desde Internet, incluyendo el puerto 443, por lo que no se identificaron servicios internos directamente expuestos a través de la dirección pública.

Resultados del análisis externo

El análisis externo realizado sobre la IP pública, no identificó puertos TCP accesibles desde Internet dentro del conjunto evaluado.

La prueba de detección de servicios mediante `nmap -Pn -sV` encontró los 1000 puertos analizados en estado `filtered`, mientras que la prueba de vulnerabilidades mediante `--script vuln` tampoco obtuvo respuestas de servicios expuestos. La prueba específica sobre el puerto 443 igualmente mostró el estado `filtered`, por lo que no fue posible realizar una evaluación de los cifrados HTTPS desde el exterior.

Resultados de la evaluación interna

El servidor utiliza Windows 10 Pro, compilación 22631, y cuenta con actualizaciones recientes, entre ellas KB5066133 y KB5068865. Sin embargo, Windows 10 terminó su soporte general el 14 de octubre de 2025. Microsoft indica que los equipos que continúan utilizando Windows 10 deben migrar a una versión soportada o estar cubiertos por el programa ESU; en la información proporcionada no se evidencia que este equipo se encuentre inscrito en ESU.

También se encontró que los tres perfiles del Firewall de Windows se encuentran deshabilitados. Aunque la empresa dispone de firewall a nivel del router, esto significa que el propio servidor no cuenta con una capa activa de filtrado local.

En el servidor se encuentran activos múltiples servicios y puertos, entre ellos MariaDB 3306, Firebird 3050, HTTP 80, 8080, 8443, FTP, impresión, servicios de

Windows y diferentes componentes de Kubapp. También se encuentran instalados y activos AnyDesk, TeamViewer y RustDesk.

Vulnerabilidades identificadas

Tabla 20. *Vulnerabilidades Identificadas en MK*

<i>ID</i>	<i>Vulnerabilidad</i>	<i>Probabilidad</i>	<i>Impacto</i>	<i>Riesgo</i>	<i>Nivel</i>
MK-01	Sistema operativo Windows 10 Pro fuera de soporte general	3	3	9	Alto
MK-02	Firewall local de Windows deshabilitado	3	3	9	Alto
MK-03	Escritorio remoto habilitado sin necesidad declarada	2	3	6	Alto
MK-04	Política de contraseñas insuficiente	3	3	9	Alto
MK-05	Cuentas locales habilitadas sin actividad reciente	2	2	4	Medio
MK-06	Múltiples herramientas de acceso remoto activas	2	2	4	Medio

Fuente: Elaboración Propia

MK-01. Sistema operativo Windows 10 Pro fuera de soporte general

Se asignó probabilidad 3 e impacto 3, debido a que el servidor utiliza Windows 10 Pro y el soporte general de esta versión finalizó el 14 de octubre de 2025. Aunque se encontraron actualizaciones instaladas recientemente, no se evidenció durante el diagnóstico la inscripción del equipo en un esquema ESU. Un sistema operativo fuera de soporte puede dejar de recibir actualizaciones de seguridad generales y aumentar la exposición frente a vulnerabilidades conocidas. Riesgo: 9 (alto).

Recomendación: migrar el servidor a una versión de Windows Server soportada o establecer formalmente un mecanismo de soporte extendido mientras se realiza la migración.

Meta: contar con el servidor sobre una plataforma con soporte de seguridad vigente y mantener evidencia de actualización.

MK-02. Firewall local de Windows deshabilitado

Se asignó probabilidad 3 e impacto 3, debido a que los tres perfiles del Firewall de Windows se encuentran deshabilitados. Aunque existe un firewall configurado a nivel del router, el servidor queda sin una capa de filtrado local que permita controlar específicamente las conexiones dirigidas hacia sus servicios. Riesgo: 9 (alto).

Recomendación: habilitar el Firewall de Windows y establecer reglas únicamente para los servicios requeridos por la operación, manteniendo el firewall perimetral como segunda capa de protección.

Meta: mantener los perfiles correspondientes del firewall local habilitados y documentar las excepciones necesarias.

MK-03. Escritorio remoto habilitado sin necesidad declarada

Se asignó probabilidad 2 e impacto 3, debido a que la configuración del sistema muestra `fDenyTSConnections = 0`, indicando que las conexiones mediante Escritorio remoto están habilitadas, mientras que en el levantamiento de información se indicó que RDP no era utilizado. Esta diferencia representa una superficie de acceso adicional que no está justificada dentro de las necesidades declaradas de la organización. Riesgo: 6 (alto).

Recomendación: deshabilitar RDP si realmente no es requerido. Si existe una necesidad operativa, restringirlo a las direcciones o redes autorizadas y aplicar mecanismos adicionales de autenticación y control.

Meta: mantener únicamente mecanismos de acceso remoto previamente autorizados y documentados.

MK-04. Política de contraseñas insuficiente

Se asignó probabilidad 3 e impacto 3, debido a que la política local establece una longitud mínima de contraseña de 0 caracteres, no mantiene historial de contraseñas y no establece un umbral de bloqueo por intentos fallidos. Estas condiciones facilitan escenarios de contraseñas débiles o ataques de fuerza bruta contra cuentas locales. Riesgo: 9 (alto).

Recomendación: establecer una longitud mínima de contraseña, historial de contraseñas y umbral de bloqueo después de varios intentos fallidos. También se recomienda utilizar cuentas individuales y evitar credenciales compartidas.

Meta: aplicar una política de contraseñas documentada que establezca requisitos mínimos de complejidad, longitud y bloqueo.

MK-05. Cuentas locales habilitadas sin actividad reciente

Se asignó probabilidad 2 e impacto 2, debido a que se encontraron cuentas habilitadas como Atalaya01 y luis cuyos últimos registros de acceso corresponden a 2024 y 2023 respectivamente. Aunque la evidencia no permite afirmar que estas cuentas sean innecesarias, su permanencia activa sin una justificación documentada incrementa la superficie de acceso del sistema. Riesgo: 4 (medio).

Recomendación: revisar periódicamente las cuentas locales y deshabilitar aquellas que ya no sean necesarias, conservando únicamente las cuentas justificadas para la operación.

Meta: mantener el 100 % de las cuentas activas asociadas a usuarios o funciones vigentes y documentadas.

MK-06. Múltiples herramientas de acceso remoto activas

Se asignó probabilidad 2 e impacto 2, debido a que en el servidor se encontraron activos AnyDesk, TeamViewer y RustDesk, además de otros componentes relacionados con conectividad. La utilización simultánea de diferentes herramientas de acceso remoto aumenta la superficie administrativa y dificulta determinar qué mecanismos deben permanecer autorizados. Riesgo: 4 (medio).

Recomendación: realizar un inventario de las herramientas de acceso remoto utilizadas, eliminar las que no sean necesarias y mantener únicamente aquellas autorizadas por la organización, con controles de autenticación y registro.

Meta: contar con un mecanismo de acceso remoto autorizado, documentado y controlado para las labores de soporte.

Diagnóstico de Sureca Ltda.

El diagnóstico técnico de Sureca Ltda. se realizó sobre una infraestructura compuesta por 17 equipos y un servidor, todos basados en Windows y ubicados en una única sede. La organización cuenta con firewall a nivel del servidor, utiliza mecanismos de acceso remoto y dispone de un esquema de copias de seguridad diarias con almacenamiento local y externo.

Resultados del análisis externo

El análisis externo realizado sobre la dirección pública, permitió identificar un puerto accesible desde Internet.

El puerto 8200/TCP se encontró abierto y Nmap lo identificó como un servicio relacionado con Hikvision IPCam. La prueba de vulnerabilidades también confirmó que el puerto permanecía accesible, aunque no identificó mediante ese script una vulnerabilidad específica.

El puerto 443 se encontró en estado filtered, por lo que no fue posible realizar una evaluación externa de los cifrados HTTPS.

Resultados de la evaluación interna

El servidor utiliza Windows Server 2022 Standard, compilación 20348. Sin embargo, las últimas actualizaciones registradas en la evidencia corresponden a marzo de 2022, incluyendo KB5010523, KB5011497 y KB5008882. Esto evidencia una brecha considerable entre la fecha de las últimas actualizaciones registradas y el momento en que se realizó el diagnóstico.

También se identificó que el servidor no cuenta con antivirus institucional, de acuerdo con la información suministrada. Aunque Windows Defender mantiene algunos servicios de seguridad activos, el levantamiento organizacional reporta ausencia de antivirus, por lo que se considera necesario fortalecer este control.

El Firewall de Windows se encuentra habilitado únicamente para el perfil de dominio, mientras que los perfiles privado y público aparecen deshabilitados. El servidor mantiene además diferentes servicios de red activos, entre ellos RDP, WinRM, SMB, Firebird y otros servicios propios de Windows.

Vulnerabilidades identificadas

Tabla 21. *Tabla de Vulnerabilidades encontradas Sureca*

<i>ID</i>	<i>Vulnerabilidad</i>	<i>Probabilidad</i>	<i>Impacto</i>	<i>Riesgo</i>	<i>Nivel</i>
SUR-01	Servicio de videovigilancia expuesto a Internet	3	3	9	Alto
SUR-02	Servidor sin actualizaciones recientes	3	3	9	Alto
SUR-03	Firebird 2.5 de 32 bits utilizado como motor de base de datos	3	3	9	Alto
SUR-04	Ausencia de antivirus institucional	3	3	9	Alto
SUR-05	Política de contraseñas insuficiente	3	3	9	Alto
SUR-06	Cuenta Invitado habilitada y con actividad reciente	3	2	6	Alto
SUR-07	Escritorio remoto habilitado	2	3	6	Alto

Fuente: Elaboración Propia

SUR-01. Servicio de videovigilancia expuesto a Internet

Se asignó probabilidad 3 e impacto 3, debido a que durante el análisis externo se identificó el puerto 8200/TCP abierto en la dirección pública de la organización, siendo identificado por Nmap como un servicio asociado a un sistema de videovigilancia Hikvision. Aunque la prueba realizada no identificó una vulnerabilidad específica, mantener este servicio accesible directamente desde Internet incrementa la superficie de ataque de la infraestructura. Riesgo: 9 (alto).

Recomendación: restringir el acceso al sistema de videovigilancia a la red interna o mediante un mecanismo de acceso remoto controlado, evitando la exposición directa del servicio hacia Internet.

Meta: eliminar la exposición directa del puerto 8200 y permitir el acceso únicamente desde redes o usuarios autorizados.

SUR-02. Servidor sin actualizaciones recientes

Se asignó probabilidad 3 e impacto 3, debido a que las últimas actualizaciones registradas en el servidor corresponden a marzo de 2022, a pesar de que el diagnóstico se realizó en septiembre de 2026. Esta diferencia evidencia una ausencia prolongada de actualización del sistema operativo y puede incrementar la exposición frente a vulnerabilidades de seguridad conocidas. Riesgo: 9 (alto).

Recomendación: establecer un proceso periódico de actualización del sistema operativo y verificar que las actualizaciones de seguridad se instalen de manera controlada.

Meta: mantener el servidor con las actualizaciones de seguridad vigentes y establecer una periodicidad documentada para su revisión.

SUR-03. Firebird 2.5 de 32 bits utilizado como motor de base de datos

Se asignó probabilidad 3 e impacto 3, debido a que el servidor utiliza Firebird 2.5 de 32 bits como motor de base de datos. Se trata de una tecnología antigua que forma parte de la infraestructura que soporta información operativa de la organización, por lo que mantenerla sin una estrategia de actualización o migración incrementa el riesgo tecnológico. Riesgo: 9 (alto).

Recomendación: evaluar la migración de la base de datos hacia una versión de Firebird con soporte vigente y compatible con las aplicaciones utilizadas por la organización. Si la migración inmediata no es posible, establecer medidas compensatorias y un plan de actualización.

Meta: disponer de un plan documentado de migración o actualización del motor de base de datos y reducir progresivamente la dependencia de Firebird 2.5.

SUR-04. Ausencia de antivirus institucional

Se asignó probabilidad 3 e impacto 3, debido a que la organización reportó que no cuenta con un antivirus institucional para proteger la infraestructura. Aunque existen servicios de seguridad de Windows activos, la ausencia de una solución de protección administrada dificulta establecer políticas centralizadas, monitoreo y respuesta frente a software malicioso. Riesgo: 9 (alto).

Recomendación: implementar una solución antivirus o EDR administrada centralmente y mantenerla actualizada.

Meta: proteger el 100 % de los equipos y servidores mediante una solución de seguridad activa, actualizada y administrada.

SUR-05. Política de contraseñas insuficiente

Se asignó probabilidad 3 e impacto 3, debido a que la política configurada establece una longitud mínima de contraseña de 0 caracteres, no mantiene historial de contraseñas y no establece un umbral de bloqueo por intentos fallidos. Estas condiciones reducen la protección de las cuentas frente a intentos de acceso no autorizado. Riesgo: 9 (alto).

Recomendación: establecer requisitos mínimos de longitud y complejidad, implementar historial de contraseñas y configurar un umbral de bloqueo ante múltiples intentos fallidos.

Meta: contar con una política de contraseñas formal que sea aplicada a todas las cuentas administrativas y de usuarios.

SUR-06. Cuenta Invitado habilitada y con actividad reciente

Se asignó probabilidad 3 e impacto 2, debido a que la cuenta Invitado se encuentra habilitada y registra un inicio de sesión el mismo día del diagnóstico. Las cuentas genéricas de invitado aumentan la dificultad para establecer trazabilidad individual sobre las acciones realizadas en el sistema. Riesgo: 6 (alto).

Recomendación: deshabilitar la cuenta Invitado si no existe una necesidad operativa justificada. En caso de requerirse una cuenta para una función específica, utilizar cuentas individuales con permisos definidos.

Meta: mantener deshabilitadas las cuentas genéricas que no sean necesarias y garantizar que los accesos puedan asociarse a usuarios identificables.

SUR-07. Escritorio remoto habilitado

Se asignó probabilidad 2 e impacto 3, debido a que la configuración del servidor confirma que el Escritorio remoto se encuentra habilitado mediante `fDenyTSConnections = 0`. Aunque RDP forma parte de los mecanismos utilizados por la organización, constituye una superficie adicional de acceso administrativo que debe mantenerse restringida y controlada. Riesgo: 6 (alto).

Recomendación: restringir el acceso RDP únicamente a usuarios autorizados y, preferiblemente, limitarlo a la red interna o a través de un mecanismo seguro de acceso remoto. También se recomienda implementar autenticación reforzada y registrar los accesos.

Meta: garantizar que el acceso RDP esté limitado exclusivamente a usuarios, equipos y redes autorizadas.

Diagnóstico de Indubolsas Contreras S.A.S.

El diagnóstico técnico de Indubolsas Contreras S.A.S. se realizó sobre una infraestructura compuesta por 23 equipos y un servidor, todos basados en Windows y ubicados en una única sede. La organización dispone de conexión a Internet mediante un router con firewall, utiliza mecanismos de acceso remoto y cuenta con sistemas de respaldo para la información.

El análisis externo se realizó sobre la dirección IP pública, mediante pruebas de reconocimiento de puertos, detección de servicios y búsqueda de vulnerabilidades conocidas utilizando Nmap. Los resultados no identificaron puertos TCP accesibles desde Internet dentro de los 1000 puertos evaluados. El puerto 443 también se encontró filtrado.

Resultados del análisis externo

El análisis externo sobre la IP pública, no identificó servicios accesibles desde Internet en los 1000 puertos TCP evaluados.

La prueba nmap -Pn -sV mostró los puertos analizados en estado filtered, mientras que la prueba mediante --script vuln tampoco obtuvo respuestas de servicios expuestos. La prueba específica sobre el puerto 443 igualmente mostró el estado filtered.

Resultados de la evaluación interna

El servidor utiliza Windows Server 2019 Standard, versión 1809, compilación 17763. A diferencia de otras empresas evaluadas, en este caso sí se encontraron actualizaciones de seguridad relativamente recientes, incluyendo actualizaciones instaladas en abril y mayo de 2026.

El firewall de Windows se encuentra habilitado para los perfiles Domain, Private y Public, lo cual constituye un control positivo.

Sin embargo, se identificó que el Escritorio remoto está habilitado, mediante `fDenyTSConnections = 0`, y que el servidor mantiene el puerto 3389/TCP en escucha. Dado que la organización reporta que utiliza RDP, no debe considerarse automáticamente una vulnerabilidad; el riesgo está relacionado con la necesidad de controlar y restringir este mecanismo de acceso.

Usuarios y cuentas

La revisión de usuarios constituye uno de los principales hallazgos de Indubolsas.

Se identificaron numerosas cuentas locales habilitadas, entre ellas:

- Almacen
- Archivo
- Asesor 1
- Asesor 2
- Asistente 1
- Asistente 2
- Auxiliar
- Comercial
- Contador
- Desarrollo
- Despachos
- Exportaciones
- Importaciones
- Inventario 1
- Inventario 2
- Nomina
- Operaciones

- Produccion
- Punto
- Revisor
- Tesoreria
- Ventas
- ventas2
- entre otras.

Algunas cuentas habilitadas presentan **últimos accesos de 2021, 2022, 2023 o 2024**, por ejemplo, Exportaciones, Inventario 2, Nomina, Operaciones, Revisor, Auxim y Desarrollo. Esto no demuestra que sean innecesarias, pero sí evidencia la necesidad de realizar una revisión periódica del ciclo de vida de las cuentas.

Vulnerabilidades identificadas

Tabla 22. *Vulnerabilidades Identificadas Indubolsas*

<i>ID</i>	<i>Vulnerabilidad</i>	<i>Probabilidad</i>	<i>Impacto</i>	<i>Riesgo</i>	<i>Nivel</i>
IND-01	Política de contraseñas insuficiente	3	3	9	Alto
IND-02	Cuenta Invitado habilitada y con actividad reciente	3	2	6	Alto
IND-03	Múltiples cuentas habilitadas sin actividad reciente	3	2	6	Alto
IND-04	Escritorio remoto habilitado	2	3	6	Alto
IND-05	Servicio MariaDB/MySQL accesible en todas las interfaces	2	3	6	Alto
IND-06	Alta cantidad de accesos remotos reportados	2	3	6	Alto

Fuente: Elaboración Propia

IND-01. Política de contraseñas insuficiente

Se asignó probabilidad 3 e impacto 3, debido a que la política de cuentas establece una longitud mínima de contraseña de 0 caracteres, no conserva historial de contraseñas y no establece un umbral de bloqueo ante intentos fallidos. Estas condiciones reducen la protección de las cuentas frente a intentos de acceso no autorizado. Riesgo: 9 (alto).

Recomendación: establecer una política de contraseñas que incluya longitud mínima, requisitos de complejidad, historial de contraseñas y bloqueo después de varios intentos fallidos.

Meta: aplicar una política de autenticación documentada y uniforme para las cuentas de los usuarios y administradores.

IND-02. Cuenta Invitado habilitada y con actividad reciente

Se asignó probabilidad 3 e impacto 2, debido a que la cuenta invitado se encuentra habilitada y registra actividad durante el mismo periodo en que se realizó el diagnóstico. Las cuentas genéricas dificultan la identificación individual de las acciones realizadas y pueden facilitar accesos que no puedan asociarse claramente con una persona. Riesgo: 6 (alto).

Recomendación: deshabilitar la cuenta Invitado y utilizar cuentas individuales para los usuarios que necesiten acceder al servidor.

Meta: mantener deshabilitadas las cuentas genéricas que no sean indispensables y garantizar trazabilidad individual de los accesos.

IND-03. Múltiples cuentas habilitadas sin actividad reciente

Se asignó probabilidad 3 e impacto 2, debido a que se identificaron numerosas cuentas habilitadas cuyos últimos accesos corresponden a períodos anteriores, incluyendo algunas con actividad registrada desde 2021, 2022, 2023 y 2024. Aunque no se puede concluir únicamente con este dato que las cuentas sean innecesarias, mantenerlas habilitadas sin una revisión documentada incrementa la superficie de acceso. Riesgo: 6 (alto).

Recomendación: realizar una revisión periódica de todas las cuentas, verificando que cada una corresponda a un trabajador, cargo o función vigente. Las cuentas que ya no sean necesarias deben ser deshabilitadas.

Meta: lograr que el 100 % de las cuentas habilitadas tengan un responsable y una función operativa vigente.

IND-04. Escritorio remoto habilitado

Se asignó probabilidad 2 e impacto 3, debido a que el servidor mantiene habilitado el Escritorio remoto (`fDenyTSConnections = 0`) y el puerto 3389 se encuentra en escucha. Aunque RDP es utilizado por la organización, representa una superficie de acceso administrativo que debe permanecer restringida. Riesgo: 6 (alto).

Recomendación: limitar RDP exclusivamente a usuarios autorizados y, cuando sea posible, restringir su acceso a la red interna o a través de mecanismos seguros de acceso remoto.

Meta: garantizar que ningún acceso RDP pueda realizarse desde redes o usuarios no autorizados.

IND-05. Servicio MariaDB/MySQL accesible en todas las interfaces

Se asignó probabilidad 2 e impacto 3, debido a que el servicio MySQL/MariaDB se encuentra escuchando en el puerto 3306 sobre todas las interfaces de red, en lugar de limitarse únicamente a localhost o a las interfaces requeridas por las aplicaciones autorizadas.

Esta configuración puede ampliar innecesariamente la superficie de acceso al motor de base de datos dentro de la red. Riesgo: 6 (alto).

Recomendación: restringir el parámetro bind-address a las interfaces necesarias y controlar mediante firewall qué equipos pueden establecer conexiones con el puerto 3306.

Meta: permitir conexiones al motor de base de datos únicamente desde los servidores o aplicaciones autorizados.

IND-06. Alta cantidad de accesos remotos reportados

Se asignó probabilidad 2 e impacto 3, debido a que la organización reporta 42 accesos remotos, cifra considerable frente a los 23 equipos que conforman la infraestructura evaluada. Una cantidad elevada de accesos incrementa la necesidad de controlar usuarios, permisos, autenticación y trazabilidad. Riesgo: 6 (alto).

Recomendación: realizar un inventario de los accesos remotos existentes, identificar a cada usuario autorizado, revisar periódicamente sus permisos y retirar aquellos accesos que ya no sean necesarios.

Meta: mantener únicamente accesos remotos asociados a usuarios y funciones vigentes, con autorización y registro.

Análisis comparativo de las empresas evaluadas

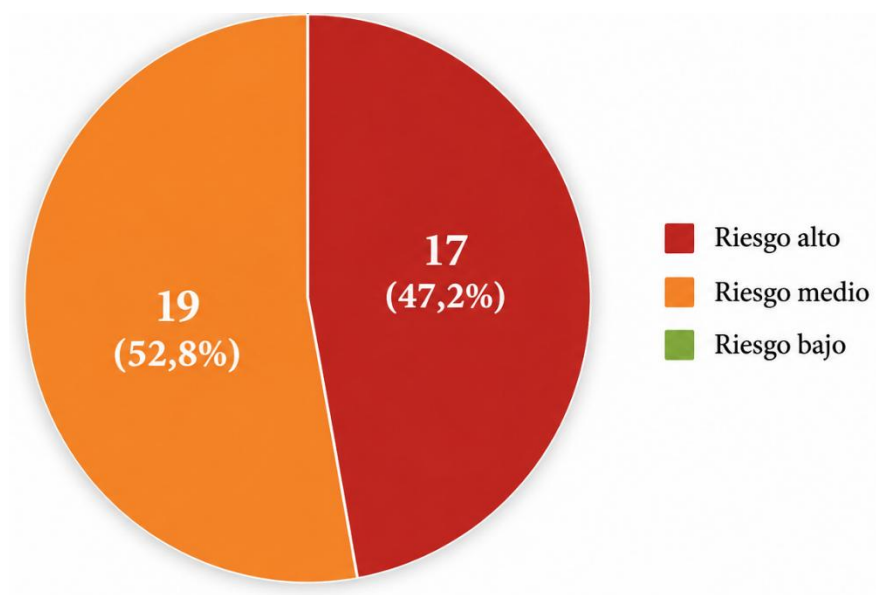
Comparación de vulnerabilidades por nivel de riesgo

Tabla 23. Resumen de vulnerabilidades de las 6 empresas evaluadas

Empresa	Riesgo alto	Riesgo medio	Riesgo bajo
Uronorte S.A.	2	4	0
Help Trauma IPS SAS	3	3	0
Sociedad Médica Los Samanes SAS	3	2	0
MK Insumos Inc. SAS	3	3	0
Sureca Ltda.	5	2	0
Indubolsas Contreras SAS	1	5	0

Fuente: Elaboración Propia

Figura 1. Distribución de vulnerabilidades por nivel de riesgo



Fuente: elaboración propia a partir de los resultados del diagnóstico técnico.

Análisis comparativo de las empresas evaluadas

La comparación de los diagnósticos permitió identificar 36 vulnerabilidades entre las seis empresas evaluadas, de las cuales 17 fueron clasificadas como de riesgo alto y 19 como de riesgo medio, sin hallazgos de riesgo bajo. Se observaron diferencias en la naturaleza de las condiciones encontradas: mientras Uronorte S.A. presentó principalmente situaciones asociadas con servicios expuestos y componentes desactualizados, Help Trauma IPS SAS concentró sus hallazgos en cuentas, contraseñas, protección de equipos y accesos remotos; Sociedad Médica Los Samanes SAS presentó condiciones relacionadas con obsolescencia tecnológica, ausencia de antivirus y respaldos; y MK Insumos Inc. SAS mostró debilidades relacionadas con sistemas fuera de soporte, firewall, contraseñas y mecanismos de acceso remoto.

Por su parte, Sureca Ltda. registró la mayor cantidad de hallazgos, con 7 vulnerabilidades, 5 de ellas de riesgo alto, relacionadas principalmente con actualización del servidor, servicios expuestos, software antiguo, protección antimalware y controles de acceso. Indubolsas Contreras SAS presentó 6 vulnerabilidades, pero con una distribución de 1 riesgo alto y 5 medios, evidenciando que la cantidad de hallazgos no representa por sí sola el nivel de exposición. De manera transversal, se identificaron situaciones recurrentes relacionadas con políticas de contraseñas, gestión de cuentas, accesos remotos, actualización de sistemas y mecanismos de protección, lo que demuestra la necesidad de fortalecer tanto los controles técnicos como los procesos de administración de la seguridad. En las IPS, estas condiciones adquieren especial importancia debido a la información clínica y personal que manejan.

Conclusiones

El diagnóstico técnico realizado permitió identificar y analizar las principales vulnerabilidades de ciberseguridad presentes en seis empresas asesoradas por Prof&Tech, encontrando un total de 36 hallazgos. La aplicación de una metodología común basada en la identificación de activos, revisión técnica, valoración de probabilidad e impacto y clasificación del riesgo permitió establecer un punto de comparación entre las organizaciones, manteniendo en consideración las características particulares de cada una.

Los resultados evidenciaron que 17 de las 36 vulnerabilidades identificadas fueron clasificadas como de riesgo alto y 19 como de riesgo medio, sin registrarse hallazgos de riesgo bajo. Esto demuestra que las condiciones encontradas no se limitan a aspectos tecnológicos específicos, sino que también involucran elementos relacionados con la administración de usuarios, políticas de contraseñas, acceso remoto, actualización de sistemas, protección contra malware, respaldos y configuración de servicios.

El análisis comparativo permitió identificar que las vulnerabilidades no dependen exclusivamente del tamaño de la infraestructura tecnológica. Uronorte, por ejemplo, cuenta con una infraestructura más amplia y diferentes mecanismos de protección, pero presenta vulnerabilidades relacionadas con servicios expuestos y componentes desactualizados. Por otra parte, organizaciones con infraestructuras más pequeñas presentan necesidades asociadas con controles básicos como antivirus, respaldos, actualización de sistemas y protección de la red. Esto evidencia la importancia de evaluar la seguridad de acuerdo con las condiciones reales de cada organización.

En las IPS evaluadas se identificó además la necesidad de considerar la protección de la información clínica dentro del análisis de ciberseguridad. Las condiciones relacionadas con cuentas, contraseñas, malware, respaldos, sistemas obsoletos y disponibilidad de los servicios pueden afectar no solamente los equipos tecnológicos, sino

también la confidencialidad, integridad, disponibilidad y trazabilidad de la información utilizada en los procesos de atención y gestión.

Referencias

Congreso de Colombia. (2009). *Ley 1273 de 2009: Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado denominado “de la protección de la información y de los datos”....* SUIN-Juriscol. <https://www.suin-juriscol.gov.co/viewDocument.asp?id=1676699>

Congreso de Colombia. (2012). *Ley 1581 de 2012: Por la cual se dictan disposiciones generales para la protección de datos personales.* SUIN-Juriscol. <https://www.suin-juriscol.gov.co/clp/contenidos.dll/Leyes/1684507>

Congreso de Colombia. (2020). *Ley 2015 de 2020: Por medio de la cual se crea la Historia Clínica Electrónica interoperable y se dictan otras disposiciones.* SUIN-Juriscol. <https://www.suin-juriscol.gov.co/viewDocument.asp?ruta=Leyes%2F30038770>

Departamento Nacional de Planeación. (2011). *Documento CONPES 3701: Lineamientos de política para ciberseguridad y ciberdefensa.* Consejo Nacional de Política Económica y Social.

Departamento Nacional de Planeación. (2016). *Documento CONPES 3854: Política nacional de seguridad digital.* Consejo Nacional de Política Económica y Social.

Departamento Nacional de Planeación. (2020). *Documento CONPES 3995: Política nacional de confianza y seguridad digital.* Consejo Nacional de Política Económica y Social.

Joint Task Force Transformation Initiative. (2012). *Guide for conducting risk assessments* (NIST Special Publication 800-30 Rev. 1). National Institute of Standards and Technology. <https://doi.org/10.6028/NIST.SP.800-30r1>

Lyon, G. (2022). *Nmap network scanning: The official Nmap project guide to network discovery and security scanning.* Nmap Project. <https://nmap.org/book/>

MariaDB. (2025). *MariaDB Server: All releases*. <https://mariadb.org/mariadb/all-releases>

Microsoft. (2025). *Windows 10 support has ended on October 14, 2025*. Microsoft Support. <https://support.microsoft.com/en-us/windows/deployment/updates-lifecycle/windows-10-support-has-ended-on-october-14-2025>

Ministerio de Salud. (1999). *Resolución 1995 de 1999, por la cual se establecen normas para el manejo de la historia clínica*.

Ministerio de Salud y Protección Social. (2021). *Resolución 866 de 2021, por la cual se reglamenta el conjunto de elementos de datos clínicos relevantes para la interoperabilidad de la historia clínica en el país y se dictan otras disposiciones*. SUIN-Juriscol. <https://www.suin-juriscol.gov.co/viewDocument.asp?id=30042299>

Ministerio de Salud y Protección Social. (2025). *Resolución 1888 de 2025, por medio de la cual se adopta el Resumen Digital de Atención en Salud (RDA) en el marco de la Interoperabilidad de la Historia Clínica Electrónica (IHCE), se establece el mecanismo para su implementación a nivel nacional y se dictan otras disposiciones*. SUIN-Juriscol. <https://www.suin-juriscol.gov.co/clp/contenidos.dll/Resolucion/30055569>

National Institute of Standards and Technology. (s. f.-a). *Cybersecurity*. NIST Computer Security Resource Center. <https://csrc.nist.gov/glossary/term/cybersecurity>

National Institute of Standards and Technology. (s. f.-b). *Asset*. NIST Computer Security Resource Center. <https://csrc.nist.gov/glossary/term/asset>

National Institute of Standards and Technology. (s. f.-c). *Risk*. NIST Computer Security Resource Center. <https://csrc.nist.gov/glossary/term/risk>

National Institute of Standards and Technology. (s. f.-d). *Threat*. NIST Computer Security Resource Center. <https://csrc.nist.gov/glossary/term/threat>

National Institute of Standards and Technology. (s. f.-e). *Vulnerability*. NIST Computer Security Resource Center. <https://csrc.nist.gov/glossary/term/vulnerability>

Python Software Foundation. (2026). *Python release Python 3.10.21*. Python.org. <https://www.python.org/downloads/release/python-31021/>

Scarfone, K., Souppaya, M., Cody, A., & Orebaugh, A. (2008). *Technical guide to information security testing and assessment* (NIST Special Publication 800-115).

National Institute of Standards and Technology. <https://doi.org/10.6028/NIST.SP.800-115>

CONSTANCIA DE AUTORIZACIÓN, PARTICIPACIÓN Y RECEPCIÓN DEL DIAGNÓSTICO TÉCNICO DE CIBERSEGURIDAD

21 de septiembre de 2026, San Jose de Cúcuta

Señores:

Prof&tech S.A.S.
Nit: 901.891.690-2

Asunto: Constancia de autorización, participación y recepción del diagnóstico técnico de ciberseguridad

Por medio de la presente **Prof&tech S.A.S.**, identificada con NIT **901.891.690-2**, deja constancia de que autorizó y permitió la realización de actividades de diagnóstico técnico relacionadas con la seguridad de la información y la ciberseguridad, desarrolladas en el marco del trabajo de grado titulado:

“ANÁLISIS DE VULNERABILIDADES EN CIBERSEGURIDAD DE SEIS EMPRESAS ASESORADAS POR PROFYTECH MEDIANTE UN DIAGNÓSTICO TÉCNICO”

desarrollado por el estudiante **Maikol Serrano Oviedo** y del programa de **Ingeniería de Sistemas de la Corporación Universitaria Remington**.

Durante el desarrollo de las actividades se realizaron procedimientos técnicos orientados a la **identificación de posibles vulnerabilidades, condiciones de riesgo y aspectos relacionados con la seguridad de los sistemas de información y la infraestructura tecnológica** de la organización, de acuerdo con el alcance previamente establecido.

Como resultado de estas actividades, la empresa manifiesta que:

1. **Autorizó la realización de las actividades de diagnóstico técnico** dentro del alcance acordado y sobre los recursos tecnológicos definidos para tal propósito.
2. **Participó y/o facilitó la información necesaria** para el desarrollo de las actividades contempladas dentro del diagnóstico, de acuerdo con las posibilidades y condiciones de la organización.
3. **Recibió los resultados obtenidos durante el diagnóstico**, incluyendo la identificación de las condiciones de seguridad observadas y las recomendaciones propuestas para el fortalecimiento de la postura de ciberseguridad de la organización.
4. **Deja constancia de haber sido informada sobre los resultados del diagnóstico**, entendiendo que estos corresponden a las condiciones observadas durante el período y bajo el alcance en que fueron realizadas las actividades.

5. Entiende que los resultados corresponden a un **diagnóstico técnico de carácter académico** y no constituyen una certificación de seguridad, auditoría integral, certificación de cumplimiento normativo ni garantía de ausencia de vulnerabilidades en la infraestructura tecnológica.
6. Autoriza que la información obtenida durante el desarrollo del trabajo sea utilizada **exclusivamente con fines académicos y de investigación**, conservando la confidencialidad de la información sensible de la organización y evitando la divulgación de datos que permitan comprometer su seguridad.

La presente constancia se expide como evidencia de la **autorización, participación y recepción de los resultados del diagnóstico técnico realizado**, para los fines académicos relacionados con el trabajo de grado anteriormente mencionado.

En constancia de lo anterior, se firma en Cúcuta, a los 21 **días del mes de septiembre de 2026**.



Gerson Daniel Palencia Chiquillo
C.C.: 88222282
Representante legal