ESTUDIO DE VULNERABILIDADES, AMENAZAS Y GESTIÓN DEL RIESGOS EN EL HOSPITAL DEPARTAMENTAL PSIQUIÁTRICO UNIVERSITARIO DEL VALLE E.S.E

ANYHELA GAMBOA CASTILLO
EDWIN RUANO GAMBOA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA (ECBTI)
CALI, COLOMBIA
2019

ESTUDIO DE VULNERABILIDADES, AMENAZAS Y GESTIÓN DEL RIESGOS EN EL HOSPITAL DEPARTAMENTAL PSIQUIÁTRICO UNIVERSITARIO DEL VALLE E.S.E

ANYHELA GAMBOA CASTILLO
EDWIN RUANO GAMBOA

TRABAJO DE PRESENTADA(O) COMO REQUISITO PARCIAL PARA OPTAR AL TÍTULO DE:

ESPECIALISTA EN SEGURIDAD INFORMÁTICA

DIRECTOR:

ESP. DANIEL FELIPE PALOMO LUNA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA (ECBTI)
CALI, COLOMBIA

2020

Nota de Aceptación:

_____

_____

_____

_____

_____

_____

_____

Firma del presidente del jurado

_____

Firma del jurado

_____

Firma del jurado

CONTENIDO

pág.

LISTA DE ILUSTRACIONES

pág.

LISTA DE TABLAS

pág.

RESUMEN

En el Hospital Departamental Psiquiátrico Universitario del Valle, la información es administrada de una forma descentralizada, puesto que para el cargue proceso y generación de información se utilizan varios sistemas de información que no cuentan con interfaces automáticas, lo que dificulta la consolidación de la misma, por lo que es necesario usar herramientas adicionales para la integración de datos, adicionalmente los procesos para la gestión de la seguridad de Información son limitados y la infraestructura tecnológica (Redes de datos) es obsoleta. Por lo que se hace necesario realizar un análisis situacional de la Institución teniendo en cuenta tres pilares fundamentales para la Entidad, como son:

- INFRAESTRUCTURA TECNOLOGICA: Entiéndase por infraestructura tecnológica los componentes de *Hardware, software* y Redes de datos.

- SISTEMAS DE INFORMACIÓN: Son las herramientas para el procesamiento de la Información Institucional.

- SEGURIDAD DE LA INFORMACIÓN: Proceso orientado a proteger toda la información de una Institución, independiente del modo de creación, procesamiento, almacenamiento, si es física o digital.

Este análisis permitirá proponer la implementación de estrategias para la Gestión de TI (Tecnologías de Información), utilizando marcos de referencia como COBIT, ITIL e ISO 27001, al igual que implementar los lineamientos establecidos por el gobierno “Gobierno Digital”, logrando identificar riesgos, vulnerabilidades y amenazas, para establecer los controles necesarios a implementar en la Institución.

INTRODUCCIÓN

El siglo XXI ha sido denominado como la nueva era de la información y el conocimiento digital, gracias a la acción transversal de las TI (Tecnologías de Información), los sistemas de Información se pueden aprovechar y desarrollar en diferentes nichos de mercado, optimizando los procesos y tiempos generando las soluciones requeridas para cada sector. Dichos sistemas mejoran la competitividad y desempeña una función clave al permitir la reestructuración y modernización empresarial. La modernización de la industria va de la mano con grandes desafíos institucionales, abriendo las puertas a nuevos mercados, a aumentarla productividad y competitividad, adaptarse a nuevas estrategias de comercialización y sobre todo competir con base en la calidad de los productos y servicios. El sector de las TIC´s requiere de un alto nivel de investigación, desarrollo tecnológico y formación de personas capaces de producir soluciones acordes con las necesidades que surgen en la actual coyuntura, necesidades que al ser atendidas eficientemente puede impactar de manera positiva a las organizaciones modernas. El HOSPITAL DEPARTAMENTAL PSIQUIATRICO UNIVERSITARIO DE VALLE E.S.E., conocedor de estas necesidades está dispuesto a realizar las valoraciones necesarias que permitan apalancar el mejoramiento de su productividad y de su eficiencia corporativa. La información como variable estratégica de la organización, debe estar actualizada soportada en las herramientas necesarias para realizar el análisis estratégico, que le permita a la gerencia tomar decisiones.

En el Hospital Departamental Psiquiátrico Universitario del Valle, el proceso de administración de la información dificulta la consolidación de la misma, por lo que es necesario en ocasiones utilizar herramientas como hojas de cálculo (Excel) para la integración de datos, adicionalmente los procesos para la gestión de la seguridad de Información son limitados y la infraestructura tecnológica (Redes de datos) es obsoleta.

Palabras clave: (Amenazas, gestión del riesgo, riesgos, seguridad informática, vulnerabilidades**).**

1. DEFINICIÓN DEL PROBLEMA

Los riesgos informáticos constituyen uno de los factores más preocupantes en seguridad de la información de las Instituciones, por lo tanto se hace necesario realizar un estudio donde se pueda evidenciar las vulnerabilidades, amenazas y riesgos en el Hospital Departamental Psiquiátrico Universitario del Valle E.S.E., y poder establecer como una gestión del riesgo informático contribuye a mejorar la productividad y eficiencia corporativa con el fin de alinearse con los principios estratégicos de la Organización.

Con base en lo anterior se plantea el siguiente interrogante:

¿Cómo el Estudio de vulnerabilidades, amenazas y gestión del Riesgos en el Hospital Departamental Psiquiátrico Universitario del Valle E.S.E contribuye a mejorar la productividad y eficiencia corporativa, alineados con los principios estratégicos?

2. JUSTIFICACIÓN

Los riesgos forman parte de la naturaleza del ser humano y están presente en todas sus actividades, más aún cuando la tendencia al uso de la tecnología como factor de desarrollo e innovación, mejora las condiciones de vida minimizando lo que se considera el riesgo asociado al factor humano, pero asumiendo nuevos riesgos derivados de la tecnología y su dependencia.

Es por ello por lo que, de la mano de los avances tecnológicos, vienen también los avances en riesgos informáticos, el auge de nuevas tecnologías lleva al cambio de los procesos empresariales adaptados a estas nuevas herramientas, como son software, sistemas de información y nuevas formas de comunicación.

Adicional el Hospital Departamental Psiquiátrico Universitario del Valle, como entidad de salud debe regirse por la normatividad frente al uso y custodia de la Historia Clínica de sus pacientes, garantizando la integridad y el uso adecuado de esta información al considerarse altamente confidencial, el uso de historia clínica sistematizada brinda una gran herramienta para el registro y consolidación de información, pero igualmente genera un factor de riesgo tecnológico a tener en cuenta en la custodia de esta información, igualmente se debe garantizar la confidencialidad, integridad y disponibilidad de toda la información empresarial, comercial y clínica de la Institución.

La tecnología no es ajena a los riesgos y en este escenario es importante identificar los eventos, vulnerabilidades y amenazas que puedan poner en riesgo los activos de información comprometiendo la operación, imagen y credibilidad de la institución. Es por esto por lo que se busca implementar estrategias que puedan mitigar la confidencialidad, integridad y disponibilidad de la información.

3. OBJETIVO GENERAL

Realizar un estudio de vulnerabilidades, amenazas y gestión del Riesgo en el Hospital Departamental Psiquiátrico Universitario del Valle E.S.E, para minimizar el impacto provocado por la materialización de riesgos asociados a los activos de información.

3.1 OBJETIVOS ESPECÍFICOS

- Identificar los riesgos, amenazas y vulnerabilidades del Hospital Departamental Psiquiátrico Universitario del Valle.
- Realizar un estudio de la gestión del Riesgo en el Hospital Departamental Psiquiátrico Universitario del Valle.
- Proponer políticas y estrategias que logren mitigar ese riesgo.
- Reducir el impacto de las amenazas
- Implementar y evaluar la gestión de seguridad Informática en la Institución

4. MARCO REFERENCIAL

4.1 ANTECEDENTES

La seguridad informática constituye un marco importante en el alcance de los Objetivos Institucionales, al proteger la integridad, disponibilidad y confidencialidad de los datos del Hospital Departamental Psiquiátrico Universitario del Valle, identificar los posibles riesgos y amenazas a los que se puede ver expuesta brinda garantías de protección y mecanismos de prevención.

Para el desarrollo de este proyecto se toma como referente las anteriores investigaciones:

- Metodología de análisis y evaluación de riesgos aplicados a la seguridad informática y de información bajo la norma ISO/IEC 27001 - Francisco Nicolás Solarte Solarte, Edgar Rodrigo Enriquez Rosero, Mirian del Carmen Benavides. Este artículo define el desarrollo de estrategias y habilidades con el fin de llevar a cabo diagnósticos que permitan la implementación de proyectos de gestión de seguridad de la información SGSI, de acuerdo con el estándar ISO/IEC 27001 e ISO/IEC 27002.

- Análisis de riesgos en seguridad de la información, Ana del Carmen Abril Estupiñan, Jarol Alexander Pulido, John Alexander Bohada Jaime, Fundación Universitaria Juan de Castellanos. Este artículo se enfoca en exponer algunas opciones y permitir generar argumentos sólidos para identificar cuál es la metodología de análisis de riesgos que proporciona una mejor oportunidad de toma de decisiones dentro de una organización frente a la custodia de la información, la cual se ha convertido en uno de los activos más importantes del

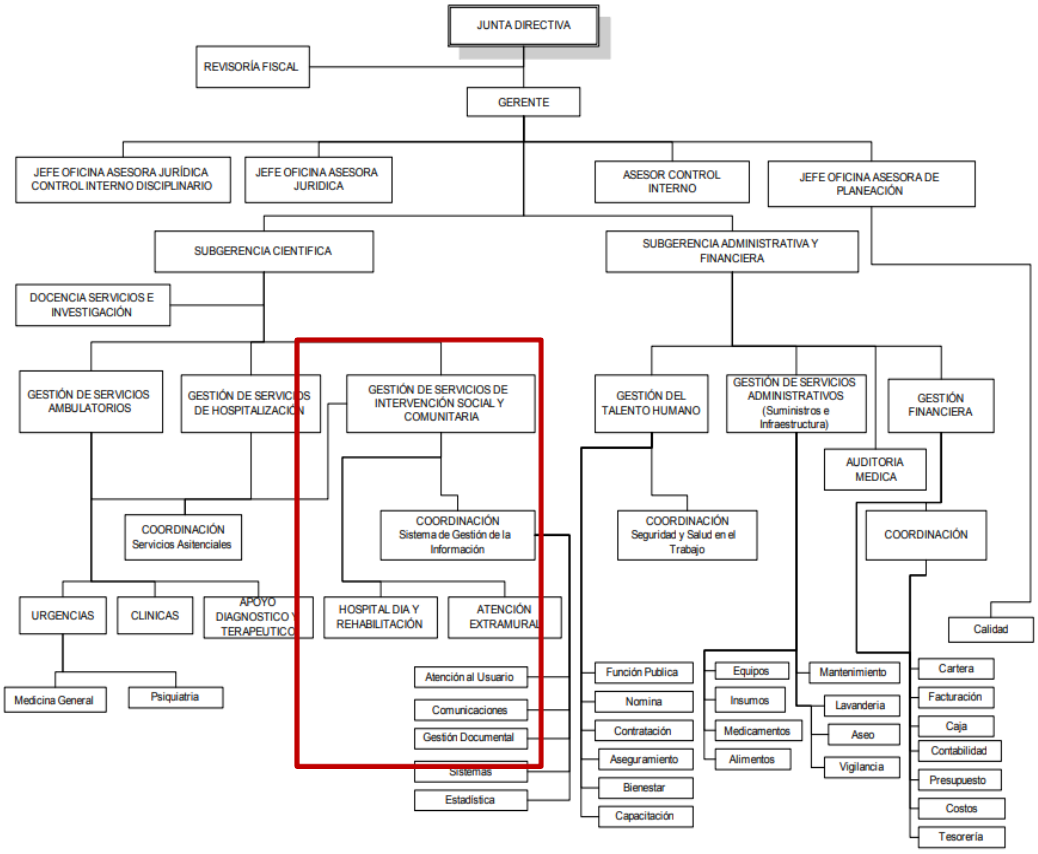
ámbito empresarial e implica una adecuada utilización y preservación para garantizar la seguridad y la continuidad del negocio.

- Metodología para la Implementación de la Gestión Automatizada de Controles de Seguridad Informática, Michel Miranda Cairo, Osmany Valdés Puga, Iván Pérez Mallea, RenierPortelles Cobas, Raúl Sánchez Zequeira. Este trabajo presenta una metodología basada en la integración de varios modelos, normas,herramientas y buenas prácticas para la implementación de la gestión automatizada de controles de seguridad informática, combinando varios métodos orientados a la gestión de riesgos con un enfoque de automatización durante las etapas de operación, monitorización y revisión de un Sistema de Gestión de Seguridad de la Información.

4.2 MARCO CONTEXTUAL

Dentro de la estructura organizacional el proceso de gestión de la información no tiene una incidencia directa en la planeación estratégica, puesto que depende de un proceso asistencial liderado por un profesional en enfermería y coordinado por un perfil estadístico epidemiólogo, el cual se encuentra en vacancia definitiva. En la figura 1 se observa la estructura organizacional de la entidad, donde se evidencia lo expuesto anteriormente:

Ilustración 1 - Estructura Organizacional



Fuente: Plataforma documental Hospital Departamental Psiquiátrico Universitario del Valle

La gestión de servicios tecnológicos se encuentra centralizada por el área de sistemas donde se tramitan y se da seguimiento a las solicitudes con usuarios, proveedores y terceros, así como también se hace levantamiento de información de necesidades tecnológicas, las cuales sirven como insumo para la elaboración de los planes anuales de inversión. El Hospital cuenta con una herramienta para la gestión de requerimientos de TI, donde se registra toda la información de requerimientos, incidentes, problemas y su respectiva gestión.

Para realizar el proceso de mantenimiento preventivo y correctivo a la infraestructura tecnológica se contrata una empresa proveedora de servicios de mantenimiento, la cual es supervisada por el área de sistemas de información.

Se puede decir que se han adelantado algunos procesos de sensibilización y capacitaciones, que tienen en cuenta el componente tecnológico, se hace necesario establecer medidas del impacto cuantitativo y/o cualitativo mediante instrumentos que permitan valorar el nivel de aceptación de la tecnología al interior de la Entidad.

SISTEMAS DE INFORMACIÓN

De acuerdo con lo dispuesto en el modelo de gestión de TI propuesto por MinTIC los sistemas de información se dividen en: apoyo, misionales y de direccionamiento estratégico. Teniendo en cuenta lo anterior, en el Hospital Departamental Psiquiátrico Universitario del Valle se tendría la siguiente categorización:

Sistemas de apoyo:

- ERP SIESA ENTERPRISE.
- DINÁMICA GERENCIAL DGH 9.0 – Administrativo (Financiero, comercial)
- CGUNO 5.0
- CGUNO 7.2

Sistemas Misionales de Gestión

- DINÁMICA GERENCIAL DGH.NET – Asistencial (Historia Clínica)
- SERVICIOS DE INFORMACIÓN DIGITAL, INCLUIDOS LOS PORTALES: PÁGINA WEB.

Tabla1. Software Institucional

Servicio	Descripción
ERP Siesa Enterprise	Se procesa información administrativa y financiera
Dinámica Gerencial	Se procesa información administrativa, facturación e
DGH 9.0	inventarios hospitalarios
CGUNO 5.0	Sistema histórico de información contable
CGUNO 7.2	Sistema histórico de información de inventarios
DGH .NET	Se procesa información de historia clínica, citas medicas
SQL Server 2005	Motor de base de datos asistencial
SQL Server 2012	Motor de base de datos administrativo y financiero
Outlook	Herramienta de correo electrónico
Paquete Office	Paquete de herramientas ofimáticas
Sitio Web	Página web institucional
Gestión de requerimientos TI	Herramienta para gestión de requerimientos de TI

Fuente: Manual de Recursos Informáticos del HDPUV

Para la Institución este dominio representa una debilidad dado el número de sistemas de información y en cada uno de ellos se debe brindar un soporte técnico, brindando de manera manual la comunicación entre cada uno de ellos, lo que genera reprocesos administrativos.

Administración de sistemas de información:

Para la gestión de los sistemas de información en El Hospital Departamental Psiquiátrico Universitario del Valle ESE la Entidad cuenta con ambientes de:

- Desarrollo
- Pruebas
- Producción.

Ambiente de Desarrollo

La Institución no realiza procesos de desarrollo, sin embargo, en este ambiente se comprende el entorno de interfaz y conexión de la información entre diferentes aplicativos, herramientas, reportes e informes. A este ambiente, puede acceder solo personal previamente autorizado y tienen los privilegios para crear, modificar y eliminar los componentes que componen o compondrán el sistema; se debe restringir los accesos a los usuarios finales o cualquier otro usuario diferente al equipo de desarrollo.

El desarrollo de esta práctica se aplica para los servidores y repositorios de datos

Ambiente de Pruebas:

Este ambiente es usado para la realización de pruebas del sistema, cada que se desarrolle una nueva función, con el fin de ser probada por los usuarios finales, este es un paso previo a la actualización en ambiente de producción.

Previo a la actualización en ambiente de producción, se debe realizar las validaciones por parte del equipo de *testing* y desarrollo a fin de identificar errores tanto estructurales, funcionales y el manejo d excepciones.

Para la correcta aplicación del entorno de pruebas se debe realizar con casos reales, con el fin de acercarse lo más posible a la realidad a la cual se va a enfrentar el aplicativo, a fin de garantizar el desarrollo y la configuración más óptima, además de poder detectar el mayor número de incidentes antes del momento de despliegue en producción

Se recomienda definir múltiples ambientes de pruebas, para evaluar y determinar el comportamiento de una funcionalidad en diferentes escenarios, este ambiente de pruebas se compone del repositorio de datos reales, datos de pruebas y los componentes a evaluar del software.

Ambiente de Producción:

Este ambiente de producción es donde se despliega las nuevas funcionalidades del software a ejecutar, previa evaluación en el ambiente de pruebas, con un resultado satisfactorio, que se debe formalizar por el representante de la fase y así poder desplegar en producción a fin de ser usadas por los usuarios finales.

Para realizar el despliegue en producción de los componentes compilados o ejecutables se tomarán las versiones probadas y aceptadas del ambiente de pruebas.

El Grupo de Trabajo de Infraestructura y Servicios de TI, es el responsable de la administración de la aplicación o el sistema en este ambiente.

Infraestructura:

La infraestructura informática es la base fundamental de todo sistema de información basado en ambiente cliente servidor, por medio de la cual un computador se puede conectar con otro, compartir información y ejecutar aplicativos centralizados desde un servidor de datos. A continuación, se detalla la infraestructura tecnológica dispuesta por el HDPUV y descrita en tres grupos (Servidores, Redes y Telefonía).

Servidores

Estos componentes se entienden como el hardware y el software que soporta los sistemas de información (misionales y de apoyo), las bases de datos y los servicios de red, los cuales se encuentran distribuidos como servidores físicos y virtuales, unidades de almacenamiento de información y dispositivos de *Backups*.

Tabla 2– Servidores

Equipo	Aplicativo	Especificaciones
Servidor HP Proliant 370	Servicios DC, DNS y DCHRP	Doble procesador Intel Xeon 2mb de cache. 3.6 GHz , 8000 Mhz F SB con EM64T, 4 GB memoria DDR - Dos discos duros de 72 Gb en Raid 0 (SC SI) - 3 Discos duros de 146 GB, en raid 5 (SC SI) - Alimentación y refrigeración redundante.
Servidor espejo HP Proliant BL460C G5 Server Blade	SQL Server 2005, Dinámica Gerencial Hospitalaria, CGUno 7.0 Cguno 5.0	Doble procesador Intel Xeoncuad 12mb de cache. 3.0 GHz , 1333 Mhz F SB con EM64T, 10 GB memoria DDR - 2 discos duros de 72 Gb en Raid 0 (SC SI) - 4 Discos duros de 146 GB, en raid 5 (SC SI) .Alimentación y refrigeración redundante
HP Proliant BL460C G5 Server Blade	SQl 2012, Siesa Enterprise	HP Proliant BL460c Gen 8 - servidor compacto 2 vias 1 Xeon E52640V2 / 2 Ghz - Ram 32GB - SaS - Hot - Swap 2.5 - Memoria cache de 20 MB, controlador de almacenamiento SAS - 2 (SAS de 6 GB / 2).
HP Proliant DL 380 G9	Servidor de virtualización	Servidor DL 380 Factor de forma: Rack Mount (2U) - Procesador 1xIntel Xeon E5-2640v4 10-Core (2.40Ghz 25 MB L3 cache) Kit -Max. 2 Proce Memoria Ram 32 GB (2x16) DDR4 24000MHz RDIMM - Total ranuras 12 Red HP Embedded 1GB Ethernet 4 port 331i adapter - Almacenamiento en disco: 3 DD de 600 GB
HP Prodesk 400	Servidor de pruebas	Intel core I7 - 6700 8 GB (1x 8 gb) DDR -2133 MHZ 1 TB 7200 RPM

Fuente: Manual de uso de los Recursos Informáticos del HDPUV

Redes

Actualmente el Hospital cuenta con una infraestructura de red LAN basada en tecnología Ethernet 10/100/1000, interconectada en topología tipo estrella, utilizando cable UTP categoría 5e y 6, bajo la norma estándar IEEE 568b. También se cuenta con una conexión de fibra óptica tipo multimodo, para enlazar áreas del hospital alejadas como son las salas de Hospitalización y la casona San Isidro. La central de cableado está ubicada en el primer piso del área administrativa del Hospital, y está administrada por equipos de conmutación de alta velocidad como *Switches* de Red capa 2 y 3, los cuales están apilados para poder administrar la transmisión de datos de todos los puntos conectados.

La red de datos del Hospital está conformada por 186 equipos de cómputo, configurados con sistema operativo Windows de Microsoft, administrados por un servidor de dominio con sistema operativo Windows 2003 Server, por medio del cual se han establecido políticas de configuración de usuario como son:

Validación de acceso por usuario y contraseña.

- Restricciones de acceso al sistema por usuario.
- Restricciones de acceso a información por usuario.
- Política de restricción de servicios.
- Restricciones de acceso a la red.

Se cuenta con un dispositivo de seguridad perimetral Firewall, IDS, IPS, con el fin de gestionar, detectar, prevenir y filtrar el tráfico entrante y saliente que hay entre las diferentes redes de la entidad. Así mismo de acuerdo con la función que realicen estos equipos, ayudan a fortalecer los controles que permiten preservar la confidencialidad, integridad y disponibilidad de la información.

Tabla 3 - Hardware de Redes

Tipo de Equipo (Hardware)	Cantidad
Swicht de red	5
Swicht de red capa 2	2
Swicht de red capa 3	1
Firewall Físico (UTM SOPHOS)	1

Fuente: Manual de uso de los Recursos Informáticos del HDPUV

Red de corriente Regulada: El Hospital cuenta con dos UPS (Sistema de poder ininterrumpido), de 36 y 12 Kva, para brindar sistema de corriente regulado a toda la infraestructura tecnológica.

Canal Internet: El Hospital dispone de un canal de Internet dedicado de 10 MB de Ancho de banda el cual está contratado con el operador Emcali.

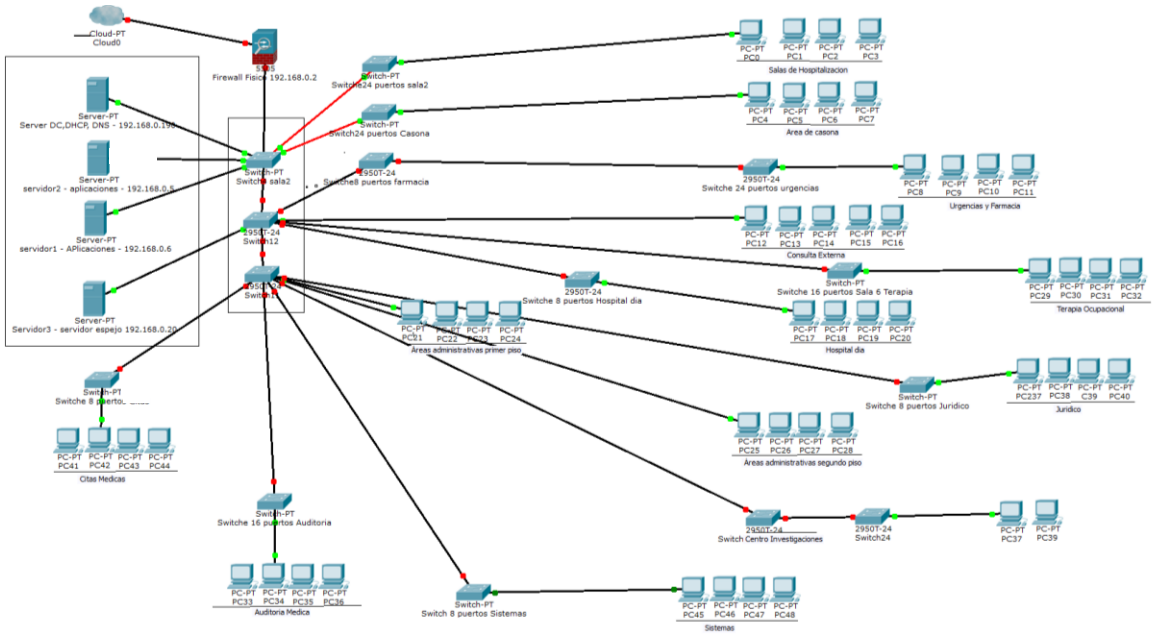
Sitio Web: El Hospital cuenta con su propio sitio web en internet www.psiquiatricocali.gov.co como herramienta de comunicación para el usuario, donde se describe su portafolio de servicios, programas, proyectos. A demás de darse a conocer nacional e internacionalmente. La página es administrada por el profesional universitario en sistemas de Hospital quien realizara revisiones cada año con el fin de evaluar solicitudes de los usuarios de la misma.

Telefonía: El Hospital cuenta con un servidor telefónico análogo y digital, para la administración de un primario de 30 líneas, adicional mente se cuenta con línea directas para los servicios de citas médicas, referencia y contra referencia y atención nocturna y fines de semana.

ESQUEMA FISICO DE LA RED INTERNA

En la siguiente ilustración se muestra la infraestructura de red física de la Entidad:

Ilustración 2–Esquema físico de Red



Fuente: Manual de Uso de los Recursos Informáticos del HDPUV

GESTIÓN DE INFORMACIÓN

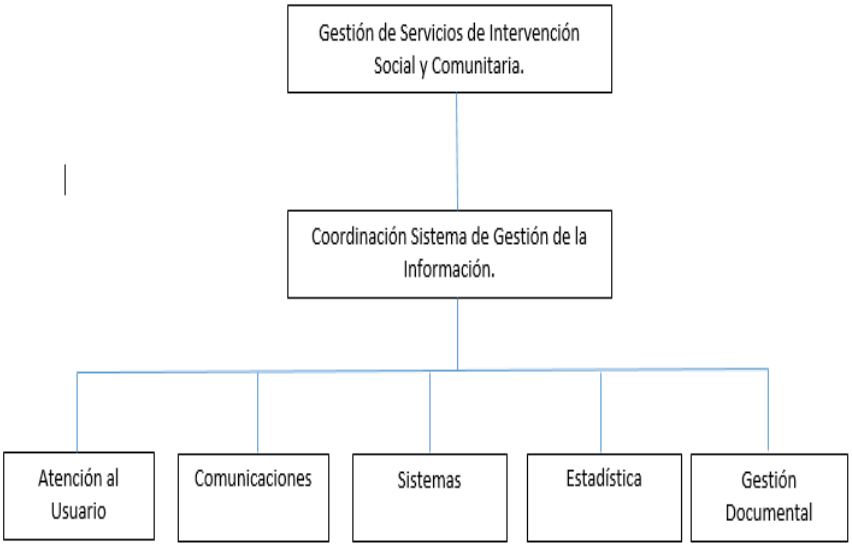
El proceso de gestión de la información tiene como base reconocer la información como ‘activo’ de la organización, gerenciar las fuentes de información dado la responsabilidad en la calidad de los datos suministrados conforme a las necesidades de los clientes y así mismo generar cambios que impacten el negocio positivamente.

Se cuenta con un plan de gerencia de la información donde se ha estandarizado todo el proceso de gestión de la información en la institución.

GOBIERNO DE TI

En la ilustración No. 3, se muestra la estructura organizacional del proceso de gestión de la información en el Hospital, donde la gestión tecnológica es realizada por el área de sistemas.

*Ilustración*3 - Estructura Organizacional de Gestión de la Información



Fuente: Plataforma documental del HDPUV

Talento Humano Área de Sistemas:

El área de sistemas del Hospital Departamental Psiquiátrico Universitario del Valle ESE, está compuesto por:

- Profesional Universitario – Sistemas.
- Técnico administrativo – Sistemas.

Profesional Universitario:

Presta servicios profesionales en sistemas de información automatizados a la Empresa en procesos operativos de ejecución de acciones de automatización y mantenimiento de los sistemas de información y el soporte al manejo de procesos automatizados en la Institución.

Funciones Esenciales:

- Participar con los líderes de programas asistenciales y administrativos en la planeación de los servicios en condiciones normales y contingentes, identificando las necesidades de recursos físicos, técnicos y tecnológicos.
- Operar las unidades del equipo de computación y los sistemas centrales y periféricos y asistir a los usuarios en su manejo.
- Garantizar el uso legal de software a través de la monitorización de caducidad de licencias.
- Aplicar y hacer cumplir las políticas de uso de los sistemas de información institucional a partir de los criterios planteados en los manuales y procedimientos para tal fin Brindar soporte técnico a todas las áreas de la institución, en la automatización y mantenimiento de los sistemas de información, en el manejo de procesos automatizados y la administración y uso del Software y Hardware utilizado.
- Garantizar la seguridad de la información mediante la consecución de software que evite ingresos maliciosos o dañinos y políticas de acceso seguro a la misma.
- Garantizar la disponibilidad de equipos e insumos técnicos y tecnológicos, de la institución a través de la programación oportuna de mantenimiento preventivo y correctivo.
- Mantener actualizada la infraestructura tecnológica (software y hardware) de la institución de acuerdo con las necesidades de los clientes internos y externos.

- Ejecutar las actividades de su responsabilidad y las resultantes de la elaboración de los planes de acción y de mejoramiento conforme a los Sistemas de Gestión Institucional.
- Proponer acciones de mejoramiento de las áreas de trabajo, atención a los usuarios y desarrollo científico y tecnológico de los procesos en la Empresa.
- Participar en los comités institucionales en los cuales se requiera el apoyo de su disciplina.
- Participar en el plan anual de capacitación institucional a través de la identificación de las necesidades propias relacionadas con la actividad que desempeña, la asistencia a cursos, talleres, reuniones y comités programados por el servicio o la institución y la divulgación de los conocimientos adquiridos.
- Participar como asistente y/o responsable en los procesos de inducción, reinducción y entrenamiento de pares.
- Custodiar, responder y hacer uso racional de los insumos, inventarios y elementos devolutivos bajo su responsabilidad.
- Las demás funciones asignadas por la autoridad competente, de acuerdo con el nivel, la naturaleza y el área de desempeño del cargo.

Técnico administrativo:

Prestar servicios de nivel técnico a la Empresa, en procesos y procedimientos que contribuyan a la misión institucional. En la realización de acciones de administración de la infraestructura computacional del hospital.

Funciones Esenciales:

- Brindar soporte técnico a todas las áreas de la institución en el manejo de los equipos de cómputo de la empresa.

- Participar en la elaboración y actualización de los procedimientos relacionados con el área de sistemas acordes al procedimiento establecido por el área de calidad.
- Apoyar en la ejecución de las actividades del plan de acción del proceso en lo referente con el área de sistemas de la institución.
- Elaborar y presentar informes sobre las actividades desarrolladas en las distintas unidades funcionales sobre soporte técnico en sistemas.
- Presentar recomendaciones cuando aplique en la mejora continua de los procesos y procedimientos de sistemas.
- Realizar actividades tendientes a controlar virus informáticos, y problemas relacionados con hardware y software institucional.
- Atender a los usuarios internos y externos en los requerimientos relacionados con el área de sistemas.
- Asistir a las capacitaciones designadas y retroalimentar al personal que le aplique para el correcto desarrollo del proceso.
- Responder, custodiar y velar por los Inventarios de los elementos devolutivos asignados y velar por la actualización permanente.
- Participar en la conformación, la capacitación y las actividades de las brigadas de emergencia para dar cumplimiento al Plan de Emergencia Hospitalario.
- Las demás funciones asignadas por la autoridad competente, de acuerdo con el nivel, la naturaleza y el área de desempeño del cargo.

4.3 MARCO TEORICO

Seguridad informática: Proceso orientado a proteger todo lo que tiene que ver con la infraestructura tecnológica (hardware - software), como columna vertebral de los sistemas de información. Para ello es importante definir los activos críticos que hacen parte de dicha infraestructura, con el fin de identificar amenazas, vulnerabilidades y gestionar los riesgos asociados.

Seguridad de la información: Proceso orientado a proteger toda la información de una institución, independiente mente del modo de creación, procesamiento, almacenamiento, si es física o digital, incluso la memoria de las personas con información institucional. Para la gestión del riesgo se tiene en cuenta las personas, los procesos y la operación del negocio, así como también los aspectos físicos y tecnológicos.

Dentro de esta se definen tres principios fundamentales como son:

Integridad: Es la salvaguarda con precisión y totalmente completa de la Información.

Confidencialidad: Es la protección de los datos, que siempre estén seguros.

Disponibilidad: Es la garantía del acceso a la información siempre que sea necesitada.

Análisis de riesgos informáticos: Es el proceso mediante el cual se identifican los activos de la Organización las vulnerabilidades y amenazas a las que se puedan ver expuestas, así como la probabilidad de que ocurran estos hechos y el impacto que puede generar con el fin de mitigar, aceptar o transferir el riesgo.

Riesgo: Es la probabilidad de que ocurra algo con consecuencias e impacto, igualmente la incertidumbre frente a la realización de un evento que afecte nuestra seguridad informática.

Amenazas: Es la potencial probabilidad que ocurra algún hecho que afecte nuestra seguridad, es decir la materialización del riesgo.

Vulnerabilidades: Son las debilidades o exposición del sistema, igualmente son las fallas ya sea por omisión o deficiencia de seguridad, que puedan ser aprovechadas por terceros.

Gestión del riesgo: Son los lineamientos dados para el manejo de la incertidumbre dada por una amenaza, eso se logra a través del estudio de los riesgos, generación de salvaguardas y controles necesarios para mitigar le riesgo.

COBIT (Objetivos de control para tecnologías de la información): Es un marco de referencia que adopta las mejores prácticas para gobernar y gestionar efectivamente **la** información y tecnología, lo cual incide en la toma efectiva de decisiones relacionadas con TI, realizar mejores inversiones, y poder generar más valor a los servicios o productos a partir de la información y los activos tecnológicos.

Características:

- Satisfacer las necesidades de los colaboradores.
- Se alinean las tecnologías de la información con las estrategias del negocio.
- Mejora los procesos de gobernanza y gestión de ti.
- Permite a los gerentes cubrir las brechas entre los requisitos de control, los aspectos técnicos y riesgos del negocio.

ITIL (biblioteca de infraestructura de tecnologías de la información): Es un marco de referencia que adopta las mejores prácticas para la gestión de servicios de TI y la relación con los procesos operativos de una empresa.

Características:

- Creación de valor a través del servicio.
- Gestión del riesgo.
- Gestión de inversión y presupuesto para TI.
- Integra la estrategia para el servicio con estrategia de negocio y necesidades de clientes.
- Mejora la interacción con los clientes.

ISO 27000: Esta norma brinda un conjunto de estándares diseñados y desarrollados por ISO (*International Organization for Standardization*) e IEC (*International Electrotechnical Commission*), proporcionando un marco de gestión de la seguridad de la información que sirve para cualquier organización, sin importar su naturaleza (pública o privada) o tamaño (grande o pequeña).

ISO 27001: Norma certificable que brinda todos los requisitos para el desarrollo, implementación, mantenimiento y mejora de un sistema de gestión de seguridad de la información.

Características:

- Compromiso de la alta dirección.
- Análisis y tratamiento de riesgos.
- Definición de objetivos y estrategias.
- Recursos y competencias.

***MAGERIT*, Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información:** Esta herramienta permite evaluar y abordar los riesgos informáticos en busca de promover la eficacia en las comunicaciones en la organización y sus colaboradores, con el fin de dar cumplimiento a los últimos estándares de la ISO 27001, 27005 y 31000 para la gestión de riesgos y brindar las justificaciones necesarias para la toma de decisiones gerenciales.

CRAMM, CCTA – Risk – Analysis – and Management Method. Se puede utilizar siempre que sea necesario para identificar la seguridad y/o requisitos de contingencia para un sistema de información o de la red.

EBIOS, Expresión de las necesidades e Identificación de los objetivos de seguridad. Ayuda a descubrir y planificar las medidas oportunas para mantener los riesgos bajo control. Adicional a esto, apoya a la preparación de la organización para procesos de evaluación, auditoría, certificación o acreditación según corresponda.

NIST SP 800 – 30, National Institute of Standards and Technology. Guía de gestión de riesgo para sistemas de tecnología de la información. Propone un conjunto de recomendaciones y actividades para una adecuada gestión de riesgos como parte de la gestión de la seguridad de la información; sin embargo, esto no es suficiente, pues se necesita del apoyo de toda la organización para que los objetivos y alcance de la gestión de riesgos concluyan con éxito.

ISO//IEC 27005 – *MEHARI*, Método armonizado de análisis de riesgos. Es una metodología utilizada para apoyar a los responsables de la seguridad informática de una empresa mediante un análisis riguroso de los principales factores de riesgo, evaluando cuantitativamente, de acuerdo con la situación de la organización, dónde se requiere el análisis; acopla los objetivos estratégicos existentes con los nuevos métodos de funcionamiento de la empresa mediante una política de seguridad y mantenimiento de los riesgos a un nivel convenido.

***CORAS, Construct a Platformfor Risk Analysis of Security Critical Systems*,** Su aplicación permite la detección de fallas de seguridad, inconsistencias, redundancia y el descubrimiento de vulnerabilidades de seguridad, exploradas en siete etapas: presentación, análisis de alto nivel, aprobación, identificación de riesgos, estimación de riesgo, evaluación de riesgo y tratamiento del riesgo

OCTAVE, Operationally Critical Threat, Asset, and Vulnerability Evaluation, Octave, evalúa los riesgos de seguridad de la información y propone un plan de mitigación de estos dentro de una organización. Sus objetivos se encuentran enfocados básicamente en concientizar a la organización en cuanto a que la

seguridad informática no es un asunto solamente técnico, y presentar los estándares internacionales que guían la implementación de seguridad de aquellos aspectos no técnicos.

COBIT, ***Control Objectives Control Objectives for Information and related Technology,*** Sus conceptos se aplican en los niveles operacional y táctico y permiten que la estructura departamento de TI el ciclo de vida de sus servicios en su conjunto, con el fin de alcanzar la excelencia operativa.

4.4 MARCO LEGAL

Ley 1266 de 2008: Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.

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"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.

Ley 1437 de 2011: Por la cual se expide el código de procedimiento administrativo y de lo contencioso administrativo.

Ley 1581 de 2012: Por la cual se dictan disposiciones generales para la protección de datos personales.

Ley 1753 de 09 de junio de 2015: Por la cual se expide el Plan Nacional de Desarrollo, 2014-2018. “Todos por un nuevo país”

Decreto 3816 de 2003: "Por el cual se crea la Comisión Intersectorial de Políticas y de Gestión de la Información para la Administración Pública".

Decreto 235 DE 2010: Por el cual se regula el intercambio de información entre entidades para el cumplimiento de funciones.

Decreto 019 de 2012: Por el cual se dictan normas para suprimir o reformar regulaciones, procedimientos y trámites innecesarios existentes en la Administración Pública.

Decreto 2609 de 2012: Por el cual se reglamenta el Título V de la Ley 594 de 2000, parcialmente los artículos 58 y 59 de la Ley 1437 de 2011 y se dictan otras disposiciones en materia de Gestión Documental para todas las Entidades del Estado.

Decreto 1078 de 2015: "Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones".

Decreto 415 de 2016: "Por el cual se adiciona el Decreto Único reglamentario del sector de la Función Pública, Decreto 1083 de 2015, en lo relacionado con la definición de lineamientos para el fortalecimiento institucional en materia de tecnologías de la información y las comunicaciones".

Decreto 2094 de 2016: Por el cual se modifica la estructura del Departamento Administrativo para la Prosperidad Social - Prosperidad Social.

Decreto 1499 de 2017: Por medio del cual se modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015.

Documento CONPES No. 3854 de 2016: Política Nacional de Seguridad Digital.

Acuerdo 003 de 2015 del AGN: “Por el cual se establecen los lineamientos generales para las entidades del Estado en cuanto a la gestión de documentos electrónicos generados como resultado del uso de medios electrónicos de conformidad con lo establecido en el capítulo IV de la Ley 1437 de 2011, se reglamenta el artículo 21 de la Ley 594 de 2000 y el capítulo IV del Decreto 2609 de 2012.

5. METODOLOGIA

5.1 METODOLOGIA DE LA INVESTIGACIÓN

La metodología MAGERIT – Versión 3.0 es la metodología de análisis y gestión de riesgos de los sistemas de Información, desarrollada por el concejo superior de administración electrónica, define los riesgos como la posibilidad que suceda un daño, tiene dos objetivos claros: el estudio de los riesgos que soportan los sistemas de información y realizar las recomendaciones de las medidas que se deben adoptar para conocer, prevenir, impedir, reducir o controlar los riesgos encontrados, realiza análisis sobre sus principales elementos los cuales define como activo, amenaza, vulnerabilidades, impacto, riesgo y salvaguarda, maneja las etapas de planificación, análisis de riesgos, gestión de riesgos y selección de salvaguardas, sus guías se dividen en tres libros: Métodos, Catalogo de Elementos y Guías Técnicas.

Los cuales contemplan el siguiente catálogo de elementos:

- Tipos de Activos
- Dimensión de valoración de los activos
- Criterios de valoración de los activos
- Amenazas típicas sobre los sistemas de Información
- Salvaguardas por considerar para proteger sistemas de Información

Aplicada esta metodología al estudio que se realiza en el desarrollo de este proyecto se recolecta la información pertinente mediante recorridos en la Institución donde se identifican los activos físicos y se plasman en la ficha técnica de activos, adicional se realizará entrevistas con el personal encargado del área informática para conocer el área y su infraestructura, las políticas ya implementadas, la documentación pertinente y el plan de seguimiento y medición, finalmente se realizará observación de las prácticas de los usuarios.

6. ANÁLISIS DE LA INFORMACIÓN

Teniendo en cuenta la metodología Magerit que hace énfasis en la identificación de activos categorizados en grupos, con el fin de identificar riesgos y realizar controles frentes a estos, se realiza la identificación de activos informáticos en el Hospital Departamental Psiquiátrico Universitario del Valle.

6.1 IDENTIFICACIÓN DE ACTIVOS

Ver anexo No. 1 Inventarios de Activos

6.2 IDENTIFICACIÓN DE VULNERABILIADES

Una vulnerabilidad es una debilidad o falla en un activo de información, la cual puede ser explotada por una amenaza, poniendo en riesgo la confidencialidad, integridad y disponibilidad de la información.

Para la identificación de vulnerabilidades se priorizaron los activos de información más sensibles de la Institución los cuales fueron analizados con software especializado como Nmap ("*Network Mapper*") que es una herramienta de distribución libre utilizada para el análisis de redes y auditorias de seguridad, esta aplicación utiliza técnicas especializadas de escaneo para identificar equipos activos en una red, sistemas operativos, puertos abiertos, protocolos y servicios en ejecución, adicionalmente contiene scripts para identificación de vulnerabilidades, lo que significa información valiosa para estructurar un ataque por parte de un ciber-delincuente, y Nessus que es un escáner de vulnerabilidades muy potente el cual se puede utilizar contra sistemas operativos, aplicaciones web, base de datos, redes, dispositivos móviles, entre otros; en busca de malware, configuraciones erróneas, software desactualizado, entre otras. Entre sus principales características

se encuentra que cuenta con una interfaz web, la cual se compone por un servidor http y el cliente web, lo que le permite ser ejecutada en cualquier plataforma, tiene además una base de datos de vulnerabilidades que se actualiza constantemente, permite también generar diversos reportes que se pueden relacionar con *framework* de explotación como Metasploit o CoreImpact.

Tabla 4 - Activos de Información Analizados

Equipo	Software/Aplicativo	Especificaciones
Servidor HP Proliant ML 370	Servicios DC, DNS y DHCP – Sistema Operativo Windows Server 2003 R2.	Doble procesador Intel Xeon 2mb de cache. 3.6 GHz , 8000 Mhz F SB con EM64T, 4 GB memoria DDR - Dos discos duros de 72 Gb en Raid 0 (SC SI) - 3 Discos duros de 146 GB, en raid 5 (SC SI) - Alimentación y refrigeración redundante.
Servidor espejo HP Proliant BL460C G5 Server Blade	SQL Server 2005, Dinámica Gerencial Hospitalaria, Cguno 7.0 Cguno 5.0 - Windows Server 2003 R2.	Doble procesador Intel Xeoncuad 12mb de cache. 3.0 GHz, 1333 Mhz F SB con EM64T, 10 GB memoria DDR-2 discos duros de 72 Gb en Raid 0 (SC SI) - 4 Discos duros de 146 GB, en raid 5 (SC SI).Alimentación y refrigeración redundante
HP Proliant BL460C G8 Server Blade	SQl 2012, Siesa Enterprise - Windows Server 2012.	HP Proliant BL460c Gen 8 - servidor compacto 2 vias 1 Xeon E52640V2 / 2 Ghz - Ram 32GB - SaS - Hot - Swap 2.5 - Memoria cache de 20 MB, controlador de almacenamiento SAS - 2 (SAS de 6 GB / 2).

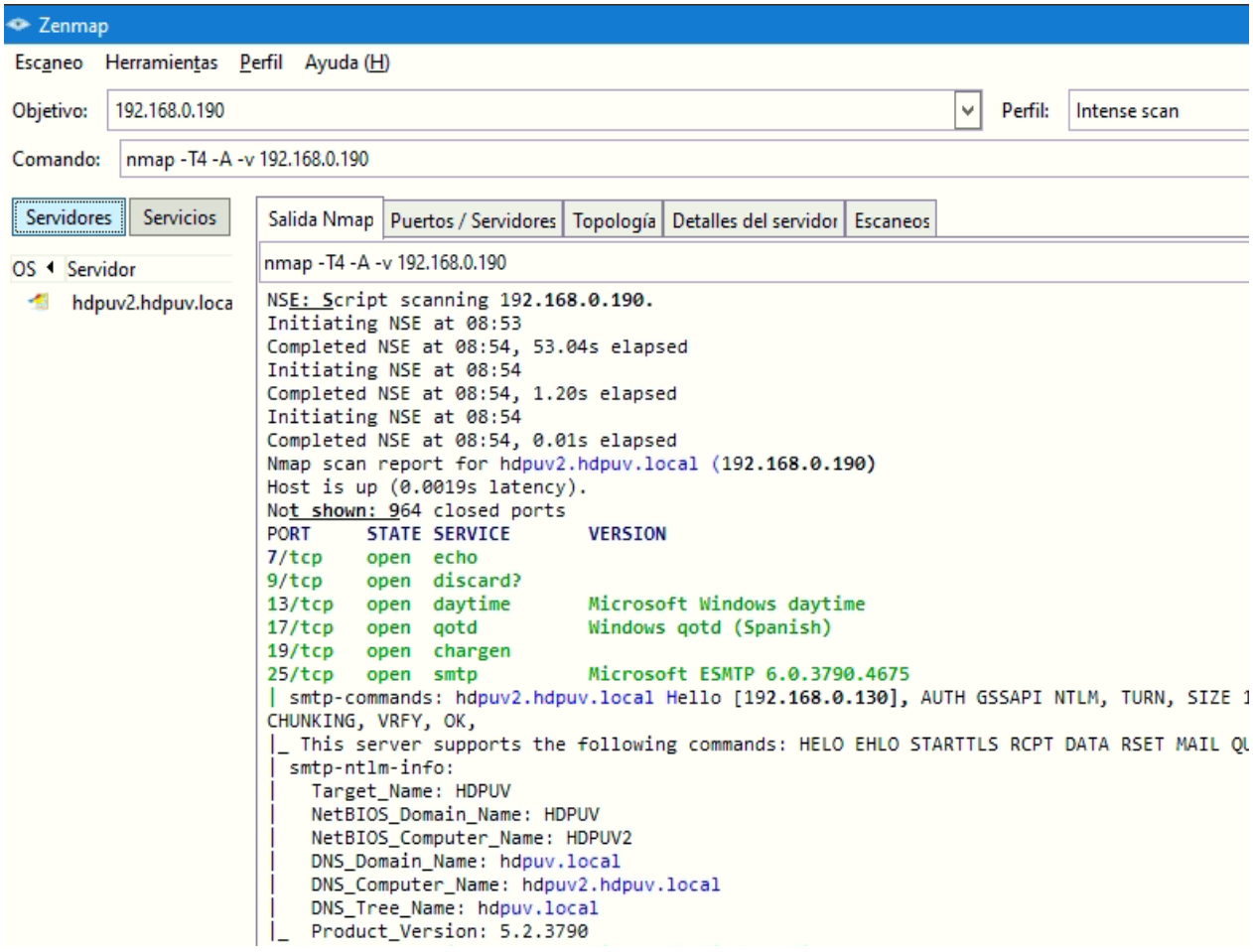
Resultados NMAP

Se ejecuta la interfaz gráfica de Nmap la cual presenta varias opciones de escaneo, en este caso se toma la opción "*Intense Scan*", que utiliza el comando nmap -T4 -A -v <dirección IP> para escanear los puertos TCP más comunes, servicios en ejecución, sistema operativo y su versión; de igual forma se ejecuta *script* para identificación de vulnerabilidades.

- **Servidor HP Proliant ML 370:**

Se realiza el análisis con el aplicativo nmap al servidor HP Proliant ML 370 con dirección IP 192.1680.0.190, con el objetivo de obtener los datos que lleve a identificar las vulnerabilidades.

Ilustración 4 – Análisis servidor - HP Proliant ML 370

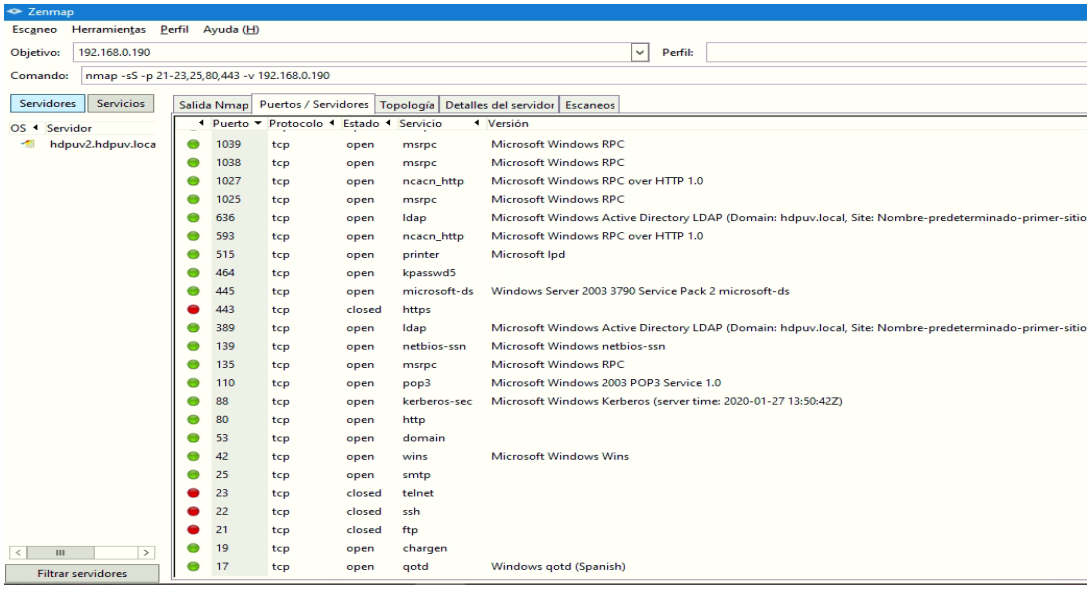


Fuente: Aplicativo NMAP

Una vez realizado el escaneo al Activo de información con IP 192.168.0.190, La herramienta muestra en diferentes pestañas la información recolectada.

En la pestaña puertos/servidores se observa un recopilatorio de todos los puertos abiertos, el número de puerto, protocolo, estado, servicio, dependiendo del tipo de escaneo que se realice, mostrando más o menos puertos.

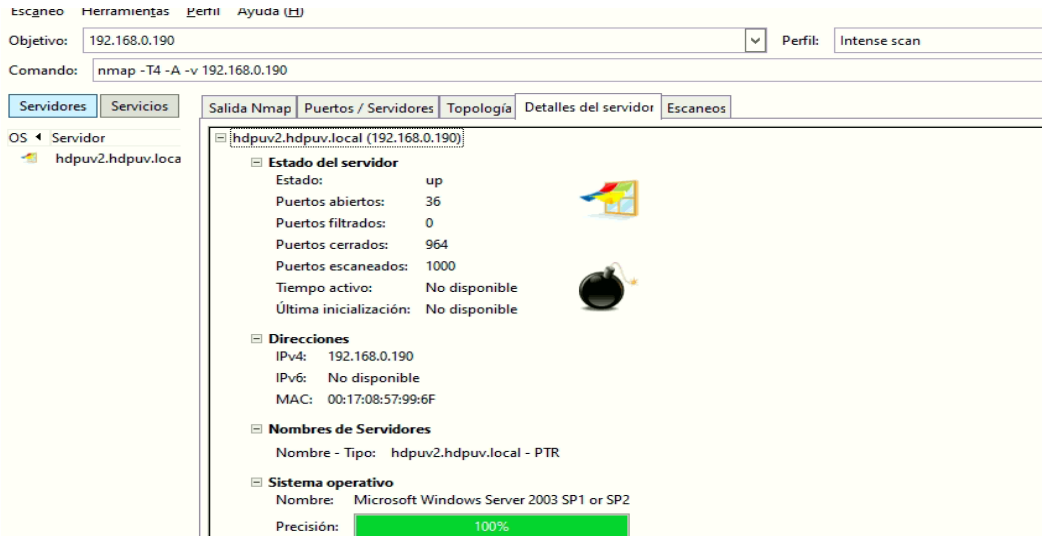
Ilustración 5 - Escaneo de Puertos y servicios - HP Proliant ML 370



Fuente: Análisis con el aplicativo NMAP

El equipo escaneado se puede ver en la pestaña Detalles del servidor donde se encuentra cada uno de los datos correspondientes al mismo.

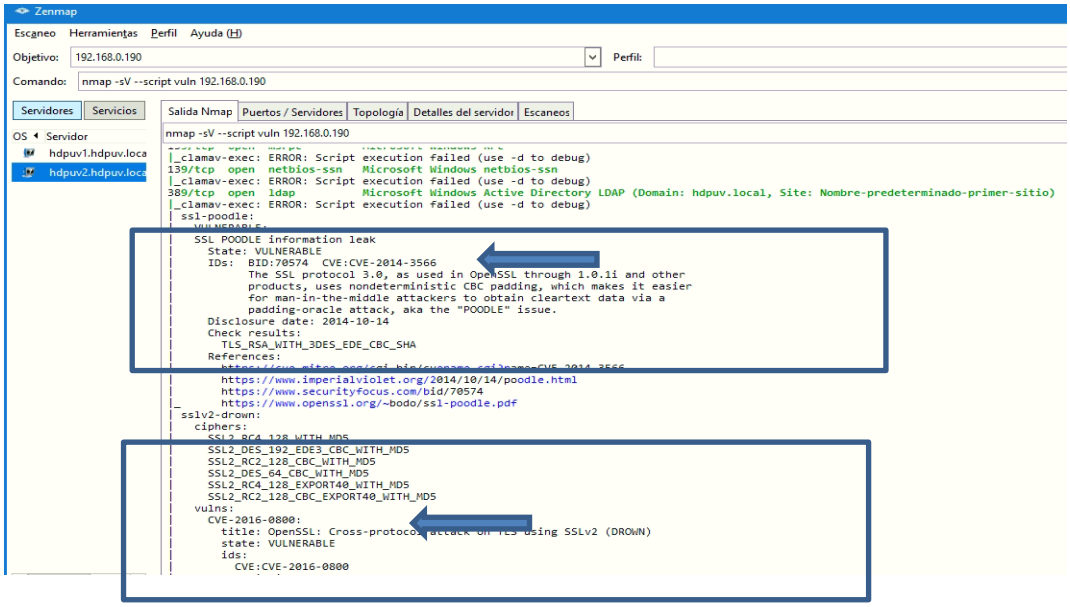
Ilustración 6– Detalles del servidor - HP Proliant ML 370



Fuente: Análisis aplicativo Nmap

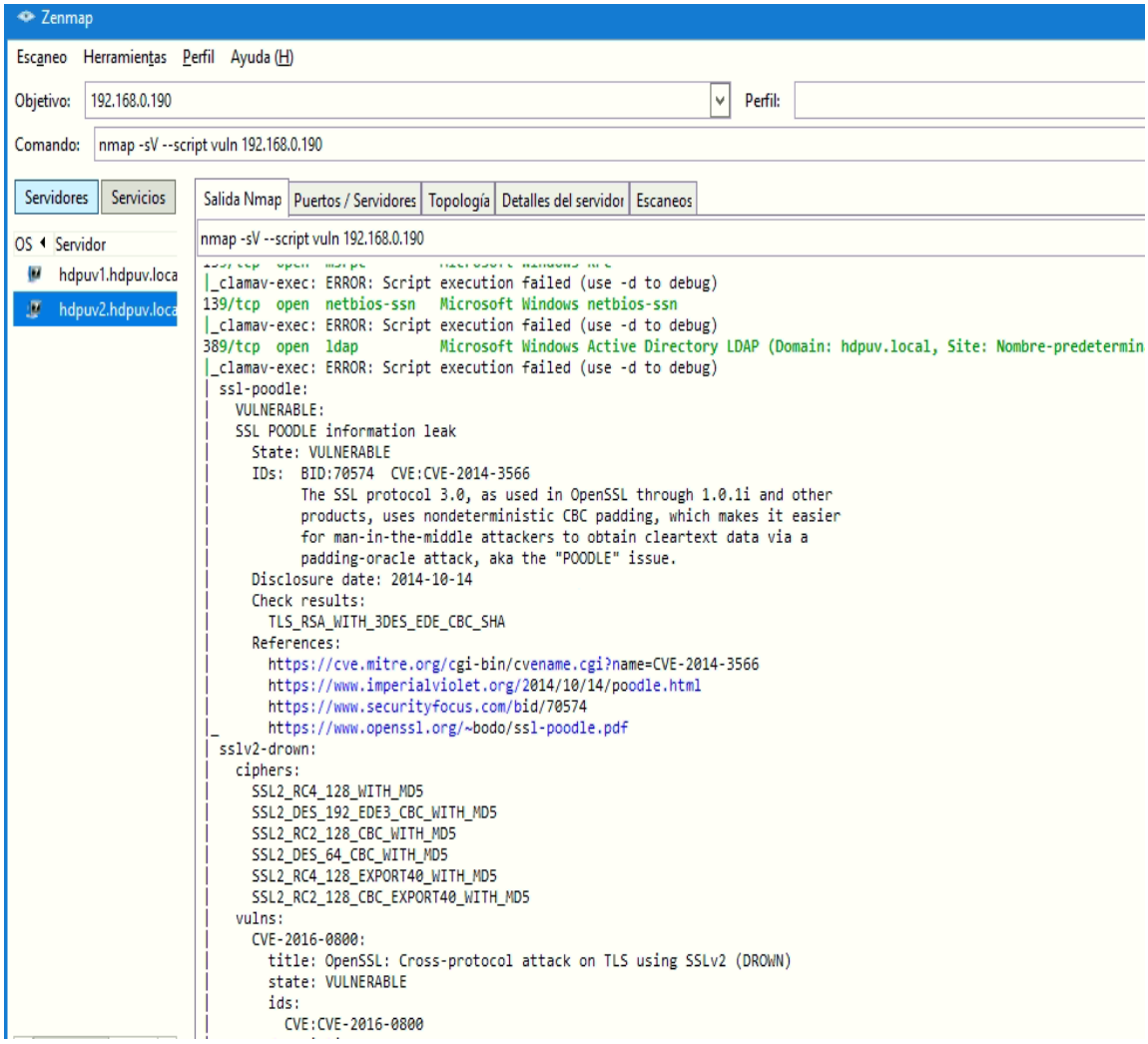
En la ilustración 7, 8 y 9 se visualizan resultados de ejecución del *scriptVuln* para la identificación de vulnerabilidades del servidor espejo HP *Proliant* ML 370con IP 192.168.0.190 desde el aplicativo Nmap

Ilustración 7 – Identificación de vulnerabilidades 1- HP Proliant ML 370



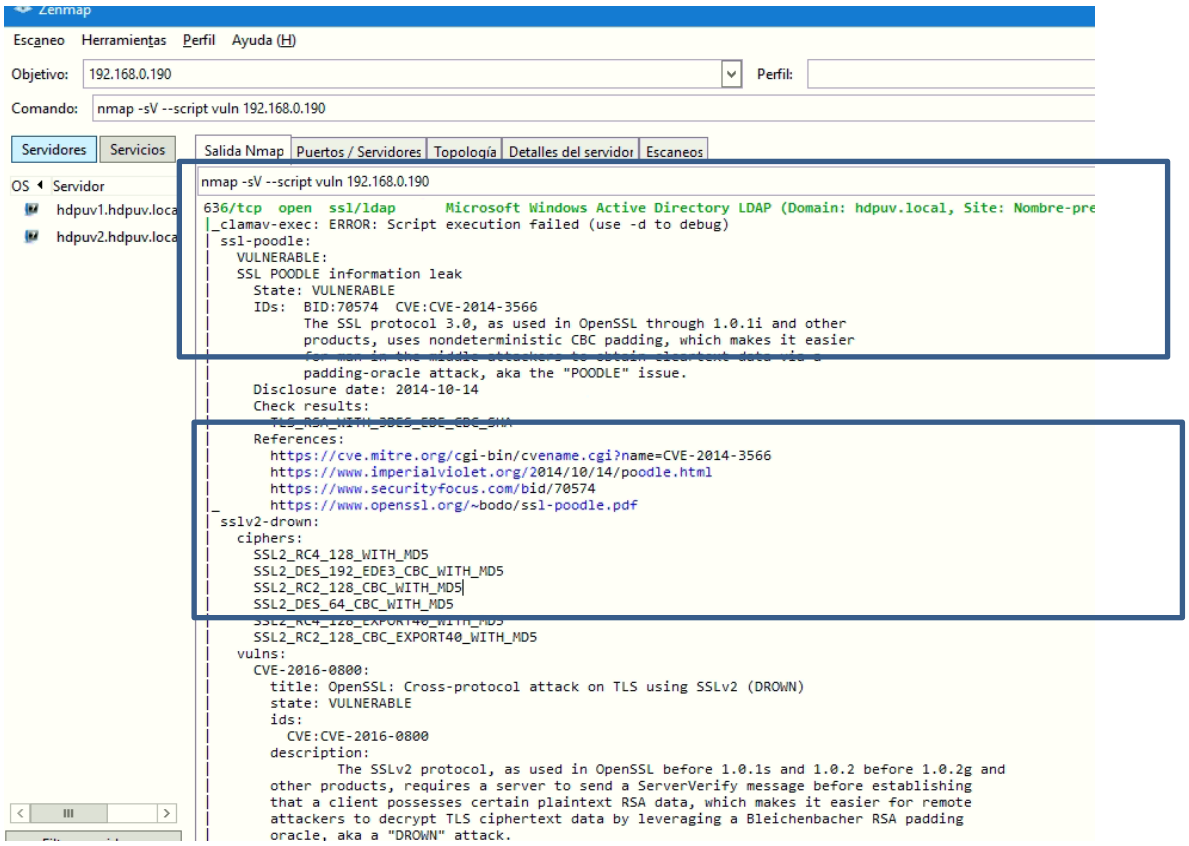
Fuente: Análisis aplicativo Nmap

Ilustración 8 - Identificación de vulnerabilidades 2 - HP Proliant ML 370



Fuente: Análisis aplicativo Nmap

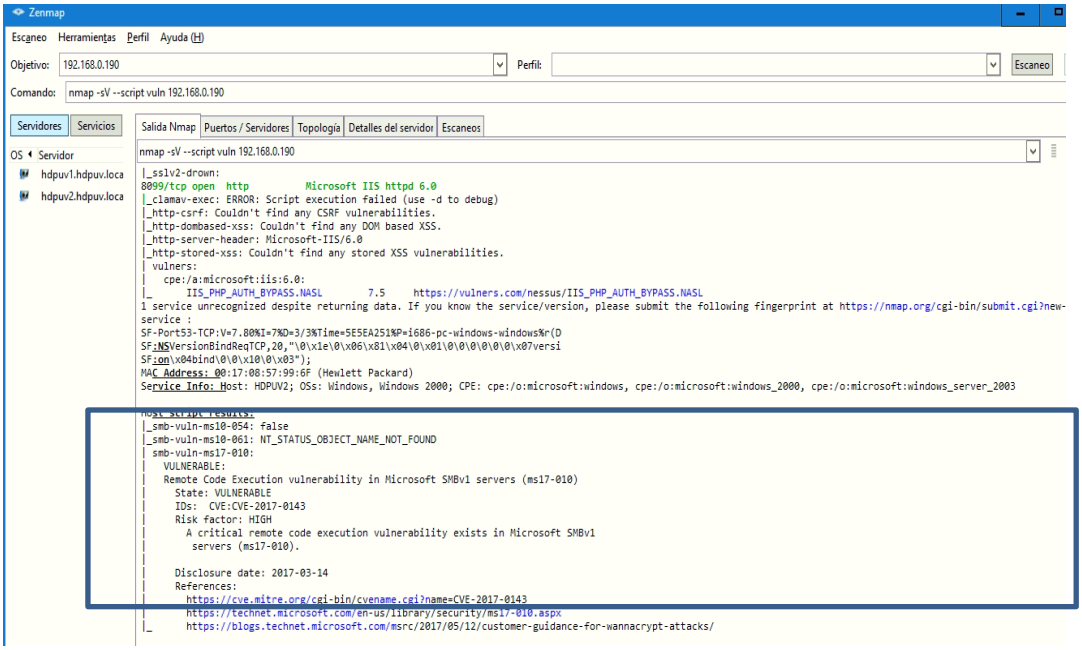
Ilustración 9 - Identificación vulnerabilidades 3- HP Proliant ML 370



Fuente: Análisis aplicativo Nmap

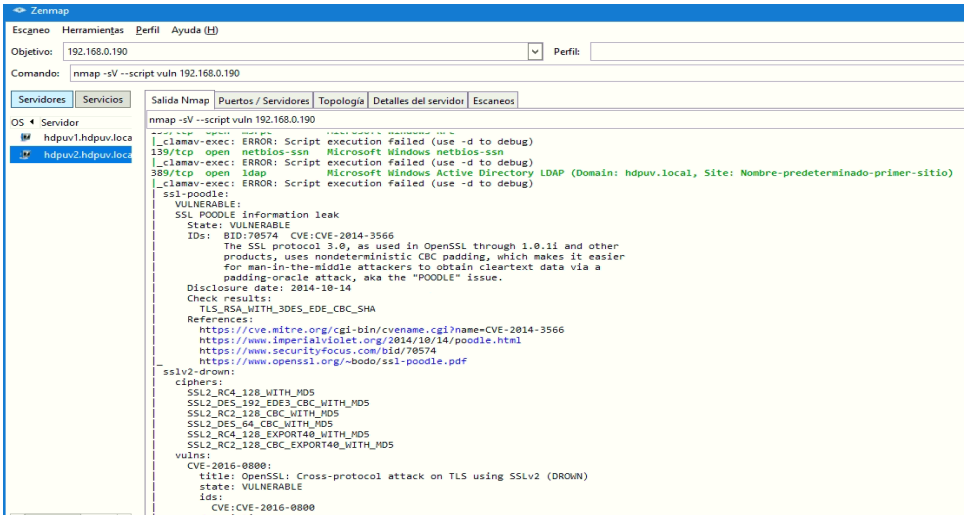
En las ilustraciones 10 y 11, se evidencia la vulnerabilidad *EternalBlue,* en el servidor con dirección IP 192.168.0.190, siendo una vulnerabilidad crítica para la institución dado que se pueden presentar ataques por *ransonware* como WannaCry.

Ilustración 10 - Identificación de vulnerabilidades 3 - HP Proliant ML 370



Fuente: Análisis aplicativo Nmap

Ilustración 11- Identificación de vulnerabilidades 4 - HP Proliant ML 370



Fuente: Análisis aplicativo Nmap

Vulnerabilidades importantes evidenciadas con Nmap en el activo de información con IP 192.168.0.190:

- CVE-2017-0143 - Vulnerabilidad de ejecución remota de código en Windows SMB.

Descripción: Existen múltiples vulnerabilidades de ejecución remota de código en *Microsoft Server Message* Block 1.0 (SMBv1) debido al manejo inadecuado de ciertas solicitudes. Un atacante remoto no autenticado puede explotar estas vulnerabilidades, a través de un paquete especialmente diseñado, para ejecutar código arbitrario. (CVE-2017-0143, CVE-2017-0144, CVE-2017-0145, CVE-2017-0146, CVE-2017-0148): existe una vulnerabilidad de divulgación de información en *Microsoft Server MessageBlock* 1.0 (SMBv1) debido a un manejo inadecuado de ciertas solicitudes. Un atacante remoto no autenticado puede explotar esto, a través de un paquete especialmente diseñado, para revelar información confidencial. (CVE-2017-0147).

ETERNALBLUE, ETERNALCHAMPION, ETERNALSANCE y ETERNALSYNERGY son cuatro de las múltiples vulnerabilidades y *exploits* del Grupo de ecuaciones reveladas en 2017/04/14 por un grupo conocido como *Shadow Brokers. WannaCry / WannaCrypt* es un programa de *ransomware* que utiliza el *exploit* ETERNALBLUE, y *EternalRocks* es un gusano que utiliza siete vulnerabilidades de EquationGroup. Petya es un programa de *ransomware* que primero utiliza CVE-2017-0199, una vulnerabilidad en Microsoft Office, y luego se propaga a través de *ETERNALBLUE*

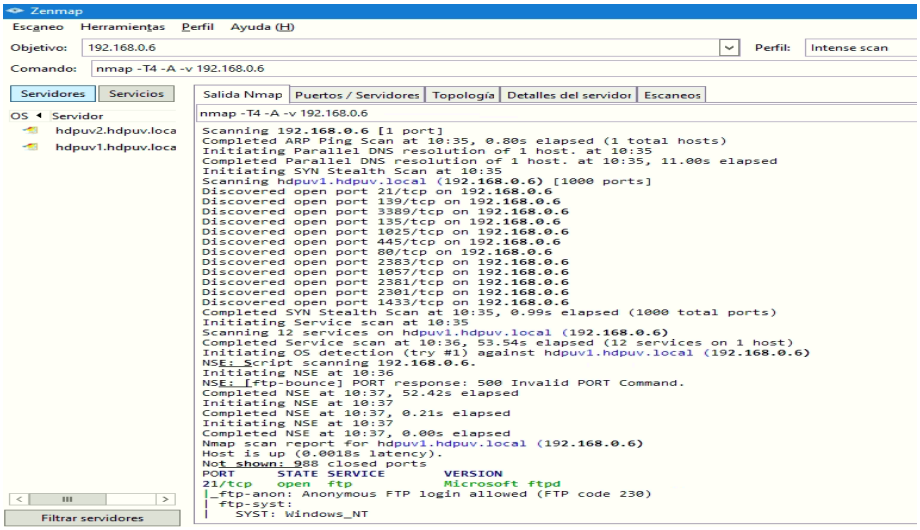
Solución: Microsoft lanzó un conjunto de parches para Windows Vista, 2008, 7, 2008 R2, 2012, 8.1, RT 8.1, 2012 R2, 10 y 2016. Microsoft también lanzó parches de emergencia para sistemas operativos Windows que ya no son compatibles, incluidos Windows XP, 2003 y 8. (Microsoft, 2017)

Para los sistemas operativos Windows no compatibles, por ejemplo, Windows XP, Microsoft recomienda que los usuarios suspendan el uso de SMBv1. SMBv1 carece de características de seguridad que se incluyeron en versiones posteriores de SMB. SMBv1 puede deshabilitarse siguiendo las instrucciones del proveedor proporcionadas en Microsoft KB2696547. Además, US-CERT recomienda que los usuarios bloqueen SMB directamente bloqueando el puerto TCP 445 en todos los dispositivos de límite de red. Para SMB sobre la API NetBIOS, bloquee los puertos TCP 137/139 y los puertos UDP 137/138 en todos los dispositivos de límite de red.

- **Servidor HP Proliant BL460C G5 Server Blade**

Se realiza el análisis con el aplicativo nmap al servidor HP Proliant BL460C G5 Server **Blade** con dirección IP 192.1680.0.6, con el objetivo de obtener los datos que lleven a la identificación de las vulnerabilidades.

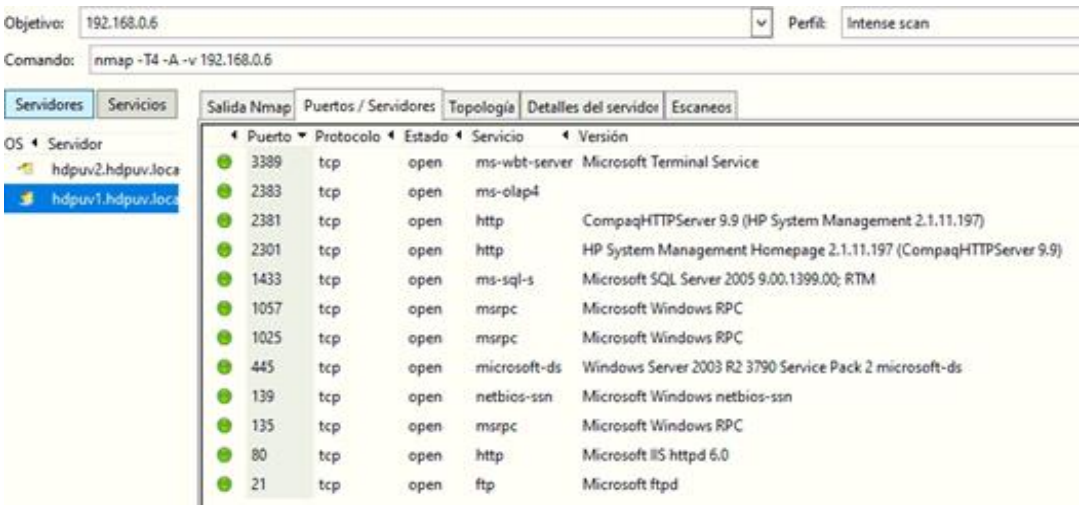
Ilustración 12- Análisis Servidor - HP Proliant BL460C G5



Fuente: Análisis aplicativo Nmap

En la pestaña puertos/servidores se observa un recopilatorio de todos los puertos abiertos, el número de puerto, protocolo, estado, servicio, dependiendo del tipo de escaneo que realicemos, se muestra más o menos puertos.

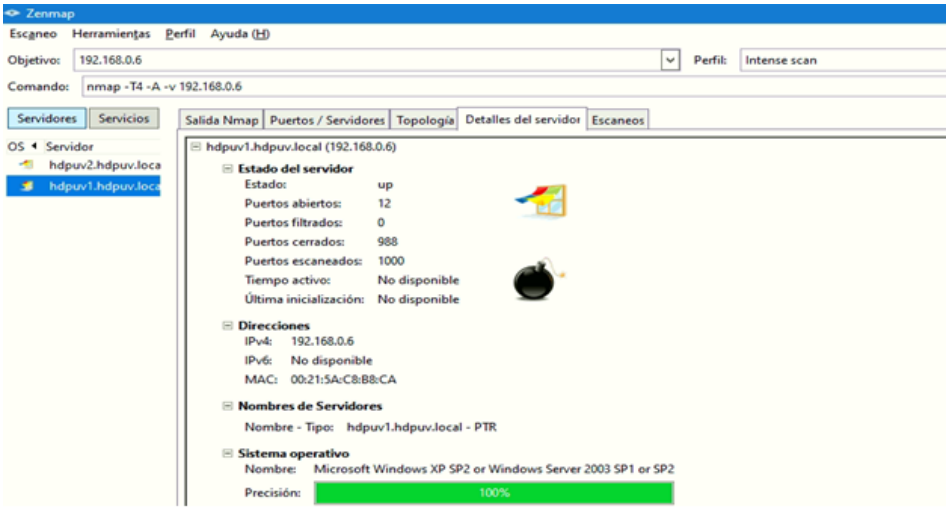
Ilustración 13 –Escaneo de puertos y servicios - HP Proliant BL460C G5



Fuente: Análisis aplicativo Nmap

El equipo escaneado se puede ver en la pestaña Detalles del servidor donde se encuentra cada uno de los datos correspondientes al mismo.

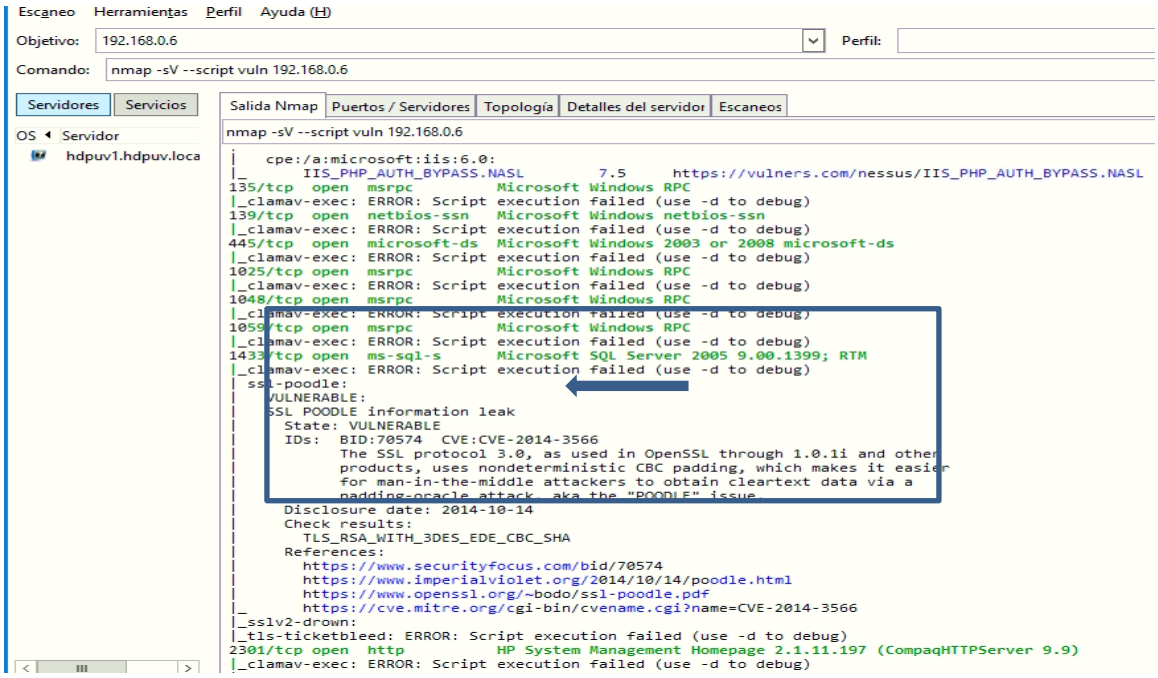
Ilustración 14– Detalles del servidor- HP Proliant BL460C G5



Fuente: Análisis aplicativo Nmap

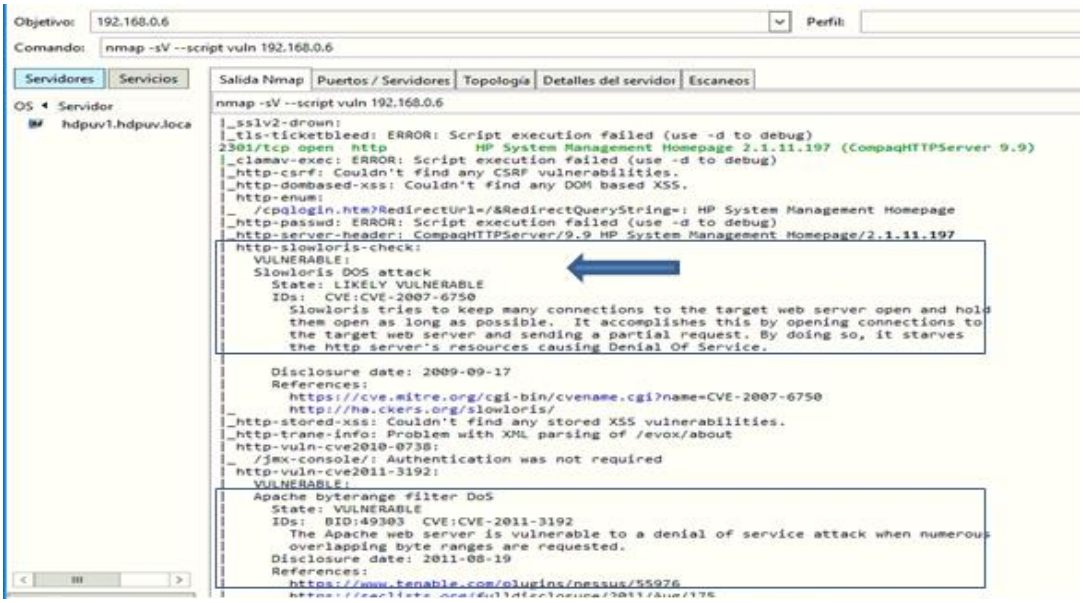
En la ilustración 15, 16 y 17 se visualizan resultados de ejecución del *scriptVuln* para la identificación de vulnerabilidades del servidor espejo HP Proliant BL460C G5con IP 192.168.0.6 desde el aplicativo Nmap.

Ilustración 15 - Escaneo de vulnerabilidades - HP Proliant BL460C G5



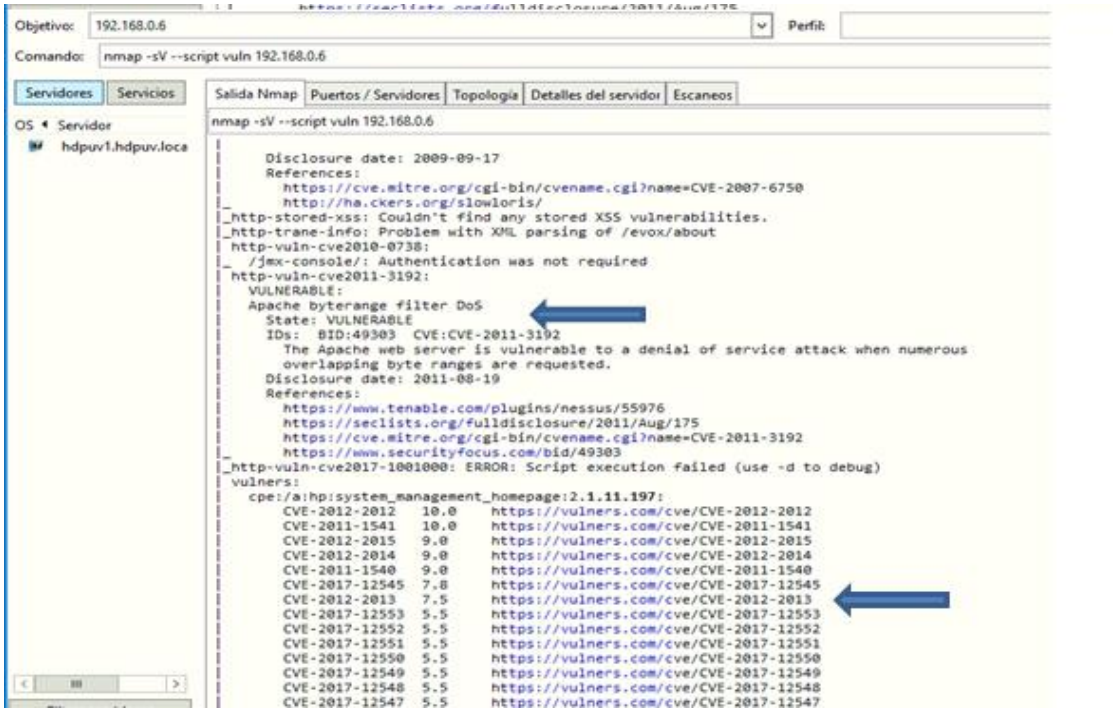
Fuente: Análisis aplicativo Nmap

Ilustración 16 - Escaneo de vulnerabilidades 2 - HP Proliant BL460C G5



Fuente: Análisis aplicativo Nmap

Ilustración 17- Escaneo de vulnerabilidades 3 - HP Proliant BL460C G5



Fuente: Análisis aplicativo Nmap

Por cada uno de los puertos identificados, se puede buscar vulnerabilidades en el código de las aplicaciones que lo ejecutan, para detectar si es posible utilizar un *exploit* que tome ventaja de dichas vulnerabilidades.

A continuación, se relacionan vulnerabilidades importantes evidenciadas con Nmap en el activo de información con IP 192.168.0.6:

- Vulnerabilidad: POODLE SSLv3 (CVE-2014-3566)

Descripción: El protocolo SSL 3.0, como se usa en OpenSSL a través de 1.0.1i y otros productos, utiliza relleno CBC no determinista, lo que facilita a los atacantes intermedios obtener datos en texto claro a través de un ataque de oráculo de relleno, también conocido como "POODLE " problema.

POODLE afecta los estándares más antiguos de encriptación, específicamente la versión 3. *Secure Socket Layer* (SSL). No afecta el nuevo mecanismo de encriptación conocido como *Transport Layer Security* (TLS).

Explotar esta vulnerabilidad no se logra fácilmente. Los ataques de hombre en el medio requieren grandes cantidades de tiempo y recursos. Si bien la probabilidad es baja, *Red Hat* recomienda implementar solo TLS para evitar fallas en SSL.

Solución: Varios proveedores han proporcionado parches a las bibliotecas criptográficas que presentan un valor de conjunto de cifrado de señalización alternativa de TLS (TLS_FALLBACK_SCSV). Este mecanismo alternativo permite a los clientes indicar a un servidor que admiten versiones SSL / TLS más nuevas que las propuestas inicialmente. En el caso de un comportamiento sospechoso en el que un cliente intenta recurrir a una versión anterior cuando se admiten versiones más recientes, el servidor cancelará la conexión.

- Vulnerabilidad: (CVE-2011-3192)

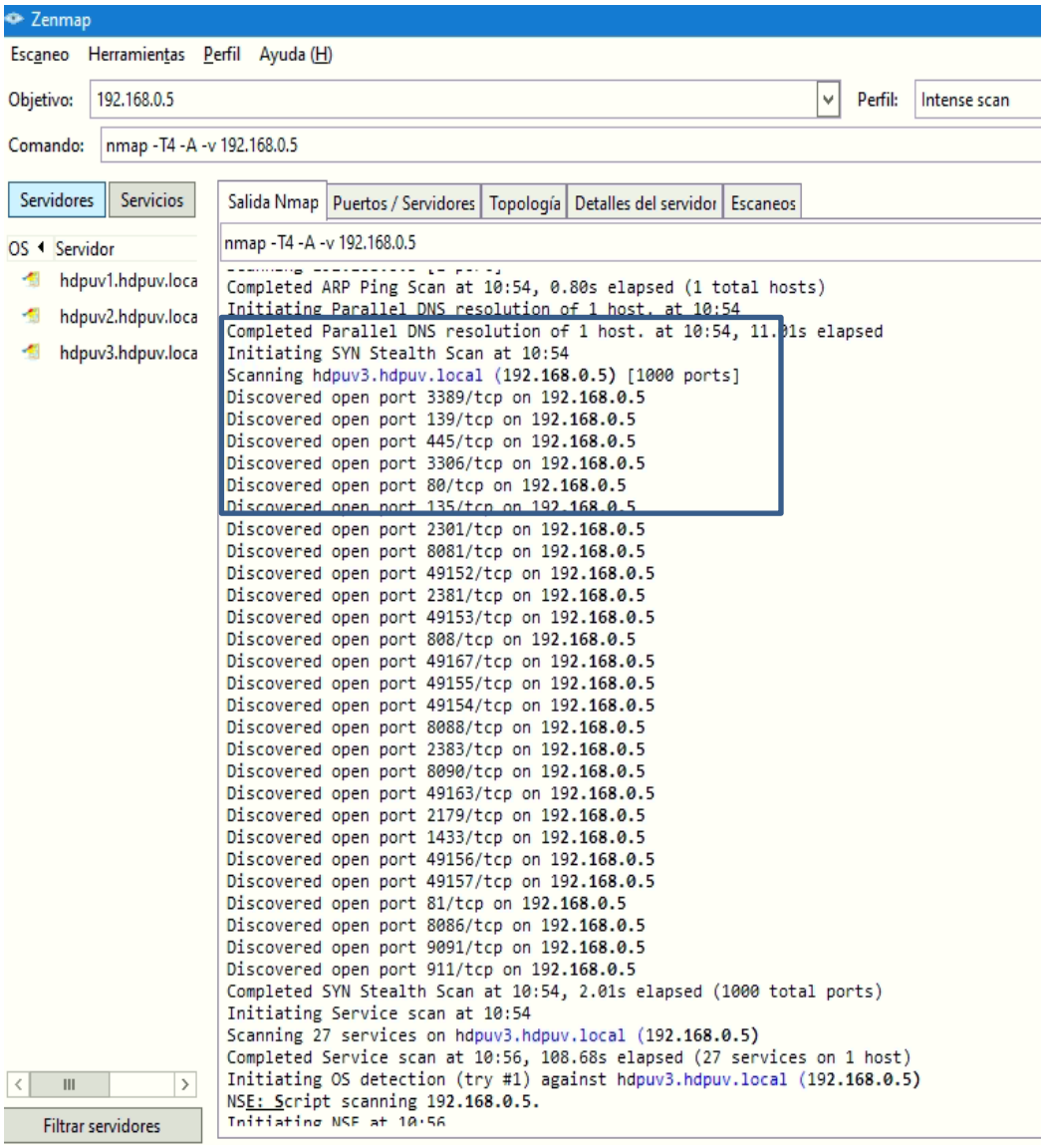
Descripción: El filtro de *byterange* en el servidor HTTP Apache 1.3.x, 2.0.x hasta 2.0.64 y 2.2.x hasta 2.2.19 permite a los atacantes remotos causar una denegación servicio (consumo de memoria y CPU) a través de un encabezado que expresa múltiples rangos superpuestos.

Solución: Use *SetEnvIf* o *mod_rewrite* para detectar una gran cantidad de rangos y luego ignore el rango encabezado o rechace la solicitud, limite el tamaño del campo de solicitud a unos pocos cientos de *bytes*,tenga en cuenta que mientrasesto mantiene el encabezado Range ofensivo corto - puede romper otros encabezados; como *cookies* de gran tamaño o campos de seguridad, *use mod_headers* para deshabilitar completamente el uso de encabezados *Range: Request Heade runset Range*, por ultimo implemente un módulo de conteo de encabezados *Range* como una medida temporal provisional.

- **HP Proliant BL460C G8 *Server Blade***

En la ilustración 18, 19 y 20 se realiza el análisis e identificación las Vulnerabilidades del servidor con dirección 192.168.0.5 identificadas con el aplicativo Nmap, para el escaneo de vulnerabilidades.

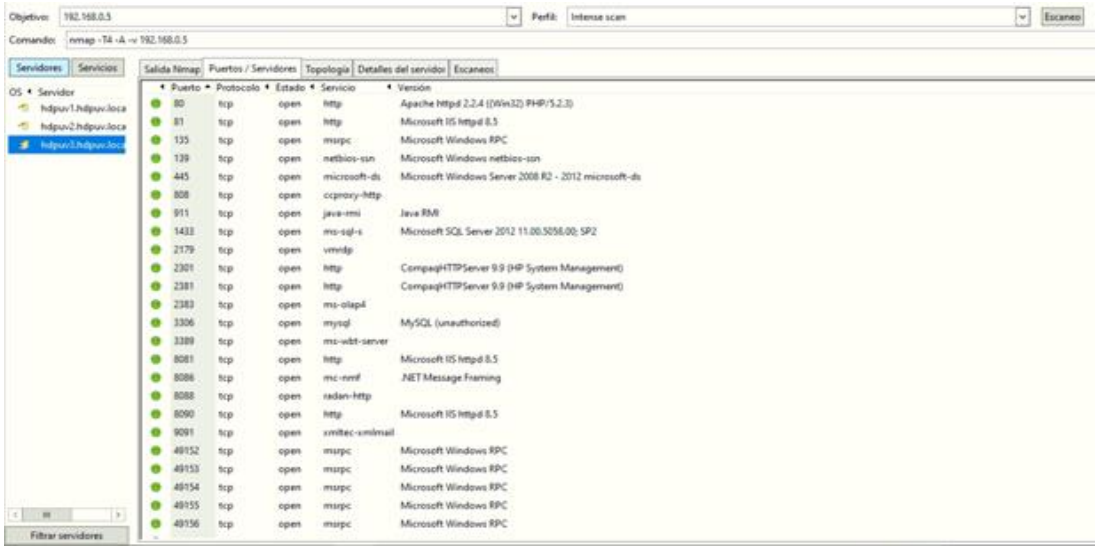
Ilustración 18 – Análisis del servidor - HP Proliant BL460C G8



Fuente: Análisis aplicativo Nmap

En la pestaña puertos/servidores se observa un recopilatorio de todos los puertos abiertos, el número de puerto, protocolo, estado, servicio, dependiendo del tipo de escaneo que realicemos, muestra más o menos puertos.

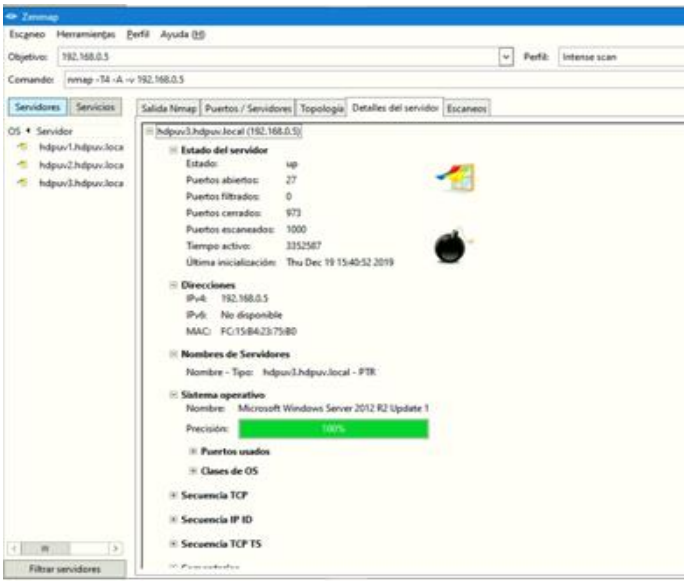
Ilustración 19–Puertos y servicios - HP Proliant BL460C G8 Server *Blade*



Fuente: Análisis aplicativo Nmap

El equipo escaneado se puede ver en la pestaña Detalles del servidor donde se encuentra cada uno de los datos correspondientes al mismo.

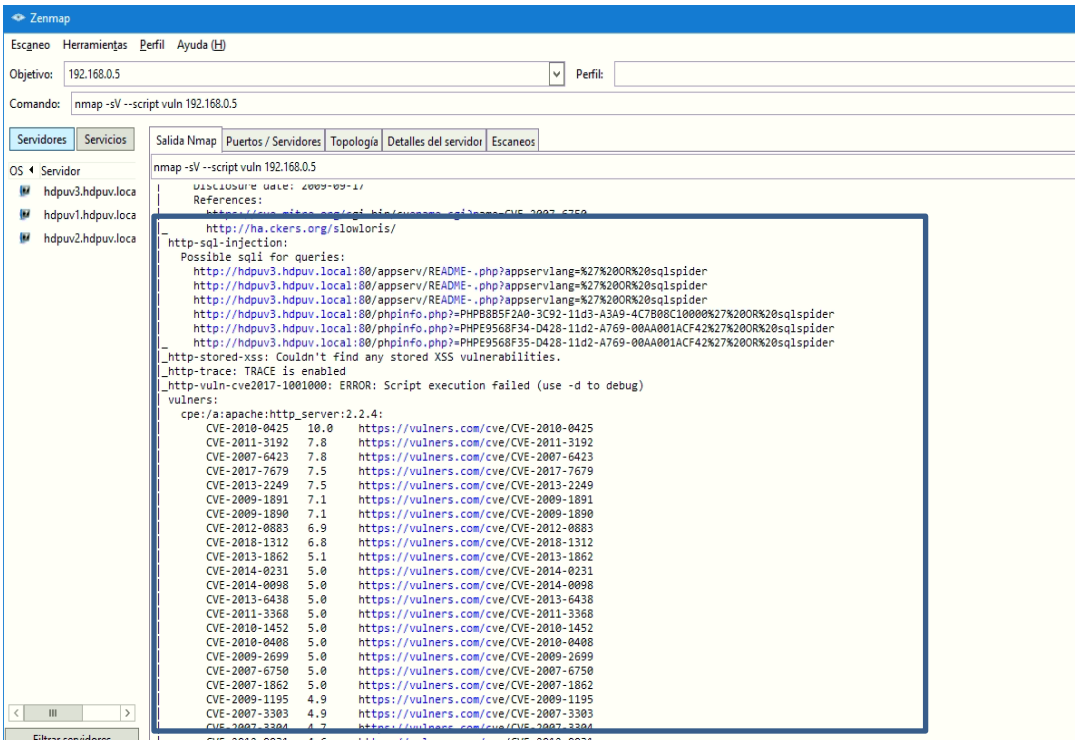
Ilustración 20 – Detalles del servidor- HP Proliant BL460C G8 Server *Blade*



Fuente: Análisis aplicativo Nmap

En la ilustración 21 se evidencia vulnerabilidades del servidor del servidor 192.168.0.5 identificadas con el aplicativo Nmap, para el escaneo de vulnerabilidades se utiliza el *scriptVuln*.

Ilustración 21– Escaneo de vulnerabilidades - HP Proliant BL460C G8 *Server* Blade 3



Fuente: Análisis aplicativo Nmap

Vulnerabilidades importantes evidenciadas con Nmap en el activo de información con IP 192.168.0.5:

- Vulnerabilidades múltiples en la versión obsoleta del Apache Server.
  Descripción: la versión de Apache 2.2.x que se ejecuta en el host remoto es anterior a 2.2.15. Por lo tanto, está potencialmente afectado por múltiples vulnerabilidades:

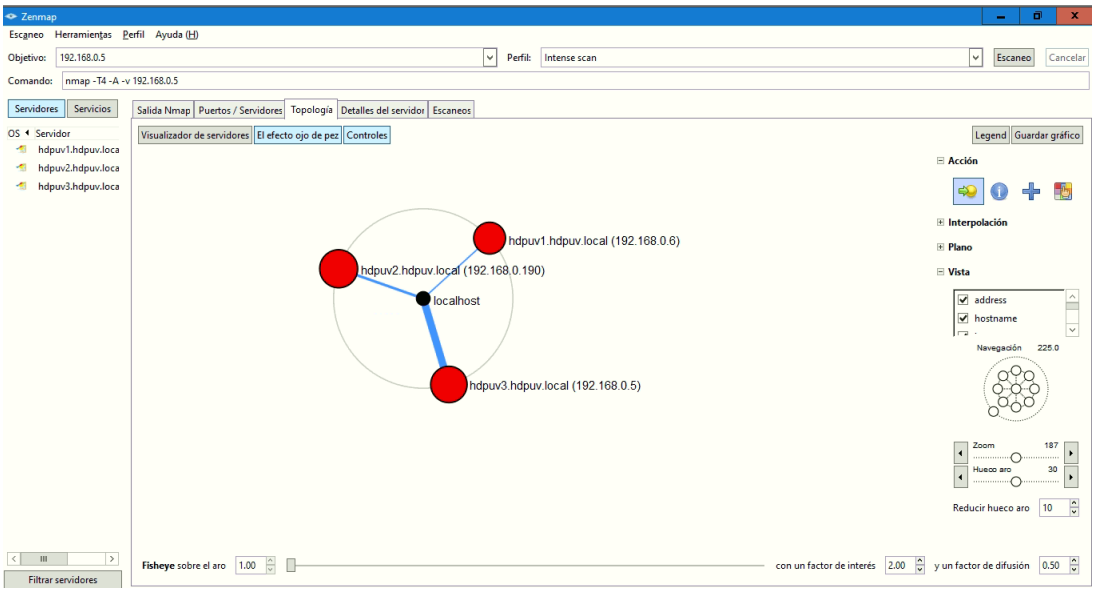
- Es posible un ataque de inyección de prefijo de renegociación TLS. (CVE-2009-3555) - El módulo *'mod_proxy_ajp'* devuelve el código de estado incorrecto si

encuentra un error que hace que el servidor de fondo se ponga en un estado de error. (CVE-2010-0408) - El *'mod_isapi'* intenta descargar el 'ISAPI.dll' cuando encuentra varios estados de error que podrían dejar devoluciones de llamadas en un estado indefinido. (CVE-2010-0425): una falla en el código del proceso de solicitud secundaria puede generar información confidencial de una solicitud manejada por el subproceso incorrecto si se utiliza un entorno de subprocesos múltiples.

Solución: Actualizar Apache a la última versión disponible.

El siguiente es el diagrama de red generado a través del aplicativo Nmap:

Ilustración 22 – Diagrama e Red generado por Nmap



Fuente: Análisis aplicativo Nmap

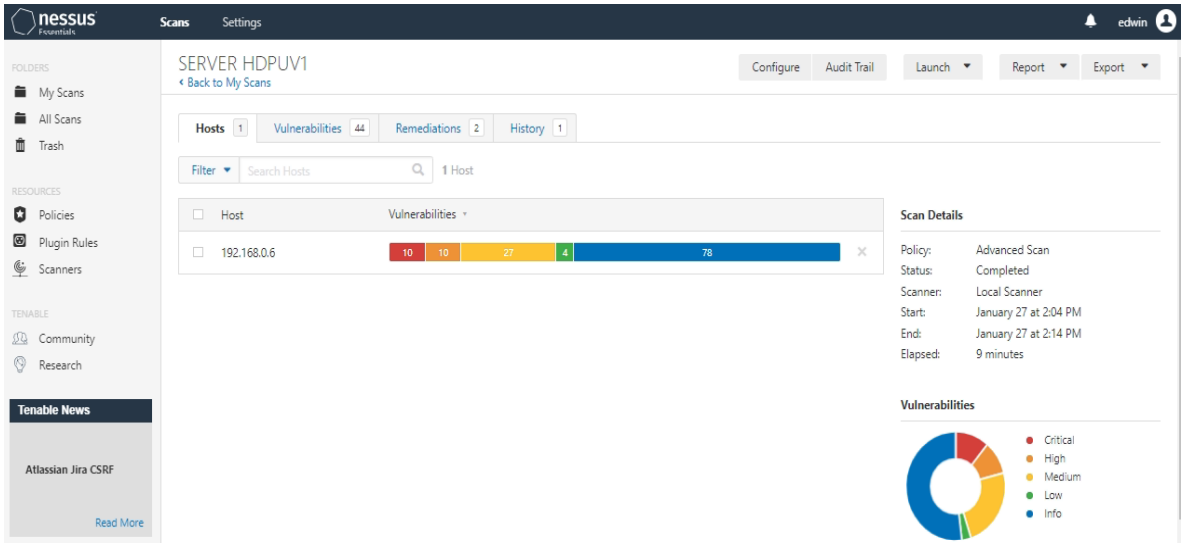
ANALISIS DE VULNERABILIDADES CON NESSUS

Nessus clasifica las vulnerabilidades según su gravedad, se derivan de la puntuación de CVSS (*El Common Vulnerability Scoring System*) que es un sistema de puntaje diseñado para proveer un método abierto y estándar que permite estimar el impacto derivado de vulnerabilidades identificadas en Tecnologías de Información, es decir, contribuye a cuantificar la severidad que pueden representar dichas vulnerabilidades, se clasifican en cinco grandes categorías:

- Vulnerabilidad de Información: con una puntuación de 0 (impacto mínimo).
- Baja: la vulnerabilidad es etiquetada como gravedad “Bajo” si tiene una puntuación base CVSS de 0.0 a 3.9.
- Medio: la vulnerabilidad es etiquetada como gravedad “Medio” si tiene una puntuación base CVSS de 4.0 a 6.9.
- Alta: la vulnerabilidad es etiquetada como gravedad “Alta” si tiene una puntuación base CVSS de 7.0 a 9.9.
- Critica: la vulnerabilidad es etiquetada como Critica si tiene una puntuación base CVSS de 10.

En la siguiente ilustración se realiza el análisis del servidor HP Proliant BL460C G5 *Server Blade* con el aplicativo nessus:

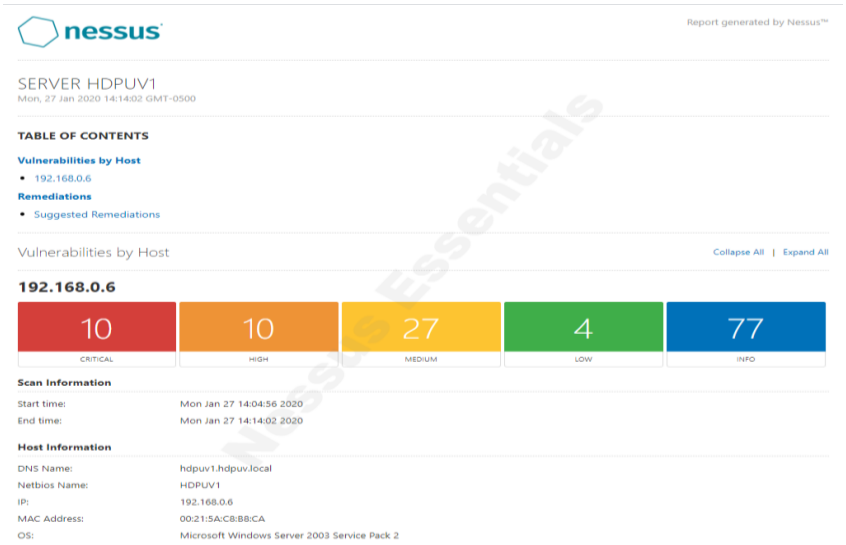
Ilustración 23–Análisis de vulnerabilidades - Servidor HP Proliant BL460C G5



Fuente: Análisis con el aplicativo Nessus

En la ilustración 24 se registra el consolidado de los datos del análisis realizado por el aplicativo Nessus al Servidor HP Proliant BL460C G5 *Server Blade* 2 con dirección IP 192.168.0.6

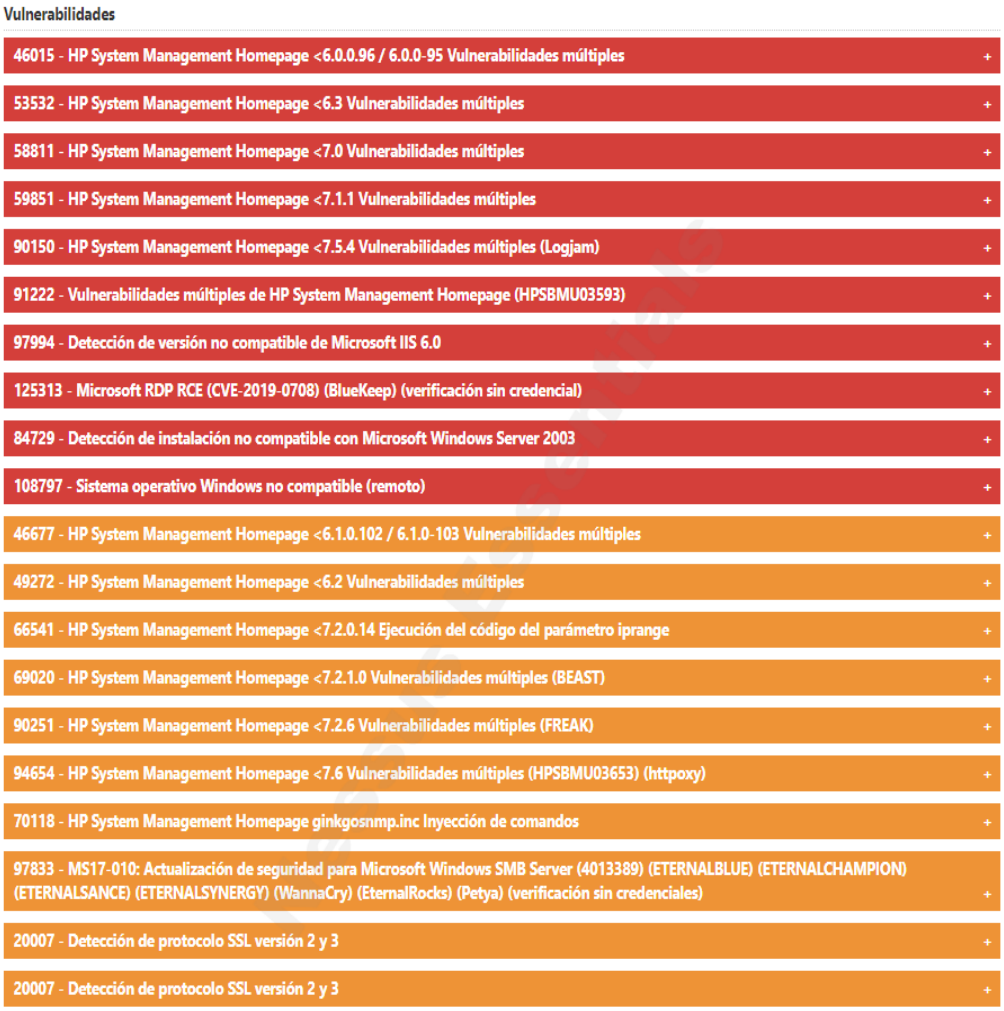
Ilustración 24–Datos consolidados del análisis - Servidor HP Proliant BL460C G5



Fuente: Análisis con el aplicativo Nessus

En la ilustración 25 se identifican las vulnerabilidades encontradas con el aplicativo Nessus al servidor HP Proliant BL460C G5 *Server Blade* 2

Ilustración 25 - Vulnerabilidades encontradas con el aplicativo Nessus - Servidor HP Proliant BL460C G5



Fuente: Análisis de vulnerabilidades con el aplicativo Nessus

Se identificaron 10 vulnerabilidades críticas, las cuales serán descritas y analizadas, y se planteara una solución para la mitigación del riesgo que representa cada una de ellas

Tabla 5 - Solución a las vulnerabilidades

VULNERABILIDAD	DESCRIPCION	SOLUCION
46015 - HP *System Management Homepage*<6.0.0.96 / 6.0.0-95 Vulnerabilidadesmúltiples	Según su número de versión auto informado, la instalación de HP *System Management Homepage* en el host remoto es anterior a 6.0.0.96 / 6.0.0-95. Dichas versiones están potencialmente afectadas por las siguientes vulnerabilidades: Una vulnerabilidad de secuencias de comandos entre sitios (XSS) debido a una falla en la desinfección de la entrada codificada UTF-7. Los navegadores solo se ven afectados si la codificación está configurada para la selección automática. (CVE-2008-1468) Un desbordamiento de enteros en la biblioteca libxml2 que puede provocar un desbordamiento del montón. (CVE-2008-4226) Un desbordamiento de búfer en la extensión mbstring de PHP. (CVE-2008-5557) Un XSS no especificado en PHP cuando *'display_errors'* está habilitado. (CVE-2008-5814) Múltiples vulnerabilidades de denegación de servicio en OpenSSL DTLS. (CVE-2009-1377, CVE-2009-1378, CVE-2009-1379, CVE-2009-1386, CVE-2009-1387) Una vulnerabilidad de secuencias de comandos entre sitios debido a una falla en la desinfección de la entrada al 'servercert' parámetro de '/ proxy / smhu / getuiinfo'. (CVE-2009-4185) Vulnerabilidad no especificada que podría permitir que un atacante acceda a información confidencial, modifique datos o provoque una denegación de servicio. (CVE-2010-1034)	Actualice a HP *System Management Homepage* 6.0.0.96 (Windows) / 6.0.0-95 (Linux) o posterior.

Tabla 5 (Continuación)

VULNERABILIDAD	DESCRIPCION	SOLUCION
53532 - HP System Management Homepage <6.3 Vulnerabilidadesmúltiples	Según el banner del servidor web, la versión de HP *System Management Homepage* (SMH) alojada en el *host* remoto es anterior a la 6.3. Dichas versiones se ven afectadas por las siguientes vulnerabilidades: - Existe un error en la función 'fnmatch' en la versión incluida de PHP que puede conducir al agotamiento de la pila. (CVE-2010-1917) - Existe una vulnerabilidad de divulgación de información en la función 'var_export' en la versión incluida de PHP que puede activarse al manejar ciertas condiciones de error. (CVE-2010-2531) - Se podría abusar de una vulnerabilidad doble libre en la función 'ssl3_get_key_exchange ()' en la biblioteca OpenSSL de terceros para bloquear la aplicación. (CVE-2010-2939) - Una vulnerabilidad de cadena de formato en la extensión phar en la versión incluida de PHP podría conducir a la divulgación del contenido de la memoria y posiblemente permitir la ejecución de código arbitrario a través de un URI 'phar: //' especialmente diseñado. (CVE-2010-2950) - Se puede abusar de una des-referencia de puntero NULL en 'ZipArchive::*getArchiveComment*' incluida con la versión incluida de PHP para bloquear la aplicación. (CVE-2010-3709) La versión incluida de libxml2 puede leer desde ubicaciones de memoria no válidas al procesar expresiones XPath con formato incorrecto, lo que da como resultado un bloqueo de la aplicación. (CVE-2010-4008)	Actualice a HP System Management Homepage 6.3 o posterior.

Tabla 5 (Continuación)

VULNERABILIDAD	DESCRIPCION	SOLUCION
58811 - HP System Management Homepage <7.0 Vulnerabilidadesmúltiples	Según el banner del servidor web, la versión de HP *System* Management *Homepage* (SMH) alojada en el host remoto es anterior a la 7.0. Como tal, según los informes, se ve afectado por las siguientes vulnerabilidades: Existe un error en la función *'generate*-id' en la biblioteca libxslt incluida que puede permitir la divulgación de direcciones de memoria de montón. (CVE-2011-0195) Existe un error de validación de entrada no especificado y puede permitir ataques de falsificación de solicitudes entre sitios. (CVE-2011-3846) Los errores no especificados pueden permitir a los atacantes realizar ataques de denegación de servicio a través de vectores no especificados. (CVE-2012-0135, CVE-2012-1993) La versión incluida de PHP contiene múltiples vulnerabilidades. (CVE-2010-3436, CVE-2010-4409, CVE-2010-4645, CVE-2011-1148, CVE-2011-1153, CVE-2011-1464, CVE-2011-1467, CVE-2011-1468, CVE -2011-1470, CVE-2011-1471, CVE-2011-1938, CVE-2011-2202, CVE-2011-2483, CVE-2011-3182, CVE-2011-3189, CVE-2011-3267, CVE-2011 -3268) Las bibliotecas OpenSSL están contenidas en varios de los componentes incluidos y contienen múltiples vulnerabilidades. (CVE-2011-0014, CVE-2011-1468, CVE-2011-1945, CVE-2011-3207, CVE-2011-3210) Las bibliotecas de rizos están contenidas en varios de los componentes incluidos y contienen múltiples vulnerabilidades. (CVE-2009-0037, CVE-2010-0734, CVE-2011-2192)	Actualice a HP System Management Homepage 7.0 o posterior.

Tabla 5 (Continuación)

VULNERABILIDAD	DESCRIPCION	SOLUCION
90150 - HP *System Management Homepage*<7.5.4 Vulnerabilidadesmúltiples (Logjam)	Según el banner del servidor web, la versión de HP *System Management Homepage* (SMH) alojada en el servidor web remoto es una versión anterior a la 7.5.4. Por lo tanto, se ve afectado por las siguientes vulnerabilidades: Existe una vulnerabilidad de denegación de servicio cuando se procesa una estructura ECParameters debido a un bucle infinito que ocurre cuando una curva específica está sobre un campo polinómico binario malformado. Un atacante remoto puede explotar esto para realizar una denegación de servicio contra cualquier sistema que procese claves públicas, solicitudes de certificados o certificados. Esto incluye clientes TLS y servidores TLS con autenticación de cliente habilitada. (CVE-2015-1788) Existe una vulnerabilidad de denegación de servicio debido a una validación incorrecta del contenido y la longitud de la cadena ASN1_TIME por la función X509_cmp_time (). Un atacante remoto puede explotar esto, a través de un certificado con formato incorrecto y CRL de varios tamaños, para causar una falla de segmentación, lo que resulta en una condición de denegación de servicio. Los clientes TLS que verifican las CRL se ven afectados. Los clientes y servidores TLS con autenticación de cliente habilitada pueden verse afectados si usan devoluciones de llamada de verificación personalizadas. (CVE-2015-1789) Existe un defecto de no referencia de puntero *NULL* en el código de análisis PKCS # 7 debido a un manejo incorrecto de 'Contenido cifrado' interno que falta. Esto permite que un atacante remoto, a través de blobs PKCS # 7 codificados con ASN.1 especialmente diseñados con contenido faltante, cause una condición de denegación de servicio u otros posibles impactos no especificados. (CVE-2015-1790)	Actualice a HP *System Management Homepage* (SMH) version 7.5.4 o posterior.

Tabla 5 (Continuación)

VULNERABILIDAD	DESCRIPCION	SOLUCION
	Existe un error de doble libre debido a una condición de carrera que ocurre cuando un cliente multiproceso recibe un *NewSessionTicket* cuando intenta reutilizar un ticket anterior. (CVE-2015-1791) Existe una vulnerabilidad de denegación de servicio en el código CMS debido a un bucle infinito que se produce al verificar un mensaje de datos firmados. Un atacante remoto puede explotar esto para causar una condición de denegación de servicio. (CVE-2015-1792)	
90150 - HP System Management Homepage <7.5.4 Vulnerabilidades múltiples (Logjam)	Existe una vulnerabilidad de omisión de validación de certificados en el subcomponente Seguridad: Cifrado debido a una falla en la función X509_verify_cert () en x509_vfy.c que se activa al localizar cadenas de certificados alternativas cuando falla el primer intento de construir una cadena de este tipo. Un atacante remoto puede explotar esto, mediante el uso de un certificado hoja válido como autoridad de certificación (CA), para emitir certificados no válidos que omitirán la autenticación. (CVE-2015-1793) Existe una vulnerabilidad de omisión de autenticación de solicitud cruzada en libcurl debido al uso de una conexión autenticada existente cuando se realiza una solicitud HTTP NTLM no autenticada posterior. Un atacante puede explotar esto para evitar los mecanismos de autenticación. (CVE-2015-3143) Existe una vulnerabilidad de denegación de servicio en libcurl debido a una falla en la función sanitize_cookie_path () que se activa al manejar un elemento de ruta de *cookie* que consiste en una comilla doble simple. Un atacante puede explotar esto para hacer que la aplicación se bloquee. (CVE-2015-3145)	Actualice a HP *System Management Homepage* (SMH) versión 7.5.4 o posterior.

Tabla 5 (Continuación)

VULNERABILIDAD	DESCRIPCION	SOLUCION
	Existe una vulnerabilidad de omisión de autenticación de solicitud cruzada en libcurl debido a una falla que se activa cuando una solicitud se 'autentica', lo que puede hacer que el programa trate la conexión completa como autenticada en lugar de solo eso solicitud específica Un atacante puede explotar esto para evitar los mecanismos de autenticación para solicitudes posteriores. (CVE-2015-3148)	
90150 - HP *System Management Homepage*<7.5.4 Vulnerabilidadesmúltiples (Logjam)	Existe una vulnerabilidad de hombre en el medio, conocida como *Logjam*, debido a una falla en el protocolo SSL / TLS. Un atacante remoto puede explotar esta falla para degradar las conexiones utilizando el intercambio de claves efímero *Diffie-Hellman* a una criptografía de grado de exportación de 512 bits. (CVE-2015-4000) Existe una falla en la función *multipart_buffer_headers* () en rfc1867.c debido a un manejo incorrecto de datos multiparte / formulario en solicitudes HTTP. Un atacante remoto puede explotar esta falla para causar un consumo de recursos de la CPU, lo que resulta en una condición de denegación de servicio. (CVE-2015-4024) Existe una falla no especificada que permite que un atacante remoto autenticado afecte la confidencialidad y la integridad. (CVE-2016-1993)	Actualice a HP *System Management Homepage* (SMH) versión 7.5.4 o posterior.
97994 - Detección de versión no compatible de Microsoft IIS 6.0	Según su número de versión auto informado, la instalación de Microsoft Internet *Information Services* (IIS) 6.0 en el host remoto ya no es compatible. La falta de soporte implica que el proveedor no lanzará nuevos parches de seguridad para el producto. Como resultado, es probable que contenga vulnerabilidades de seguridad.	Actualice a una versión de Microsoft IIS que sea compatible actualmente.

Tabla 5 (Continuación)

VULNERABILIDAD	DESCRIPCION	SOLUCION
91222 Vulnerabilidadesmúltiples de HP *System Management Homepage* (HPSBMU03593)	Según su banner, la versión de HP *System Management Homepage* (SMH) alojada en el servidor web remoto se ve afectada por las siguientes vulnerabilidades: Existe una vulnerabilidad de denegación de servicio en el servidor HTTP Apache debido a la falta del módulo *mod_reqtimeout*. Un atacante remoto no autenticado puede explotar esto, a través de una saturación de solicitudes HTTP parciales, para causar una interrupción del demonio. (CVE-2007-6750) Existe una vulnerabilidad de secuencias de comandos entre sitios (XSS) en jQuery cuando se utiliza *location.hash* para seleccionar elementos. Un atacante remoto no autenticado puede explotar esto, a través de una etiqueta especialmente diseñada, para inyectar código de script arbitrario o HTML en la sesión del navegador del usuario. (CVE-2011-4969) Existe un defecto de des-referencia de puntero NULL en el archivo *rsa_ameth.c* debido al manejo incorrecto de las firmas ASN.1 a las que les falta el parámetro PSS. Un atacante remoto puede explotar esto para hacer que la rutina de verificación de firma se bloquee, lo que resulta en una condición de denegación de servicio. (CVE-2015-3194) Existe una falla en la implementación ASN1_TFLG_COMBINE en el archivo tasn_dec.c relacionado con el manejo de estructuras X509_ATTRIBUTE mal formadas. Un atacante remoto puede explotar esto para causar una pérdida de memoria al desencadenar una falla de decodificación en una aplicación PKCS # 7 o CMS, lo que resulta en una denegación de servicio. (CVE-2015-3195)	Actualice a HP *System Management Homepage*versión 7.5.5 o posterior.

Tabla 5 (Continuación)

VULNERABILIDAD	DESCRIPCION	SOLUCION
91222 – Vulnerabilidadesmúltiples de HP *System Management Homepage* (HPSBMU03593)	Existe un error de lectura fuera de los límites en CURL y *libcurl* dentro de la función *smb_request_state* () debido a una comprobación incorrecta de los límites. Un atacante remoto no autenticado puede explotar esto, utilizando un servidor SMB malicioso y valores de longitud y desplazamiento diseñados, para revelar información confidencial de la memoria o causar una condición de denegación de servicio. (CVE-2015-3237) Existe una falla en libxslt en la función xsltStylePreCompute () dentro del archivo preproc.c debido a una falla al verificar si el nodo padre es un elemento. Un atacante remoto no autenticado puede explotar esto, a través de un archivo XML especialmente diseñado, para causar una condición de denegación de servicio. (CVE-2015-7995).	Actualice a HP *System Management Homepage*versión 7.5.5 o posterior.
84729 - Detección de instalación no compatible con Microsoft Windows Server 2003	El host remote ejecuta Microsoft Windows *Server* 2003. El soporte para este sistema operativo por parte de Microsoft finalizó el 14 de julio de 2015. La falta de soporte implica que el proveedor no lanzará nuevos parches de seguridad para el producto. Como resultado, es probable que contenga vulnerabilidades de seguridad. Además, es poco probable que Microsoft investigue o reconozca los informes de vulnerabilidades.	Actualice a una versión de Windows que sea compatible actualmente.
108797 - Sistema operativo Windows no compatible (remoto)	A la versión remota de Microsoft Windows le falta un paquete de servicio o ya no es compatible. Como resultado, es probable que contenga vulnerabilidades de seguridad.	Actualice a un paquete de servicio o sistema operativo compatible

Tabla 5 (Continuación)

VULNERABILIDAD	DESCRIPCION	SOLUCION
59851 - HP *System Management Homepage*<7.1.1 Vulnerabilidadesmúltiples	Según el banner del servidor web, la versión de HP *System Management Homepage* (SMH) alojada en el host remoto es anterior a 7.1.1 y, por lo tanto, según los informes, se ve afectada por las siguientes vulnerabilidades: La versión incluida de la biblioteca libxml2 contiene múltiples vulnerabilidades (CVE-2011-1944, CVE-2011-2821, CVE-2011-2834) La versión incluida de PHP contiene múltiples vulnerabilidades. (CVE-2011-3379, CVE-2011-4153, CVE-2011-4885, CVE-2012-1823, CVE-2012-0057, CVE-2012-0830) La versión incluida del Servidor Apache HTTP contiene múltiples vulnerabilidades. (CVE-2011-3607, CVE-2011-4317, CVE-2011-4415, CVE-2012-0021, CVE-2012-0031, CVE-2012-0053) Existe un problema en el script *'include / iniset.php'* en la versión incrustada de *Round Cube Web mail* que podría conducir a una denegación de servicio. (CVE-2011-4078) La versión incluida de OpenSSL contiene múltiples vulnerabilidades. (CVE-2011-4108, CVE-2011-4576, CVE-2011-4577, CVE-2011-4619, CVE-2012-0027, CVE-2012-1165) La versión incluida de *curl* y *libcurl* no se considera especialmente adecuada caracteres durante la extracción de un nombre de ruta desde una URL. (CVE-2012-0036) No existe un atributo de autocompletar desactivado para campos de formulario no especificados, lo que facilita a los atacantes remotos obtener acceso al aprovechar una estación de trabajo desatendida. (CVE-2012-2012)	Actualice a HP *System Management Homepage* 7.1.1 o posterior.

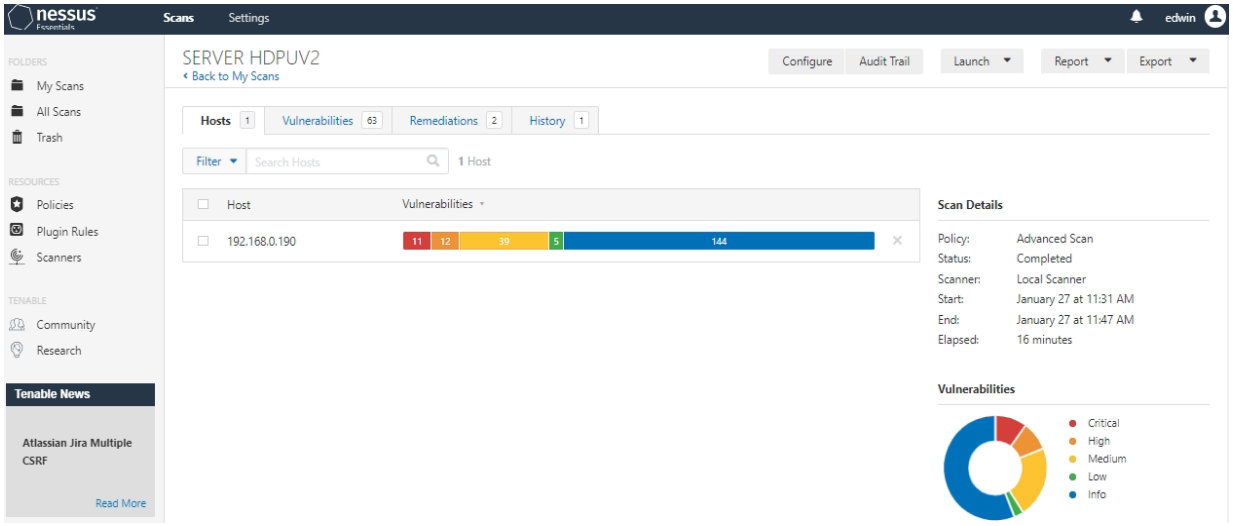
Tabla 5 (Continuación)

VULNERABILIDAD	DESCRIPCION	SOLUCION
59851 - *HP System Management Homepage*<7.1.1 Vulnerabilidadesmultiples	Existe una vulnerabilidad no especificada que podría permitir a un atacante remoto causar una denegación de servicio u obtener información confidencial o modificar datos. (CVE-2012-2013)	Actualice a HP *System Management Homepage* 7.1.1 o posterior.
125313 - Microsoft RDP RCE (CVE-2019-0708) (*BlueKeep*) (verificación sin credencial)	El host remoto se ve afectado por una vulnerabilidad de ejecución remota de código en *Remote Desktop Protocol* (RDP). Un atacante remoto no autenticado puede explotar esto, a través de una serie de solicitudes especialmente diseñadas, para ejecutar código arbitrario.	Microsoft ha lanzado un conjunto de parches para Windows XP, 2003, 2008, 7 y 2008 R2.

Fuente: Análisis de vulnerabilidades con el aplicativo Nessus

En la ilustración 26 se registra el consolidado de los datos del análisis realizado por el aplicativo Nessus al Servidor HP Proliant ML 370 con IP 192.168.0.190

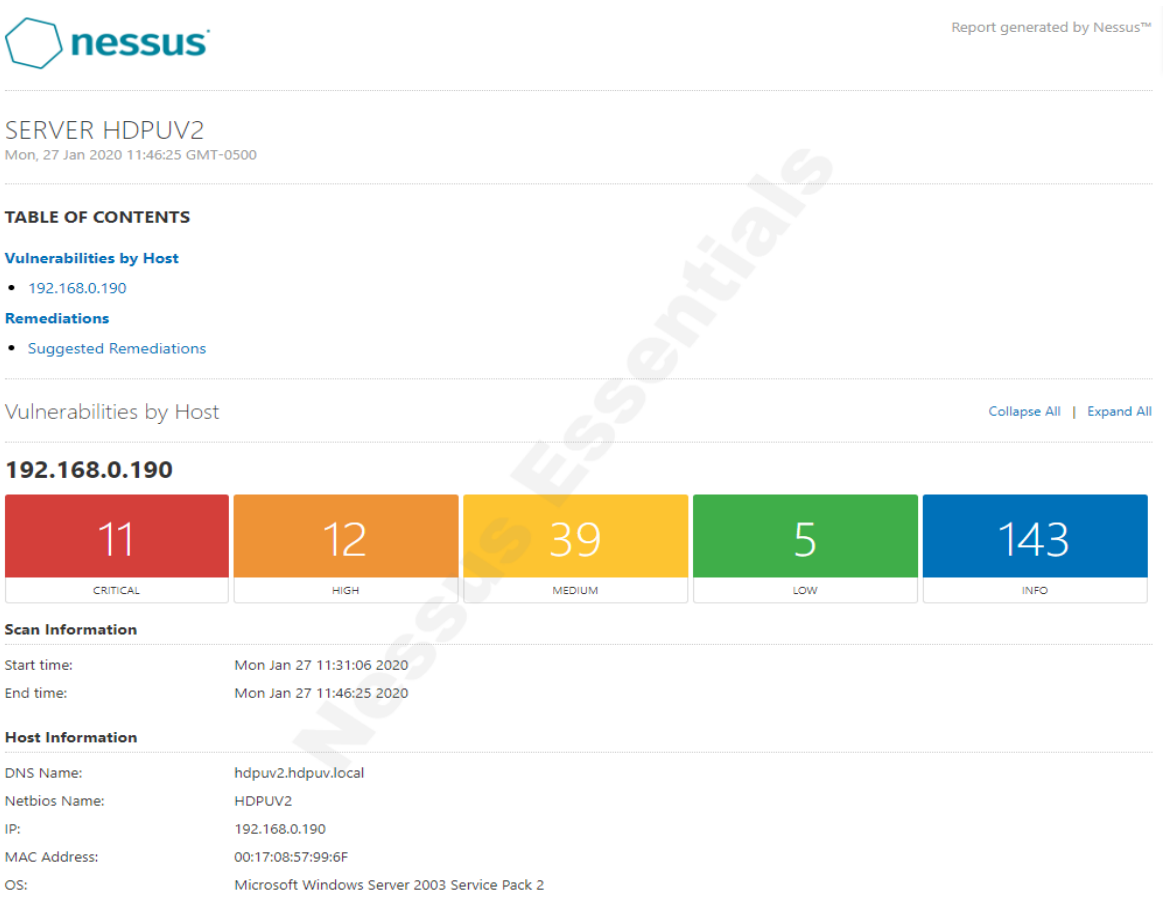
Ilustración 26–Análisis de vulnerabilidades - Servidor HP Proliant ML 370



Fuente: Análisis con el aplicativo Nessus

En la ilustración 27 se registra el consolidado de los datos del análisis realizado por el aplicativo Nessus al Servidor HP Proliant ML 370con IP 192.168.0.190.

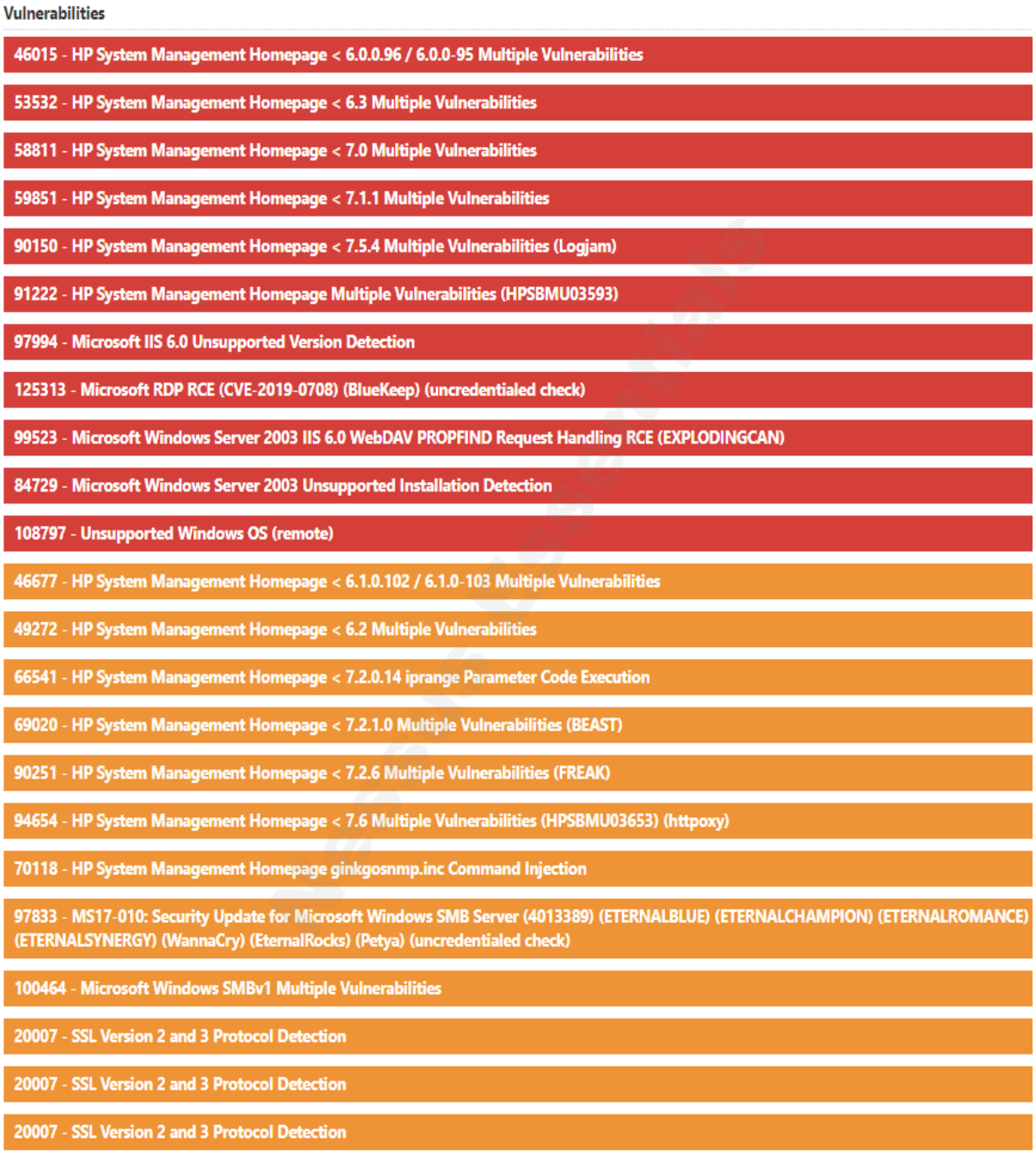
Ilustración 27 - Datos consolidados del análisis - Servidor HP Proliant ML 370



Fuente: Análisis con el aplicativo Nessus

En la ilustración 28 se identifican las vulnerabilidades encontradas con el aplicativo Nessus al servidor HP Proliant ML 370.

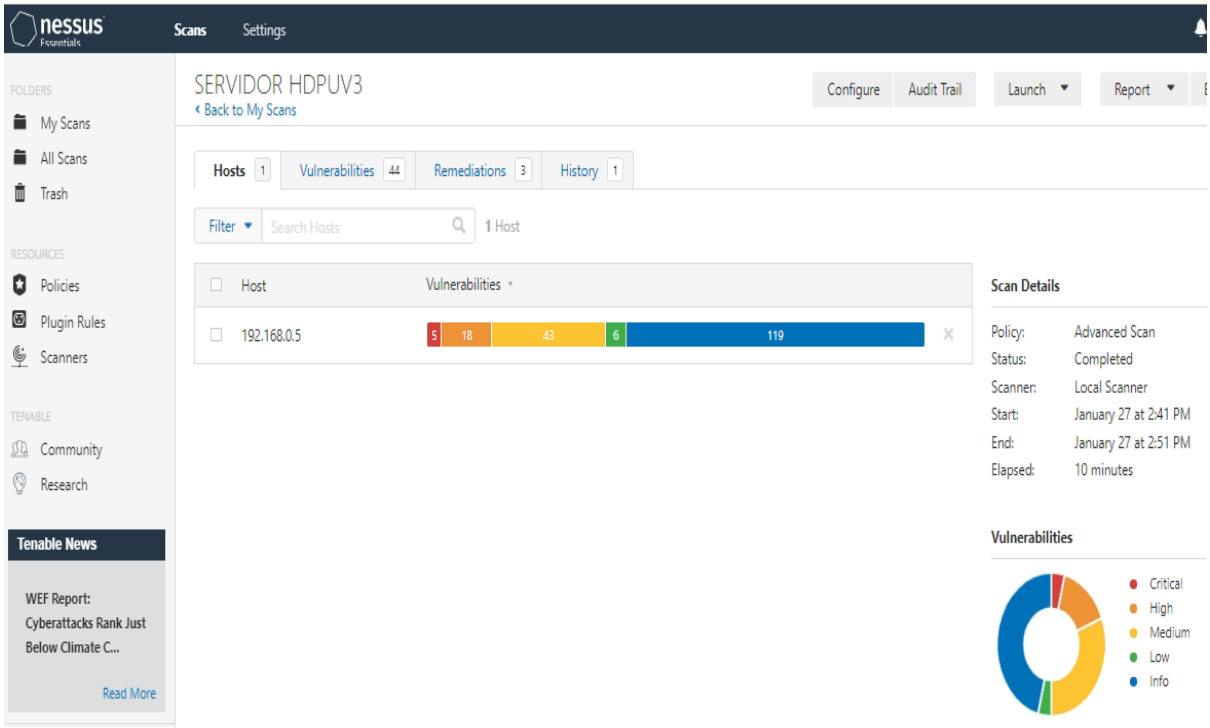
Ilustración 28 - Vulnerabilidades encontradas con el aplicativo Nessus -Servidor HP Proliant ML 370 2



Fuente: Análisis con el aplicativo Nessus

En la ilustración 29 se registra el consolidado de los datos del análisis realizado por el aplicativo Nessus al Servidor HP *Proliant* BL460C G8 Server *Blade* con dirección IP 192.168.0.5.

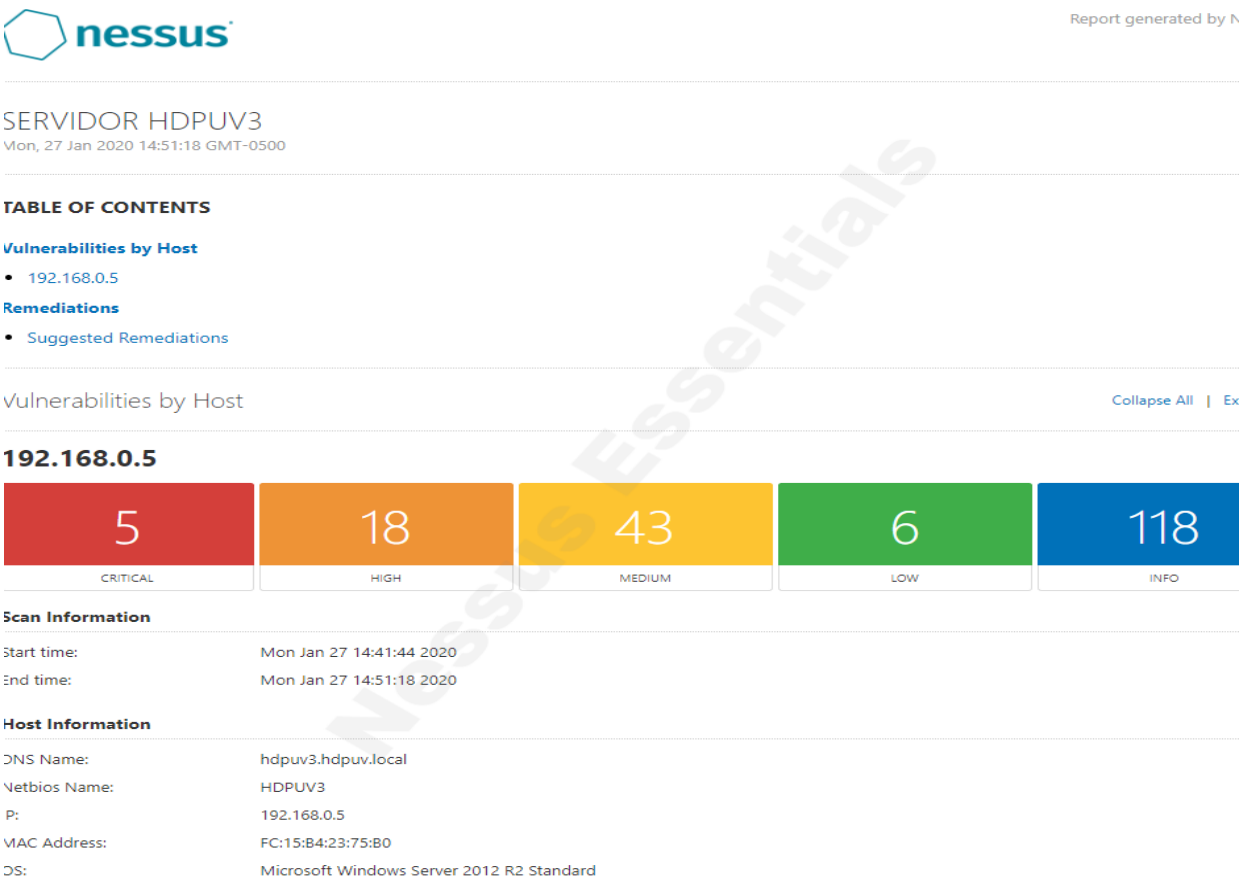
Ilustración 29- Análisis de vulnerabilidades - HP Proliant BL460C G8 *Server Blade*



Fuente: Análisis con el aplicativo Nessus

En la ilustración 30 se registra el consolidado de los datos del análisis realizado por el aplicativo Nessus al Servidor HP Proliant BL460C G8 *Server Blade* con dirección IP 192.168.0.5.

Ilustración 30 -Datos consolidados del análisis - HP Proliant BL460C G8 *Server Blade*



nessus

Report generated by N

SERVIDOR HDPUV3

Mon, 27 Jan 2020 14:51:18 GMT-0500

TABLE OF CONTENTS

Vulnerabilities by Host

- 192.168.0.5

Remediations

- Suggested Remediations

Vulnerabilities by Host

Collapse All | Ex

192.168.0.5

5	18	43	6	118
CRITICAL	HIGH	MEDIUM	LOW	INFO

Scan Information

Start time:	Mon Jan 27 14:41:44 2020
End time:	Mon Jan 27 14:51:18 2020

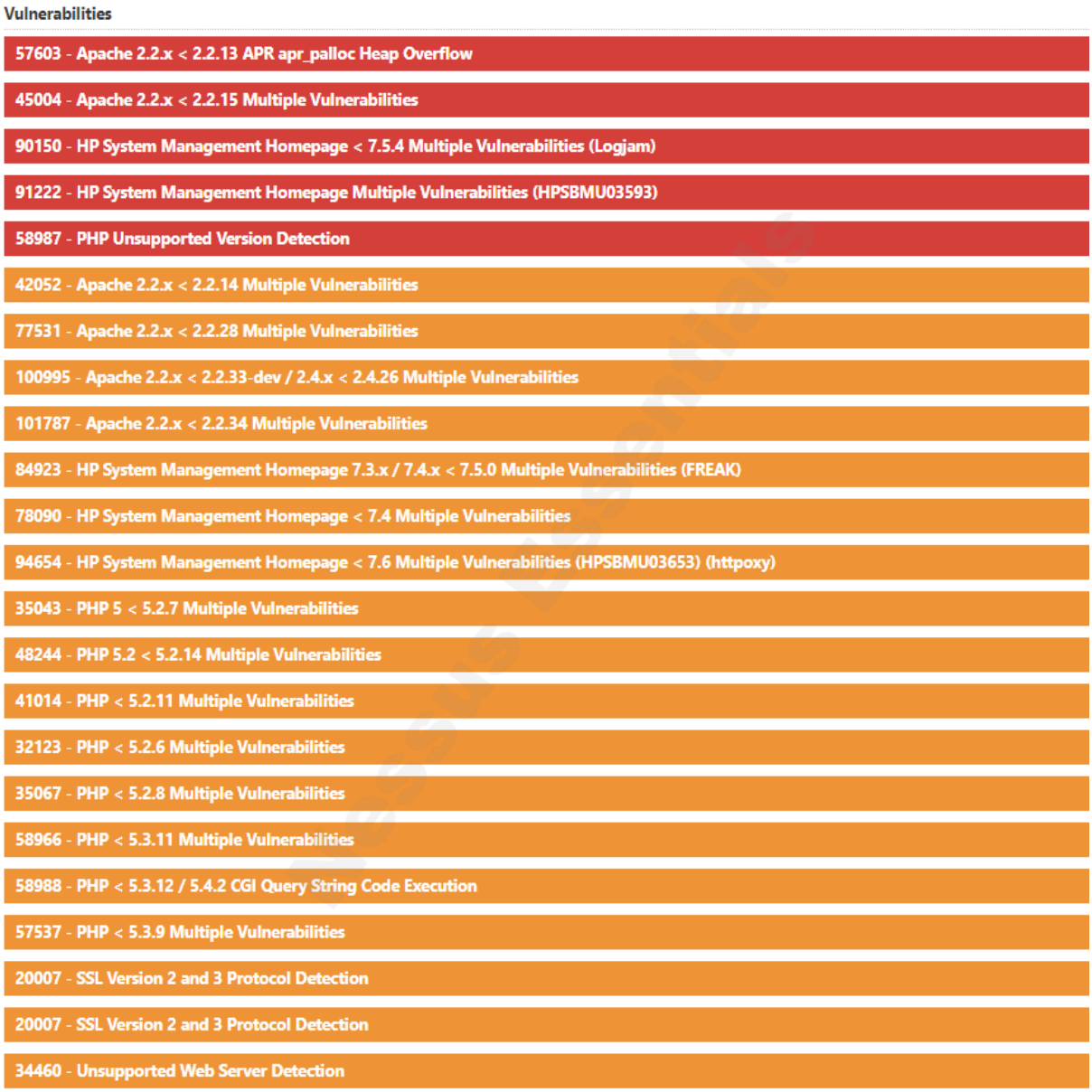
Host Information

DNS Name:	hdpuv3.hdpuv.local
Netbios Name:	HDPUV3
IP:	192.168.0.5
MAC Address:	FC:15:B4:23:75:B0
OS:	Microsoft Windows Server 2012 R2 Standard

Fuente: Análisis con el aplicativo Nessus

En la ilustración 31 se identifican las vulnerabilidades encontradas con el aplicativo Nessus al - HP Proliant BL460C G8 *Server Blade* con dirección IP 192.168.0.5

Ilustración 31 - Vulnerabilidades encontradas con el aplicativo Nessus - HP Proliant BL460C G8 *Server Blade*



Fuente: Análisis con el aplicativo Nessus

6.3 ANÁLISIS DE RIESGOS

CARACTERIZACIÓN E IDENTIFICACION DE AMENAZAS

En este apartado se identifican las amenazas a que están expuestos los activos de la empresa, para ello se utiliza la siguiente clasificación:

(A) Ataque intencionado
(E) Errores y fallos no intencionados
(I) Origen industrial
(N) Desastre natural

Tabla 6 - Análisis de Riesgos

ACTIVO	AMENAZAS
Internet	(A.10) Acceso no autorizado (E.8) Uso no controlado (E.8) Fallas en los servicios de comunicación (E.9) Averías de origen físico y/o lógico
Backup BD DGH y DGH.net	(E.5) Vulnerabilidad en el programa (E.3) Errores en la actualización (A.7) Suplantación de usuarios (E.9) Averías de origen físico y/o lógico
Backup BD Siesa Enterprise.	(E.5) Vulnerabilidad en el programa (E.3) Errores en la actualización (A.7) Suplantación de usuarios (E.9) Averías de origen físico y/o lógico
Backup BD Cguno 8.5	(E.5) Vulnerabilidad en el programa (E.3) Errores en la actualización (A.8) Suplantación de usuarios (E.5) Averías de origen físico y/o lógico
ERP SIESA ENTERPRISE.	(E.5) Vulnerabilidad en el programa (E.3) Errores en la actualización (A.7) Suplantación de usuarios (E.6) Fallas en la configuración y parámetros
DINÁMICA GERENCIAL DGH 9.0.	(E.6) Fallas en la configuración y parámetros (E.5) Vulnerabilidad en el programa (E.3) Errores en la actualización (A.7) Suplantación de usuarios

Tabla. 6 (Continuación)

ACTIVO	AMENAZA
CGUNO	(E.7) Suplantación de usuarios (E.7) Accesos no autorizados (E.7) Cambios en la parametrización e información
DGH.NET	(A.4) Accesos no autorizados, (A.3) Modificación de la información, (N.4) Desastres naturales (N.2) Daño por condiciones ambientales inadecuadas
SQL SERVER	(E.6) Inadecuada configuración (A.7) Accesos no autorizados (I.4) Averías lógicas y físicas
OUTLOOCK	(A.7) Difusión de software dañino (A.6) Filtrado de información
PAQUETE OFFICE	(I.3) Averías de origen lógico (A.6) Vulnerabilidades del programa
SITIO WEB	(A.7) Difusión de software dañino (A.7) Acceso de terceros al sistema
ESET ENDPOINT SECURITY	(A.7) Difusión de software dañino (E.4) Fallas en las actualizaciones
Servidor HP PROLIANT 370.	(D.4) Daño físico por inundaciones (D.4) Daño físico por fuego (D.4) Desastres naturales (E.3) Condiciones ambientales inadecuadas (E.4) Errores en la administración (A.4) Accesos no autorizados (E.4) Manipulación inadecuada del hardware
Servidor HP PROLIANT BL460C G5 SERVER BLADE	(D.4) Daño físico por inundaciones (D.4) Daño físico por fuego (D.4) Desastres naturales (E.3) Condiciones ambientales inadecuadas (E.4) Errores en la administración (A.4) Accesos no autorizados (E.4) Manipulación inadecuada del hardware

Tabla.6 (Continuación)

ACTIVO	AMENAZAS
hp *prodesk* 400	(D.4) Daño físico por inundaciones (D.4) Daño físico por fuego (D.4) Desastres naturales (E.3) Condiciones ambientales inadecuadas (E.4) Errores en la administración (A.4) Accesos no autorizados (E.4) Manipulación inadecuada del hardware
Switche·s	(I.4) Fallas en conexión (E.4) Fallas en configuración (A.5) Acceso no autorizado (I.4) Daño lógicos y/o físicos (D.3) Daño por agua (D.3) Daño por fuego
*Firewall*Físico (UTM SOPHOS)	(E.4) Fallas en las actualizaciones de seguridad (E.4) Condiciones ambientales inadecuadas
Servidor de almacenamiento de red NAS	(D.4) Daño físico por inundaciones (D.4) Daño físico por fuego (D.4) Desastres naturales (E.3) Condiciones ambientales inadecuadas (E.4) Errores en la administración (A.4) Accesos no autorizados (E.4) Manipulación inadecuada del hardware
Procesos Disciplinarios	(D.4) Daños por condiciones ambientales inadecuadas (A.5) Accesos no autorizados (E.5) Fallas en el almacenamiento
Historia Clínica Laboral	(D.4) Daños por condiciones ambientales inadecuadas (A.5) Accesos no autorizados (E.5) Fallas en el almacenamiento
Historias Clínicas Activas	(D.4) Daños por con|diciones ambientales inadecuadas (A.5) Accesos no autorizados (E.5) Fallas en el almacenamiento

Tabla 6. (Continuación)

ACTIVO	AMENAZA
	(D.4) Daños por condiciones ambientales inadecuadas
Cuentas por Cobrar	(A.5) Accesos no autorizados
	(E.4) Fallas en el almacenamiento
	(A.3) Alteración de la información
	(D.4) Daños por condiciones ambientales inadecuadas
Informes de Medios Magnéticos	(A.5) Accesos no autorizados
	(E.4) Fallas en el almacenamiento
	(A.3) Alteración de la información
	(D.4) Daños por condiciones ambientales inadecuadas
Historia Jurídica de Pacientes Inimputables	(A.5) Accesos no autorizados
	(E.4) Fallas en el almacenamiento
	(A.3) Alteración de la información
	(D.4) Daños por condiciones ambientales inadecuadas
Contratos	(A.5) Accesos no autorizados
	(E.4) Fallas en el almacenamiento
	(A.3) Alteración de la información
	(D.4) Daños por condiciones ambientales inadecuadas
Acciones legales	(A.5) Accesos no autorizados
	(E.4) Fallas en el almacenamiento
	(A.3) Alteración de la información
	(E.6) Caída del sistema por agotamiento del recurso.
Equipos de cómputo - Escritorio	(E.7) Privilegios de acceso inadecuados o abuso de los mismos
	(E.3) Averías de origen físico y lógico
	(D.4) Daños por agua, fuego
	(D.4) Desastres naturales |

Tabla 6 (Continuación)

ACTIVO	AMENAZA
HP PROLIANT BL460C G9 SERVER BLADE	(D.4) Daño físico por inundaciones
	(D.4) Daño físico por fuego, (D.4) Desastres naturales
	(E.3) Condiciones ambientales inadecuadas
	(E.4) Errores en la administración
	(A.4) Accesos no autorizados
HP PROLIANT DL380 G9	(D.4) Daño físico por inundaciones
	(D.4) Daño físico por fuego
	(D.4) Desastres naturales
	(E.3) Condiciones ambientales inadecuadas
	(E.4) Errores en la administración
	(A.4) Accesos no autorizados
	(E.4) Manipulación inadecuada del hardware
Hojas De Vida De Equipos Biomédicos	(D.4) Daños por condiciones ambientales inadecuadas
	(A.5) Accesos no autorizados
	(E.5) Fallas en el almacenamiento
Hojas De Vida De Equipos Industriales	(D.4) Daños por condiciones ambientales inadecuadas
	(A.5) Accesos no autorizados
	(E.5) Fallas en el almacenamiento
Historias Laborales Activos e inactivos	(D.4) Daños por condiciones ambientales inadecuadas
	(A.5) Accesos no autorizados
	(E.5) Fallas en el almacenamiento
Comprobantes de Egreso	(D.4) Daños por condiciones ambientales inadecuadas
	(A.5) Accesos no autorizados
	(E.5) Fallas en el almacenamiento

Fuente: Plataforma Documental HDPUV

6.4 VALORACIÓN DE AMENAZAS

Aquí se evalúa la probabilidad de ocurrencia para cada una de las amenazas identificadas sobre los activos de información que son más relevantes para la operación de la empresa, así como de la pérdida o degradación que se causaría sobre el activo si la amenaza identificada llegara a presentarse.

Para llevar a cabo esta valoración, se utilizan los siguientes criterios:

Tabla 7 - Pérdida o degradación del activo (D)

ITEM	ABREVIATURA
Muy alta	MA
Alta	A
Media	M
Baja	B
Muy baja	MB

Fuente: MAGERIT – versión 3.0Metodología de Análisis y Gestiónde Riesgos de los Sistemas de Información

Tabla 8 - Probabilidad (P)

ITEM	ABREVIATURA
Diaria	MA
Mensual	A
Anual	M
Cada 10 años	B
Cada Siglo	MB

Fuente: MAGERIT – versión 3.0Metodología de Análisis y Gestiónde Riesgos de los Sistemas de Información

Tabla 9 - Valoración de Amenazas

ACTIVO	AMENAZA	P	D
Internet	(A.10) Acceso no autorizado	M	A
	(E.8) Uso no controlado	A	A
	(E.8) Fallas en los servicios de comunicación	A	A
Backup BD DGH y DGH.net	(E.9) Averías de origen físico y/o lógico	M	A
	(E.5) Vulnerabilidad en el programa	M	A
	(E.3) Errores en la actualización	B	M
	(A.7) Suplantación de usuarios	M	A
Backup BD Siesa Enterprise.	(E.9) Averías de origen físico y/o lógico	M	A
	(E.5) Vulnerabilidad en el programa	M	A
	(E.3) Errores en la actualización	B	A
	(A.7) Suplantación de usuarios	M	A
Backup BD Cguno 8.5	(E.9) Averías de origen físico y/o lógico	M	A
	(E.5) Vulnerabilidad en el programa	B	A
	(E.3) Errores en la actualización	B	M
	(A.8) Suplantación de usuarios	B	A
	(E.5) Vulnerabilidad en el programa	M	A
	(E.3) Errores en la actualización	B	M
	(A.7) Suplantación de usuarios	B	A
	(E.5) Averías de origen físico y/o lógico	M	A
	(E.6) Fallas en la configuración y parámetros	M	A

Tabla 9. (Continuación)

ACTIVO	AMENAZA	P	D
DINÁMICA GERENCIAL DGH 9.0.	(E.5) Averías de origen físico y/o lógico	M	A
	(E.5) Vulnerabilidad en el programa	M	A
	(E.3) Errores en la actualización	B	M
	(A.7) Suplantación de usuarios	M	A
	(E.6) Fallas en la configuración y parámetros	M	A
CGUNO	(E.7) Suplantación de usuarios	M	A
	(E.7) Accesos no autorizados	M	A
	(E.7) Cambios en la parametrización y en la información	MB	A
DGH.NET	(A.4) Accesos no autorizados	MB	A
	(A.3) Modificación de la información	MB	A
	(N.4) Desastres naturales	M	A
	(N.2) Daño por condiciones ambientales inadecuadas	MB	A
SQL SERVER	(E.6) Inadecuada configuración	M	A
	(A.7) Accesos no autorizados	B	A
	(I.4) Averías lógicas y físicas	M	A
OUTLOOK	(A.7) Difusión de software dañino	A	B
	(A.6) Filtrado de información	A	A
PAQUETE OFFICE	(I.3) Averías de origen lógico	M	B
	(A.6) Vulnerabilidades del programa	A	B
SITIO WEB	(A.7) Difusión de software dañino	A	A
	(A.7) Acceso de terceros al sistema	M	A

Tabla 9. (Continuación)

ACTIVO	AMENAZA	P	D
ESET ENDPOINT SECURITY	(A.7) Difusión de software dañino	A	A
	(E.4) Fallas en las actualizaciones	M	A
	(D.4) Daño físico por inundaciones	B	A
	(D.4) Daño físico por fuego	B	
	(D.4) Desastres naturales	B	A
Servidor HP PROLIANT 370.	(E.3) Condiciones ambientales inadecuadas	M	A
	(E.4) Errores en la administración	M	A
	(A.4) Accesos no autorizados	M	A
	(E.4) Manipulación inadecuada del hardware	B	A
	(D.4) Daño físico por inundaciones	B	A
	(D.4) Daño físico por fuego	B	A
	(D.4) Desastres naturales	M	A
Servidor HP PROLIANT BL460C G5 SERVER BLADE	(E.3) Condiciones ambientales inadecuadas	B	A
	(E.4) Errores en la administración	M	A
	(A.4) Accesos no autorizados	M	A
	(E.4) Manipulación inadecuada del hardware	B	A
	(D.4) Daño físico por inundaciones	B	A
	(D.4) Daño físico por fuego	B	A
	(D.4) Desastres naturales	M	A
HP PROLIANT BL460C G9 SERVER BLADE	(E.3) Condiciones ambientales inadecuadas	B	A
	(E.4) Errores en la administración	M	A
	(A.4) Accesos no autorizados	M	A
	(E.4) Manipulación inadecuada del hardware	B	A

Tabla 9. (Continuación)

ACTIVO	AMENAZA	P	D
Procesos Disciplinarios	(D.4) Daños por condiciones ambientales inadecuadas	M	M
	(A.5) Accesos no autorizados	M	M
	(E.5) Fallas en el almacenamiento	B	M
Historia Clínica Laboral	(D.4) Daños por condiciones ambientales inadecuadas	M	A
	(A.5) Accesos no autorizados	M	M
	(E.5) Fallas en el almacenamiento	B	M
Historias Clínicas Activas	(D.4) Daños por condiciones ambientales inadecuadas	M	A
	(A.5) Accesos no autorizados	M	A
	(E.5) Fallas en el almacenamiento	B	M
Hojas De Vida De Equipos Biomédicos	(D.4) Daños por condiciones ambientales inadecuadas	M	A
	(A.5) Accesos no autorizados	M	A
	(E.5) Fallas en el almacenamiento	B	M
Hojas De Vida De Equipos Industriales	(D.4) Daños por condiciones ambientales inadecuadas	M	A
	(A.5) Accesos no autorizados	M	A
	(E.5) Fallas en el almacenamiento	B	M
Comprobantes de Egreso	(D.4) Daños por condiciones ambientales inadecuadas	M	A
	(A.5) Accesos no autorizados	M	A
	(E.5) Fallas en el almacenamiento	B	M
Cuentas por Cobrar	(D.4) Daños por condiciones ambientales inadecuadas	B	A
	(A.5) Accesos no autorizados	M	A
	(E.4) Fallas en el almacenamiento (A.3) alteración de información	B	M

Tabla 9. (Continuación)

ACTIVO	AMENAZA	P	D
Informes de Medios Magnéticos	(D.4) Daños por condiciones ambientales inadecuadas	B	A
	(A.5) Accesos no autorizados	M	A
	(E.4) Fallas en el almacenamiento	B	M
Historia Jurídica de Pacientes Inimputables	(A.3) Alteración de la información	M	A
	(D.4) Daños por condiciones ambientales inadecuadas	B	A
	(A.5) Accesos no autorizados	M	A
	(E.4) Fallas en el almacenamiento	M	M
Contratos	(A.3) Alteración de la información	M	A
	(D.4) Daños por condiciones ambientales inadecuadas	B	A
	(A.5) Accesos no autorizados	M	A
	(E.4) Fallas en el almacenamiento	M	M
Acciones legales	(A.3) Alteración de la información	M	A
	(D.4) Daños por condiciones ambientales inadecuadas	B	A
	(A.5) Accesos no autorizados	M	A
	(E.4) Fallas en el almacenamiento	M	M
Equipos de cómputo - Escritorio	(A.3) Alteración de la información	M	A
	(E.6) Caída del sistema por agotamiento del recurso	A	A
	(E.7) Privilegios de acceso inadecuados o abuso de los mismos	M	A
	(E.3) Averías de origen físico y lógico	M	A
	(D.4) Daños por agua, fuego	B	B
	(D.4) Desastres naturales	M	B

Fuente: Plataforma documental HDPUV

6.5 DETERMINACIÓN DEL RIESGO POTENCIAL

Ilustración 32 – Determinación Riesgo Potencial

riesgo		*probabilidad*				
		MB	B	M	A	MA
impacto	MA	A	MA	MA	MA	MA
	A	M	A	A	MA	MA
	M	B	M	M	A	A
	B	MB	B	B	M	M
	MB	MB	MB	MB	B	B

Fuente: MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información

Tabla 10- Riesgo Potencial

ACTIVO	AMENAZA	P	D	R
Internet	(A.10) Acceso no autorizado	M	A	A
	(E.8) Uso no controlado	A	A	MA
	(E.8) Fallas en los servicios de comunicación	A	A	MA
Backup BD DGH y DGH.net	(E.9) Averías de origen físico y/o lógico	M	MA	MA
	(E.5) Vulnerabilidad en el programa	M	A	A
	(E.3) Errores en la actualización	B	M	M
	(A.7) Suplantación de usuarios	M	A	A
Backup BD Siesa Enterprise.	(E.9) Averías de origen físico y/o lógico	M	MA	MA
	(E.5) Vulnerabilidad en el programa	M	A	A
	(E.3) Errores en la actualización	B	A	A
	(A.7) Suplantación de usuarios	M	A	A

Tabla 10. (Continuación)

ACTIVO	AMENAZA	P	D	R
Backup BD Cguno 8.5	(E.9) Averías de origen físico y/o lógico	M	MA	MA
	(E.5) Vulnerabilidad en el programa	B	A	A
	(E.3) Errores en la actualización	B	M	M
	(A.8) Suplantación de usuarios	B	A	A
ERP SIESA ENTERPRISE.	(E.5) Averías de origen físico y/o lógico	M	A	MA
	(E.5) Vulnerabilidad en el programa	M	A	A
	(E.3) Errores en la actualización	B	M	M
	(A.7) Suplantación de usuarios	B	A	A
	(E.6) Fallas en la configuración y parámetros	M	A	A
DINÁMICA GERENCIAL DGH 9.0.	(E.5) Averías de origen físico y/o lógico	M	A	MA
	(E.5) Vulnerabilidad en el programa	M	A	A
	(E.3) Errores en la actualización	B	M	M
	(A.7) Suplantación de usuarios	M	A	A
	(E.6) Fallas en la configuración y parámetros	M	A	A
CGUNO	(E.7) Suplantación de usuarios	M	A	A
	(E.7) Accesos no autorizados	M	A	A
	(E.7) Cambios en la parametrización y en la información	MB	A	M
DGH.NET	(A.4) Accesos no autorizados	MB	A	M
	(A.3) Modificación de la información	MB	A	M
	(N.4) Desastres naturales	M	A	A
	(N.2) Daño por condiciones ambientales inadecuadas	MB	A	M
SQL SERVER	(E.6) Inadecuada configuración	M	A	A
	(A.7) Accesos no autorizados	B	A	A
	(I.4) Averías lógicas y físicas	M	A	A
OUTLOOK	(A.7) Difusión de software dañino	A	B	M
	(A.6) Filtrado de información	A	A	MA
PAQUETE OFFICE	(I.3) Averías de origen lógico	M	B	B
	(A.6) Vulnerabilidades del programa	A	B	M

Tabla 10. (Continuación)

ACTIVO	AMENAZA	P	D	R
SITIO WEB	(A.7) Difusión de software dañino	A	A	MA
	(A.7) Acceso de terceros al sistema	M	A	A
ESET ENDPOINT SECURITY	(A.7) Difusión de software dañino	A	A	MA
	(E.4) Fallas en las actualizaciones	M	A	A
Servidor HP PROLIANT 370.	(D.4) Daño físico por inundaciones	B	MA	MA
	(D.4) Daño físico por fuego	B		A
	(D.4) Desastres naturales	B	A	A
	(E.3) Condiciones ambientales inadecuadas	M	A	A
	(D.3) Daño por agua	B	A	A
	(E.4) Errores en la administración	M	A	A
	(A.4) Accesos no autorizados	M	A	A
	(E.4) Manipulación inadecuada del hardware	B	A	A
Servidor HP PROLIANT BL460C G5	(D.4) Daño físico por inundaciones	B	A	A
	(D.4) Daño físico por fuego	B	A	A
	(D.4) Desastres naturales	M	A	A
	(E.3) Condiciones ambientales inadecuadas	B	A	A
	(E.4) Errores en la administración	M	A	A
	(A.4) Accesos no autorizados	M	A	A
	(E.4) Manipulación inadecuada del hardware	B	A	A
HP PROLIANT BL460C G9 SERVER BLADE	(D.4) Daño físico por inundaciones	B	A	A
	(D.4) Daño físico por fuego	B	A	A
	(D.4) Desastres naturales	M	A	A
	(E.3) Condiciones ambientales inadecuadas	B	A	A
	(E.4) Errores en la administración	M	A	A
	(A.4) Accesos no autorizados	M	A	A
	(E.4) Manipulación inadecuada del hardware	B	A	A

Tabla 10. (Continuación)

ACTIVO	AMENAZA	P	D	R
HP PROLIANT DL380 G9	(D.4) Daño físico por inundaciones	B	A	A
	(D.4) Daño físico por fuego	B	A	A
	(D.4) Desastres naturales	M	A	A
	(E.3) Condiciones ambientales inadecuadas	B	A	A
	(E.4) Errores en la administración	M	A	A
	(A.4) Accesos no autorizados	M	A	A
	(E.4) Manipulación inadecuada del hardware	B	A	A
hp prodesck 400	(D.4) Daño físico por inundaciones	B	A	A
	(D.4) Daño físico por fuego	B	A	A
	(D.4) Desastres naturales	M	A	A
	(E.3) Condiciones ambientales inadecuadas	B	A	A
	(E.4) Errores en la administración	M	A	A
	(A.4) Accesos no autorizados	M	A	A
	(E.4) Manipulación inadecuada del hardware	B	A	A
Switche·s	(I.4) Fallas en conexión	B	M	M
	(E.4) Fallas en configuración	M	B	B
	(A.5) Acceso no autorizado	B	A	A
	(I.4) Daño lógicos y/o físicos	A	M	A
	(D.3) Daño por agua	B	M	M
	(D.3) Daño por fuego	MB	M	B
Firewall Fisico (UTM SOPHOS)	(E.4) Fallas en las actualiz. de seguridad	M	A	A
	(E.4) Condiciones ambientales inadecuadas	B	B	B
Servidor de almacenamiento de red NAS	(D.4) Daño físico por inundaciones	B	A	A
	(D.4) Daño físico por fuego	B	A	A
	(D.4) Desastres naturales	M	A	A
	(E.3) Condiciones ambientales inadecuad.	B	A	A
	(E.4) Errores en la administración	M	A	A
	(A.4) Accesos no autorizados	M	A	A
	(E.4) Manipulación inadecuada del hardware	B	M	M

Tabla 10. (Continuación)

ACTIVO	AMENAZA	P	D	R
Procesos Disciplinarios	(D.4) Daños por condiciones ambientales inadecuadas	M	M	M
	(A.5) Accesos no autorizados	M	M	M
	(E.5) Fallas en el almacenamiento	B	M	M
Historia Clínica Laboral	(D.4) Daños por condiciones ambientales inadecuadas	M	A	A
	(A.5) Accesos no autorizados	M	M	M
	(E.5) Fallas en el almacenamiento	B	M	M
Historias Clínicas Activas	(D.4) Daños por condiciones ambientales inadecuadas	M	A	A
	(A.5) Accesos no autorizados	M	A	A
	(E.5) Fallas en el almacenamiento	B	M	M
Hojas De Vida De Equipos Biomédicos	(D.4) Daños por condiciones ambientales inadecuadas	M	A	A
	(A.5) Accesos no autorizados	M	A	A
	(E.5) Fallas en el almacenamiento	B	M	M
Hojas De Vida De Equipos Industriales	(D.4) Daños por condiciones ambientales inadecuadas	M	A	A
	(A.5) Accesos no autorizados	M	A	A
	(E.5) Fallas en el almacenamiento	B	M	M
Historias Laborales Activos e inactivos	(D.4) Daños por condiciones ambientales inadecuadas	M	A	A
	(A.5) Accesos no autorizados	M	A	A
	(E.5) Fallas en el almacenamiento	B	M	M
Comprobantes de Egreso	(D.4) Daños por condiciones ambientales inadecuadas	M	A	A
	(A.5) Accesos no autorizados	M	A	A
	(E.5) Fallas en el almacenamiento	B	M	M
Cuentas por Cobrar	(D.4) Daños por condiciones ambientales inadecuadas	B	A	A
	(A.5) Accesos no autorizados	M	A	A
	(E.4) Fallas en el almacenamiento	B	M	M
	(A.3) Alteración de la información	M	A	A

Tabla 10. (Continuación)

ACTIVO	AMENAZA	P	D	R
Informes de Medios Magnéticos	(D.4) Daños por condiciones ambientales inadecuadas	B	A	A
	(A.5) Accesos no autorizados	M	A	A
	(E.4) Fallas en el almacenamiento	B	M	M
Historia Jurídica de Pacientes Inimputables	(A.3) Alteración de la información	M	A	A
	(D.4) Daños por condiciones ambientales inadecuadas	B	A	A
	(A.5) Accesos no autorizados	M	A	A
	(E.4) Fallas en el almacenamiento	M	M	M
Contratos	(A.3) Alteración de la información	M	A	A
	(D.4) Daños por condiciones ambientales inadecuadas	B	A	A
	(A.5) Accesos no autorizados	M	A	A
	(E.4) Fallas en el almacenamiento	M	M	M
Acciones legales	(A.3) Alteración de la información	M	A	A
	(D.4) Daños por condiciones ambientales inadecuadas	B	A	A
	(A.5) Accesos no autorizados	M	A	A
	(E.4) Fallas en el almacenamiento	M	M	M
Equipos de cómputo - Escritorio	(A.3) Alteración de la información	M	A	A
	(E.6) Caída del sistema por agotamiento del recurso	A	A	MA
	(E.7) Privilegios de acceso inadecuados o abuso de los mismos	M	A	A
	(E.3) Averías de origen físico y lógico	M	A	A
	(D.4) Daños por agua, fuego	B	B	B
	(D.4) Desastres naturales	M	B	B

Fuente: Plataforma Documental HDPUV

7. SALVAGUARDAS

7.1 CARACTERIZACIÓN DE LAS SALVAGUARDAS

En este ítem se definen las medidas que se implementan para reducir el riesgo. Son aquellas metodologías, políticas, procedimientos y/o elementos que deben adoptarse para que la empresa se encuentre con una protección razonable para sus activos de información.

A continuación, se hace una descripción de las salvaguardas establecidas por la empresa para la protección de sus activos, identificando y valorando las mismas.

Protección general de los activos

Propias de todos los activos, se identifican las salvaguardas que son transversales y que aplican independientemente del activo que se trate.

Autorización de Acceso

Hace referencia a la restricción que se implementa para el acceso tanto en datos, servicios, aplicaciones, equipos, redes y soporte de información. Se controla el personal que tiene acceso a estos medios y, el alcance que se le permite en cada uno de ellos. Con esto se protege la integridad y confidencialidad.

Este se enfoca en la protección de las amenazas:

- Acceso no autorizado
- Suplantación de usuarios

- Cambios en la parametrización y en la información
- Modificación de la información
- Filtrado de información
- Acceso de terceros al sistema
- Errores en la administración
- Alteración de la información
- Privilegios de acceso inadecuados o abuso de los mismos

Filtración contra códigos maliciosos

Hace referencia a que se pongan en marcha de manera controlada las herramientas que posee la empresa para detectar los códigos maliciosos que quieran ser incluidos en los sistemas. Mantener en constante actualización, para contar con lo último en códigos de protección. Esto solo aplica sobre el software, por lo que debe mantenerse actualizado, tanto la herramienta antivirus como el sistema de defensa y arranque del sistema. Asegura la confidencialidad y disponibilidad de la información.

Esta salvaguarda protege contra las amenazas de:

- Vulnerabilidad en el programa
- Errores en la actualización
- Accesos no autorizados
- Difusión de software dañino
- Filtrado de información
- Vulnerabilidades del programa
- Acceso de terceros al sistema
- Fallas en las actualizaciones de seguridad

Protección de instalación de software y aplicaciones

La empresa está en proceso de actualización de su política de seguridad de la información. Esto conlleva a que está en proceso de establecer mejores controles para restringir el uso de software no autorizado por la empresa y la descarga de aplicaciones que pueden llegar a ser potencialmente peligrosas para los sistemas de información. Se asegura así la confidencialidad e integridad.

Esto exige que se lleve estricto control de las actualizaciones del sistema, la persona responsable de esto y los tiempos en que se realiza.

Esta salvaguarda apunta a las siguientes amenazas:

- Acceso no autorizado
- Uso no controlado
- Errores en la actualización
- Difusión de software dañino
- Filtrado de información
- Acceso de terceros al sistema
- Fallas en las actualizaciones
- Daños lógicos y/o físicos
- Fallas en las actualizaciones de seguridad

Protección de equipos

Se debe implementar y aplicar los perfiles para el ingreso a los equipos, protección física de los mismos y uso de medios extraíbles. Una herramienta que permite configurar esto es el directorio activo, que puede ser una opción para el control con

políticas aplicables a todos los equipos que deben incluirse en la red. Con esto se protege la integridad, confidencialidad y autenticidad en los activos de información. Sin embargo, este directorio activo se encuentra alojado en un Windows server 2003 para lo cual se debe realizar actualización.

Esta salvaguarda cubre las amenazas de:

- Acceso no autorizado
- Errores en la administración

Protección de comunicaciones

La empresa debe robustecer el control sobre la red que administra sus sistemas de información, implementando perfiles, haciendo seguimiento al uso de la red, controlando IP de conexión para cada usuario o grupo de usuarios. Para el acceso a internet se debe garantizar un control de filtrado, configurar navegadores, restringir descargas, monitorear tráfico, instalar anti-spyware y controlar dispositivos que permitan navegación.

Con esto se controla la autenticidad, confidencialidad e integridad y se hace frente a la amenaza de:

- Accesos no autorizados
- Uso no controlado
- Difusión de software dañino

Protección física

Todos los equipos y herramientas (incluidos servidores, *switch* y demás) deben tener una protección no solo contra el acceso de terceros, sino contra las condiciones del medio en el que se encuentran o instalan. Por eso se recomienda validar las condiciones locativas, la seguridad física de las instalaciones y establecer la metodología para el ingreso y salida del personal, en función de validar que la información permanezca en la empresa.

Con esto se guarda la confidencialidad de la información y se cubren las amenazas de:

- Averías de origen físico y/o lógico
- Accesos no autorizados
- Daño por condiciones ambientales inadecuadas
- Averías lógicas y físicas
- Acceso de terceros al sistema
- Daño físico por inundaciones
- Daño físico por fuego
- Daño por agua
- Daño por fuego

Protección de instalaciones

Disponer de norma de seguridad para las instalaciones, áreas específicas para la custodia de equipos y archivos digitales y físicos, protección perimetral.

Este ítem, hace frente a las amenazas de:

- Acceso no autorizado
- Acceso de terceros al sistema

Mantenimientos

No solo se debe velar por el mantenimiento físico de las instalaciones, se debe implementar plan y cronograma para el mantenimiento lógico de los sistemas de información, es decir mantener las aplicaciones actualizadas, los equipos y servidores en las capacidades que deben estar acordes a las actividades que se realizan.

Con esto la empresa cubre las amenazas de:

- Fallas en la configuración y parámetros
- Desastres naturales
- Averías lógicas y físicas
- Caída del sistema por agotamiento del recurso.

Tabla 11 - Salvaguardas

ACTIVO	AMENAZAS	SALVAGUARDAS
Internet	(A.10) Acceso no autorizado (E.8) Uso no controlado (E.8) Fallas en los servicios de comunicación	Control de acceso lógico y físico Dispositivos de seguridad perimetral. Canal de Backups

Tabla 11 – (Continuación)

ACTIVO	AMENAZA	SALVAGUARDAS
Backup BD DGH y DGH.net	(E.9) Averías de origen físico y/o lógico	Política de *Backups*.
	(E.5) Vulnerabilidad en el programa	Proceso de gestión de cambios documentado
	(E.3) Errores en la actualización	Plan de contingencia documentado y actualizado
	(A.7) Suplantación de usuarios	Control de acceso lógico y físico
Backup BD Siesa Enterprise.	(E.9) Averías de origen físico y/o lógico	Política de Backus.
	(E.5) Vulnerabilidad en el programa	Proceso de gestión de cambios documentado
	(E.3) Errores en la actualización	Plan de contingencia documentado y actualizado
	(A.7) Suplantación de usuarios	Control de acceso lógico y físico
Backup BD Cguno 8.5	(E.9) Averías de origen físico y/o lógico	Política de *Backups*.
	(E.5) Vulnerabilidad en el programa	Proceso de gestión de cambios documentado
	(E.3) Errores en la actualización	Plan de contingencia documentado y actualizado
	(A.8) Suplantación de usuarios	Control de acceso lógico y físico
ERP SIESA ENTERPRISE.	(E.5) Averías de origen físico y/o lógico	Contrato de Mantenimiento con Proveedor
	(E.5) Vulnerabilidad en el programa	Proceso de gestión de cambios documentado
	(E.3) Errores en la actualización	Plan de contingencia documentado y actualizado
	(A.7) Suplantación de usuarios	Control de acceso lógico y físico
	(E.6) Fallas en la configuración y parámetros	Plan de contingencia documentado y actualizado
DINÁMICA GERENCIAL DGH 9.0.	(E.5) Averías de origen físico y/o lógico	Contrato de Mantenimiento con Proveedor
	(E.5) Vulnerabilidad en el programa	Proceso de gestión de cambios documentado

Tabla 11. (Continuación)

ACTIVO	AMENAZA	SALVAGUARDA
CGUNO	(E.7) Suplantación de usuarios	Control de acceso lógico y físico
	(E.7) Accesos no autorizados	Política de gestión de usuarios.
	(E.7) Cambios en la parametrización y en la información	Políticas Institucionales de manejo de Información y sistemas de información
DGH.NET	(A.4) Accesos no autorizados	Política de gestión de usuarios.
	(A.3) Modificación de la información	Políticas Institucionales de manejo de Información y sistemas de información
	(N.4) Desastres naturales	Seguros contra desastres naturales
SQL SERVER	(E.6) Inadecuada configuración	Política de *Backups*.
	(A.7) Accesos no autorizados	Control de acceso lógico y físico
	(I.4) Averías lógicas y físicas	Aseguramiento de la disponibilidad, Sistemas redundantes.
OUTLOOK	(A.7) Difusión de software dañino	Plataforma de seguridad perimetral y Antivirus.
	(A.6) Filtrado de información	Acuerdos de Confidencialidad, manual de uso de recursos informáticos
PAQUETE OFFICE	(I.3) Averías de origen lógico	Mantenimiento a Software.
	(A.6) Vulnerabilidades del programa	Sistemas Actualizados
SITIO WEB	(A.7) Difusión de software dañino	Plataforma de seguridad perimetral y Antivirus.
	(A.7) Acceso de terceros al sistema	Control de acceso lógico.
ESET ENDPOINT SECURITY	(A.7) Difusión de software dañino	Acuerdos de Confidencialidad, manual de uso de recursos informáticos.
	(E.4) Fallas en las actualizaciones	Entornos de prueba de software.

Tabla 11. (Continuación)

ACTIVO	AMENAZA	SALVAGUARDA
Servidor HP PROLIANT 370.	(D.4) Daño físico por inundaciones	Sensores ambientales (humo, humedad y temperatura), Plan de contingencia.
	(D.4) Daño físico por fuego	Sensores ambientales (humo, humedad y temperatura), Plan de contingencia.
	(D.4) Desastres naturales	Sensores ambientales (humo, humedad y temperatura), Plan de contingencia.
	(E.3) Condiciones ambientales inadecuadas	Sensores ambientales (humo, humedad y temperatura), Plan de contingencia.
	(E.4) Errores en la administración	Manual de configuraciones.
	(A.4) Accesos no autorizados	Control de acceso lógico y físico
	(E.4) Manipulación inadecuada del hardware	Plan de contingencia documentado y actualizado
Servidor HP PROLIANT BL460C G5 SERVER BLADE	(D.4) Daño físico por inundaciones	Sensores ambientales (humo, humedad y temperatura), Plan de contingencia.
	(D.4) Daño físico por fuego	Sensores ambientales (humo, humedad y temperatura), Plan de contingencia.
	(D.4) Desastres naturales	Sensores ambientales (humo, humedad y temperatura), Plan de contingencia.
	(E.3) Condiciones ambientales inadecuadas	Sensores ambientales (humo, humedad y temperatura), Plan de contingencia.
	(E.4) Errores en la administración	Manual de configuraciones.
	(A.4) Accesos no autorizados	Control de acceso lógico y físico
	(E.4) Manipulación inadecuada del hardware	Plan de contingencia documentado y actualizado

Tabla 11. (Continuación)

ACTIVO	AMENAZA	SALVAGUARDA
HP PROLIANT DL380 G9	(D.4) Daño físico por inundaciones	Sensores ambientales (humo, humedad y temperatura), Plan de contingencia.
	(D.4) Daño físico por fuego	Sensores ambientales (humo, humedad y temperatura), Plan de contingencia.
	(D.4) Desastres naturales	Sensores ambientales (humo, humedad y temperatura), Plan de contingencia.
	(E.3) Condiciones ambientales inadecuadas	Sensores ambientales (humo, humedad y temperatura), Plan de contingencia.
	(E.4) Errores en la administración	Manual de configuraciones.
	(A.4) Accesos no autorizados	Control de acceso lógico y físico
	(E.4) Manipulación inadecuada del hardware	Plan de contingencia documentado y actualizado
HP *prodesk* 400	(D.4) Daño físico por inundaciones	Sensores ambientales (humo, humedad y temperatura), Plan de contingencia.
	(D.4) Daño físico por fuego	Sensores ambientales (humo, humedad y temperatura), Plan de contingencia.
	(D.4) Desastres naturales	Sensores ambientales (humo, humedad y temperatura), Plan de contingencia.
	(E.3) Condiciones ambientales inadecuadas	Sensores ambientales (humo, humedad y temperatura), Plan de contingencia.
	(E.4) Errores administrativos	Manual de configuraciones.
DINÁMICA GERENCIAL DGH 9.0.	(A.4) Accesos no autorizados	Control de acceso lógico y físico.
	(E.4) Manipulación inadecuada del hardware	Plan de contingencia documentado y actualizado.

Tabla 11. (Continuación)

ACTIVO	AMENAZA	SALVAGUARDA
Switches	(I.4) Fallas en conexión	Consola de administración configurada.
	(E.4) Fallas en configuración	Manual de configuraciones.
	(A.5) Acceso no autorizado	Control de acceso lógico y físico
	(I.4) Daño lógicos y/o físicos	Plan de contingencia de TI.
	(D.3) Daño por agua	Sensores ambientales (humo, humedad y temperatura), Plan de contingencia.
	(D.3) Daño por fuego	Sensores ambientales (humo, humedad y temperatura), Plan de contingencia.
Firewall Físico (UTM SOPHOS)	(E.4) Fallas en las actualizaciones de seguridad	*Backup* periódico de configuración.
	(E.4) Condiciones ambientales inadecuadas	Sensores ambientales (humo, humedad y temperatura), Plan de contingencia.
	(D.4) Daño físico por inundaciones	Sensores ambientales (humo, humedad y temperatura), Plan de contingencia.
	(D.4) Daño físico por fuego	Sensores ambientales (humo, humedad y temperatura), Plan de contingencia.
	(D.4) Desastres naturales	Sensores ambientales (humo, humedad y temperatura), Plan de contingencia.
Servidor de almacenamiento de red NAS	(E.3) Condiciones ambientales inadecuadas	Sensores ambientales (humo, humedad y temperatura), Plan de contingencia.
	(E.4) Errores administración	Manual de configuraciones.
	(A.4) Accesos no autorizados	Control de acceso lógico y físico
	(E.4) Manipulación inadecuada del hardware	Plan de contingencia documentado y actualizado.

Tabla 11. (Continuación)

ACTIVO	AMENAZA	SALVAGUARDA
Procesos Disciplinarios	(D.4) Daños por condiciones ambientales inadecuadas	Sensores ambientales (humo, humedad y temperatura), Plan de contingencia.
	(A.5) Accesos no autorizados	Control de acceso lógico y físico
	(E.5) Fallas en el almacenamiento	Política de *Backups* establecidas y socializadas.
Historia Clínica Laboral	(D.4) Daños por condiciones ambientales inadecuadas	Sensores ambientales (humo, humedad y temperatura), Plan de contingencia.
	(A.5) Accesos no autorizados	Control de acceso lógico-físico
	(E.5) Fallas en el almacenamiento	Política de *Backups* establecidas y socializadas.
Historias Clínicas Activas	(D.4) Daños por condiciones ambientales inadecuadas	Sensores ambientales (humo, humedad y temperatura), Plan de contingencia.
	(A.5) Accesos no autorizados	Control de acceso lógico-físico
	(E.5) Fallas en el almacenamiento	Política de *Backups* establecidas y socializadas.
Hojas De Vida De Equipos Biomédicos	(D.4) Daños por condiciones ambientales inadecuadas	Sensores ambientales (humo, humedad y temperatura), Plan de contingencia.
	(A.5) Accesos no autorizados	Control de acceso lógico y físico
	(E.5) Fallas en el almacenamiento	Política de *Backups* establecidas y socializadas.
Hojas De Vida De Equipos Industriales	(D.4) Daños por condiciones ambientales inadecuadas	Sensores ambientales (humo, humedad y temperatura), Plan de contingencia.
	(A.5) Accesos no autorizados	Control de acceso lógico y físico
	(E.5) Fallas en el almacenamiento	Política de *Backups* establecidas y socializadas.
Historias Laborales Activos e inactivos	(D.4) Daños por condiciones ambientales inadecuadas	Sensores ambientales (humo, humedad y temperatura), Plan de contingencia.
	(A.5) Accesos no autorizados	Control de acceso lógico y físico
	(E.5) Fallas en el almacenamiento	Política de *Backups* establecidas y socializadas.

Tabla 11 Continuación

ACTIVO	AMENAZA	SALVAGUARDA
Comprobantes de Egreso	(D.4) Daños por condiciones ambientales inadecuadas	Sensores ambientales (humo, humedad y temperatura), Plan de contingencia.
	(A.5) Accesos no autorizados	Control de acceso lógico y físico
	(E.5) Fallas en el almacenamiento	Política de *Backups* establecidas y socializadas.
Cuentas por Cobrar	(D.4) Daños por condiciones ambientales inadecuadas	Sensores ambientales (humo, humedad y temperatura), Plan de contingencia.
	(A.5) Accesos no autorizados	Control de acceso lógico/físico
	(E.4) Fallas en el almacenamiento	Política de Backups establecidas y socializadas.
	(A.3) Alteración de la información	Acuerdos de Confidencialidad, manual de uso de recursos informáticos
Informes de Medios Magnéticos	(D.4) Daños por condiciones ambientales inadecuadas	Sensores ambientales (humo, humedad y temperatura), Plan de contingencia.
	(A.5) Accesos no autorizados	Control de acceso lógico físico
	(E.4) Fallas en el almacenamiento	Política de Backups establecidas y socializadas.
	(A.3) Alteración de la información	Acuerdos de Confidencialidad, manual de uso de recursos informáticos
Historia Jurídica de Pacientes Inimputables	(D.4) Daños por condiciones ambientales inadecuadas	Sensores ambientales (humo, humedad y temperatura), Plan de contingencia.
	(A.5) Accesos no autorizados	Control de acceso lógico y físico
	(E.4) Fallas en el almacenamiento	Política de Backups establecidas y socializadas.
	(A.3) Alteración de la información	Acuerdos de Confidencialidad, manual de uso de recursos informáticos

Tabla 11 (Continuación)

ACTIVO	AMENAZA	SALVAGUARDA
Contratos	(D.4) Daños por condiciones ambientales inadecuadas	Sensores ambientales (humo, humedad y temperatura), Plan de contingencia.
	(A.5) Accesos no autorizados	Control de acceso lógico y físico
	(E.4) Fallas en el almacenamiento	Política de *Backups* establecidas y socializadas.
	(A.3) Alteración de la información	Acuerdos de Confidencialidad, manual de uso de recursos informáticos
Acciones legales	(D.4) Daños por condiciones ambientales inadecuadas	Sensores ambientales (humo, humedad y temperatura), Plan de contingencia.
	(A.5) Accesos no autorizados	Control de acceso lógico y físico
	(E.4) Fallas en el almacenamiento	Política de *Backups* establecidas y socializadas.
	(A.3) Alteración de la información	Acuerdos de Confidencialidad, manual de uso de recursos informáticos
Equipos de cómputo – Escritorio	(E.6) Caída del sistema por agotamiento del recurso	Plan de contingencia.
	(E.7) Privilegios de acceso inadecuados o abuso de los mismos	Política de gestión de usuarios.
	(E.3) Averías de origen físico y lógico	Plan de contingencia.
	(D.4) Daños por agua, fuego	Sensores ambientales (humo, humedad y temperatura), Plan de contingencia.
	(D.4) Desastres naturales	Sensores ambientales (humo, humedad y temperatura), Plan de contingencia.
	(E.3) Errores en la actualización	Plan de contingencia documentado y actualizado
	(A.7) Suplantación de usuarios	Control de acceso lógico y físico
	(E.6) Fallas en la configuración y parámetros	Plan de contingencia documentado y actualizado

Fuente: Plataforma Documental HDPUV

8. POLÍTICAS Y ESTRATEGIAS

De acuerdo con la situación actual del Hospital Departamental Psiquiátrico Universitario del Valle, y en consecuencia del análisis de riesgos y las salvaguardas propuestas se implementan una serie de políticas Institucionales y estrategias con el fin de mitigar el riesgo informático, optimizar los recursos informáticos y reducir el impacto de la materialización de las amenazas identificadas del Hospital Departamental Psiquiátrico Universitario del Valle. Estás estrategias hacen parte integral del presente proyecto y se presentan como anexos:

8.1 INVENTARIO DE ACTIVOS

Este inventario contiene la información de los activos informáticos de la Institución asignándole un identificador, responsable y criticidad del activo según el formato estándar de INCIVE, este nos permite catalogar de manera ordenada y completa la información.

8.2 PETI, PLAN ESTRATÉGICO DE TECNOLOGÍAS DE LA INFORMACIÓN

Este instrumento se utiliza para expresar la Estrategia de TI. Incluye una visión, unos principios, unos indicadores, un mapa de ruta, un plan de comunicación y una descripción de todos los demás aspectos (financieros, operativos, de manejo de riesgos, etc.) necesarios para la puesta en marcha y gestión del plan estratégico. El PETI hace parte integral de la estrategia de la institución. Cada vez que una entidad hace un ejercicio o proyecto de Arquitectura Empresarial, su resultado debe ser integrado al PETI. ((Ministerio de Tecnologías de la Información y las Comunicaciones, 2013)

8.3 POLÍTICA DE SEGURIDAD INFORMÁTICA DEL HOSPITAL DEPARTAMENTAL PSIQUIÁTRICO UNIVERSITARIO DEL VALLE E.S.E.

Bajo la cual el Hospital Departamental Psiquiátrico Universitario del Valle E.S.E. reconoce la importancia estratégica de la información y los sistemas de información y por lo cual es importante generar estrategias que permitan garantizar la confidencialidad, disponibilidad e integridad de la información, como herramienta que aporte a la prestación de servicios de manera segura y confiable.

8.4 MANUAL DE USO DE LOS RECURSOS INFORMÁTICOS

Este manual brinda a los clientes internos una guía para el manejo de los recursos informáticos en su labor diaria, propone el autocontrol como base fundamental para la optimización de recursos y mitigación de los riesgos asociados al factor humano, incluye la normatividad que rige a los empleados públicos y las directrices aprobadas por la dirección en cuanto a sanciones por falta de cumplimiento del manual.

8.5 MANTENIMIENTO PREVENTIVO Y CORRECTIVO DE EQUIPOS

Se estable el proceso y los procedimientos con los que se debe llevar a cabo el mantenimiento preventivo y correctivo de equipos de cómputo tales como: computadores (CPU, monitor, teclado y mouse), Impresoras, Scanner, Servidores, Swicht y UPS.

8.6 PLAN DE CONTINGENCIA Y CONTINUIDAD DEL NEGOCIO

El objetivo de este plan es mantener la continuidad de los sistemas de Información frente a eventos adversos que puedan afectar el normal funcionamiento de la infraestructura informática en el Hospital Psiquiátrico Universitario del Valle, y minimizar el impacto negativo sobre la misma, sus usuarios y el servicio.

9. EVALUACIÓN DE LA GESTIÓN INFORMATICA

Con el fin de evaluar la efectividad de las acciones propuestas y poder establecer un valor real de materialización de las amenazas y el impacto generado en caso de presentarse, se realiza inicialmente una encuesta a los clientes internos, se implementan indicadores de gestión de la seguridad informática de la Institución.

9.1 ENCUESTA A CLIENTES INTERNOS

Tabla 12 - Ficha Técnica Encuestas

FICHA TÉCNICA	
Diseño y realización:	Ingeniero Edwin Ruano Gamboa
Tipo de Encuesta:	Encuesta electrónica
Universo :	45
Tamaño de la muestra:	24
Población objetivo:	Empleados de las áreas administrativas del HPDUV
Fecha de la encuesta:	Abril 08 al 15 del 2019
Lugar:	Hospital Departamental Psiquiátrico Universitario del Valle
Análisis:	Edwin Ruano Gamboa – Profesional Universitario
Revisión:	Angélica María Soto González, Líder de proceso

Fuente: Plataforma documental HDPUV

9.2 INDICADOR DE PÉRDIDA DE INFORMACIÓN

Este indicador proporciona información real de datos perdidos en la Institución, ya sea por falla humana o técnica, brindando herramientas para establecer y ejercer controles frente a estas posibles fallas.

Tabla 13 - Indicador de pérdida de Información

PERDIDA DE INFORMACIÓN					
NOMBRE	Perdida de Información	**OBJETIVO**	Medir el nivel de seguridad de la información mediante el porcentaje de fallas que se presenten por periodo		
FORMULA	$\frac{Perdida\ de\ Información}{Total\ de\ equipos}$	**FRECUENIA**	Mensual	**META**	0%
RESPON-SABLE	Ingeniero de Sistemas	**PROCESO**	Gestión de la Información	**FUENTE DEL DATO**	Registro Eventos informáticos

Fuente: Plataforma Documental Hospital Departamental Psiquiátrico Universitario del Valle

9.3 INDICADOR DE TRATAMIENTOS DE EVENTOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

El indicador permite determinar la eficiencia en el tratamiento de eventos relacionados la seguridad de la información. Los eventos serán reportados por los usuarios o determinadas en las auditorías planeadas para el sistema

Tabla 14 - Indicador de tratamientos de eventos de seguridad y privacidad de la información

Indicador de tratamientos de eventos de seguridad y privacidad de la información					
NOMBRE	Disponibilidad de Infraestructura de TI	**OBJETIVO**	Medir el porcentaje de gestión y evolución del modelo de seguridad y privacidad de la información		
FORMULA	$\frac{\#\ eventos - \#\ eventos\ cerrados\ satisfactorio}{Total\ eventos}$	**FRECUENCIA**	Mensual	**META**	95%
RESPONSABLE	Ingeniero de Sistemas	**PROCESO**	Gestión de la Informa-ción	**FUENTE DEL DATO**	Registro Eventos informáti-cos

Fuente: Plataforma Documental Hospital Departamental Psiquiátrico Universitario del Valle

9.4 INDICADOR DE EVENTOS INFORMÁTICOS

Este indicador de oportunidad brinda información de los eventos por tipo que se generan en el área informática, establece la cantidad de eventos de seguridad que se registran en la Institución.

Tabla 15 - Indicador de Eventos Informáticos

EVENTOS INFORMATICOS					
NOMBRE	Eventos Informáticos	**OBJETIVO**	Medir la oportunidad en el tiempo de respuesta y demanda por tipo y áreas de las solicitudes por parte de los usuarios		
FORMULA	Cantidad de Eventos informáticos por tipo	**FRECUENCIA**	Mensual	**META**	90%
RESPONSABLE	Ingeniero de Sistemas	**PROCESO**	Gestión de la Información	**FUENTE DEL DATO**	Registro Eventos informáticos

Fuente: Plataforma Documental Hospital Departamental Psiquiátrico Universitario del Valle

9.5 INDICADOR PLAN DE CAPACITACIÓN

Este indicador mide el plan de capacitación en temática de seguridad informática establecido por la Institución, igualmente el nivel de comprensión y aceptación por parte de los usuarios finales.

Tabla 16 - Indicador Plan de Capacitación

PLAN DE CAPACITACIÓN					
NOMBRE	PLAN DE CAPACITACIÓN	**OBJETIVO**	Establecer la efectividad de los planes de capacitación a usuarios finales sobre la seguridad informática en cuanto a fallas humanas		
FORMULA	$\frac{\#\ de\ fallas\ humanas\ en\ usuarios}{Personal\ Capacitado}$	**FRECUENCIA**	Mensual	**META**	90%
RESPONSABLE	Ingeniero de Sistemas	**PROCESO**	Gestión de la Información	**FUENTE DEL DATO**	Registro Eventos informáticos

Fuente: Plataforma Documental Hospital Departamental Psiquiátrico Universitario del Valle

10. CONCLUSIONES

Uno de los principales retos a los que se enfrentan las entidades del gobierno en la actualidad es controlar la creciente oleada de ataques informáticos, más cuando los datos del negocio están orientados al sector salud, donde el activo de información más sensible es la historia clínica del paciente, por ende, la identificación de amenazas, vulnerabilidades y riesgos que puedan atentar contra la confidencialidad, integridad y disponibilidad de todos los activos de información, se convierte en una estrategia inicial para el establecimiento de controles que hagan frente a los *ciber* ataques.

La falta de conciencia y conocimiento en riesgos de seguridad de la información de directivos del Hospital Psiquiátrico Universitario del Valle fue un punto clave e importante intervenido en el desarrollo de este trabajo.

Realizar un levantamiento exhaustivo de información de cada uno de los activos, permite documentar un inventario completo de activos de información del Hospital Psiquiátrico Universitario del Valle, así como también identificar características importantes que fueron evaluadas en el proceso de gestión del riesgo, bajo la metodología MAGERIT.

Durante la ejecución de los diferentes escaneos y procedimientos de análisis de riesgos se logró identificar 26 vulnerabilidades críticas distribuidas en tres activos de información más sensibles de la entidad como son servidores de aplicaciones y de servicios de red, cuya importancia en la operación de la infraestructura del Hospital Departamental Psiquiátrico Universitario del Valle, amerita una intervención oportuna.

La gestión del riesgo bajo la metodología MAGERIT utilizada en el desarrollo de este trabajo, permite analizar los riesgos que soportan los sistemas de información y realizar las recomendaciones de las medidas que se deben adoptar para conocer, prevenir, impedir, reducir o controlar los riesgos encontrados, realizar un análisis sobre sus principales elementos los cuales define como activo, amenaza, vulnerabilidades, impacto, riesgo y salvaguarda.

11. RECOMENDACIONES

Una vez la Institución tome conciencia desde sus directivos hasta sus clientes internos, de la importancia de la información, no solo como parte activo informático, si no como parte fundamental para el crecimiento y efectividad de los procesos, es mucho más fácil la procura de la integridad, confidencialidad y disponibilidad de la información, más cuando gran parte del procesamiento de datos está dado por sistemas informáticos, como lo son computadores, redes, servidores y otros dispositivos que no manejados adecuadamente pueden poner en riesgo la institución.

Para la continuidad del sistema de gestión de seguridad informática dentro de la institución se brindan las siguientes recomendaciones:

- Actualización tecnológica

Establecer un plan de actualización tecnológico para los activos de información más sensibles como son servidores de aplicaciones y de servicios de red, el cual aborde principalmente las vulnerabilidades más críticas evidenciadas en el presente trabajo.

- Capacitación

Brindar capacitación al área de Sistemas de información, manteniendo actualizados sobre últimas tecnologías, ataques y mecanismos de prevención, igualmente normatividad vigente.

- Implementación de metodologías de *Hacking* Ético

Estas prácticas consisten en realizar pruebas en ambientes controlados y con fines educativos e investigativos con el fin de identificarlos factores de riesgos que

puedan afectar contra la integridad de sistemas informáticos del Hospital Departamental Psiquiátrico Universitario del Valle, a través de esta práctica se puede determinar políticas, protocolos e implantación de mecanismos de prevención.

- Auditoria internas

Realizar auditorías internas semestrales, con el fin de evaluar el cumplimiento de las políticas, procesos y procedimientos implementados del sistema de gestión de seguridad Informática.

- Certificación de la norma ISO 27001

El proceso de Certificación con la norma ISO 27001:2013, brindará al Hospital Departamental Psiquiátrico Universitario del Valle protección de los datos a clientes internos y externos, de igual manera genera una buena imagen corporativa frente a sus partes interesadas que en este caso son pacientes, empresas administradoras de planes de beneficios, entes gubernamentales y funcionarios, donde se logra demostrar el compromiso con la seguridad de la información, reduciendo el riesgo informático, optimizando los recursos y logrando mejorar el rendimiento de los procesos.

BIBLIOGRAFÍA

ABRIL ESTUPIÑAN ANA DEL CARMEN, JAROL ALEXANDER PULIDO, JOHN ALEXANDER BOHADA JAIME: Análisis de riesgos en seguridad de la información. Fundación Universitaria Juan de Castellanos. Santiago de Cali. 2018

ENRIQUEZ EDGAR RODRIGO, NICOLAR SOLARTE FRANCISCO: Metodologia de análisis y evaluación de riesgos aplicados a la seguridad informática y de información bajo la norma ISO/IEC 27001. Santiago de Cali. 2016

GOBIERNO DE COLOMBIA. FUNCIÓN PÚBLICA Sistemas de Información: Modelo Integrado de Planeación y Gestión MIPG. Santa Fe de Bogotá. 2017

GOBIERNO DE ESPAÑA, VICEPRECIDENCIA TERCERA DEL GOBIERNO, ministerio de asuntos económicos y transformación digital, secretaria de estado de digitalización e inteligencia artificial, Instituto nacional de ciberseguridad, [sitio web]. España [Consultado: 30 de abril de 2020]. Disponible en: https://www.incibe-cert.es/alerta-temprana/vulnerabilidades

GORDON LYON, NETWORK MAPPER. (05 de 2020). [Sitio web]. USA; [Consultado: 28 de abril de 2020]. Disponible en: nmap.org: https://nmap.org/book/man.html#man-description

HOSPITAL DEPARTAMENTAL PSIQUIÁTRICO UNIVERSITARIO DEL VALLE. Sistemas de Información: Manual de uso de los recursos informaticos. Plataforama documental. Santiago de Cali. 2014

INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN. Documentación. Bogotá: ICONTEC, 1995. (NTC 1487)

INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN. 17 de febrero de 2016. Bogotá: ICONTEC. NTC 6166

MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS. MAGERIT: Versión 3.0, Metodología de Análisis y Gestiónde Riesgos de los Sistemas de Información. Libro I – Método. Ministerio de Hacienda y Administraciones Públicas Secretaría General Técnica, Subdirección General de Información,Documentación y PublicacionesCentro de Publicaciones. Madrid, octubre de 2012

MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS. MAGERIT: versión 3.0Metodología de Análisis y Gestiónde Riesgos de los Sistemas de InformaciónLibro II - Catálogo de Elementos. Ministerio de Hacienda y Administraciones PúblicasSecretaría General Técnica, Subdirección General de Información,Documentación y PublicacionesCentro de Publicaciones. Madrid, octubre de 2012.

MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS. MAGERIT: versión 3.0Metodología de Análisis y Gestiónde Riesgos de los Sistemas de InformaciónLibro III - Guía de Técnicas. Ministerio de Hacienda y Administraciones PúblicasSecretaría General Técnica, Subdirección General de Información,Documentación y PublicacionesCentro de Publicaciones. Madrid, octubre de 2012

MIRANDA CAIRO MICHEL, VALDÉS PUGA OSMANY: Metodología para la Implementación de la Gestión Automatizada de Controles de Seguridad Informática. Santiago de Cali, 2017.

National Institute of Standars and Technology, U.S. Department of commerce, [sitio web]. USA; [Consultado: 30 de abril de 2020]. Disponible en: https://nvd.nist.gov/vuln.

The MITRE Corporation. Agosto 19 2020. CVE, Common Vulnerabilities and Exposures. U.S. Department of Homeland Security. [sitio web]. USA; [Consultado: 22 de mayo de 2020]. Disponible desde Internet en: https://cve.mitre.org/

12. ANEXOS

A. Inventario de Activos

B. PETI, Plan estratégico de tecnologías de la Información

C. Política de Seguridad de la Información y uso de los recursos Informáticos del Hospital Departamental Psiquiátrico Universitario del Valle E.S.E

D. Manual de Seguridad de la Información y Uso de los Recursos Informáticos

E. Mantenimiento preventivo y correctivo de equipos de cómputo

F. Procedimiento contingencia y acciones preventivas para sistemas